Algebra Abstracta

Teoría y Aplicaciones

Algebra Abstracta

Teoría y Aplicaciones

Thomas W. Judson
Stephen F. Austin State University

Sage Exercises for Abstract Algebra

Robert A. Beezer
University of Puget Sound

Traducción (parcial) al español

Antonio Behn
Universidad de Chile

August 5, 2017

Edición: Annual Edition 2017

Sitio web: abstract.pugetsound.edu

Agradecimentos

I would like to acknowledge the following reviewers for their helpful comments and suggestions.

- David Anderson, University of Tennessee, Knoxville
- Robert Beezer, University of Puget Sound
- Myron Hood, California Polytechnic State University
- Herbert Kasube, Bradley University
- John Kurtzke, University of Portland
- Inessa Levi, University of Louisville
- Geoffrey Mason, University of California, Santa Cruz
- Bruce Mericle, Mankato State University
- Kimmo Rosenthal, Union College
- Mark Teply, University of Wisconsin

I would also like to thank Steve Quigley, Marnie Pommett, Cathie Griffin, Kelle Karshick, and the rest of the staff at PWS Publishing for their guidance throughout this project. It has been a pleasure to work with them.

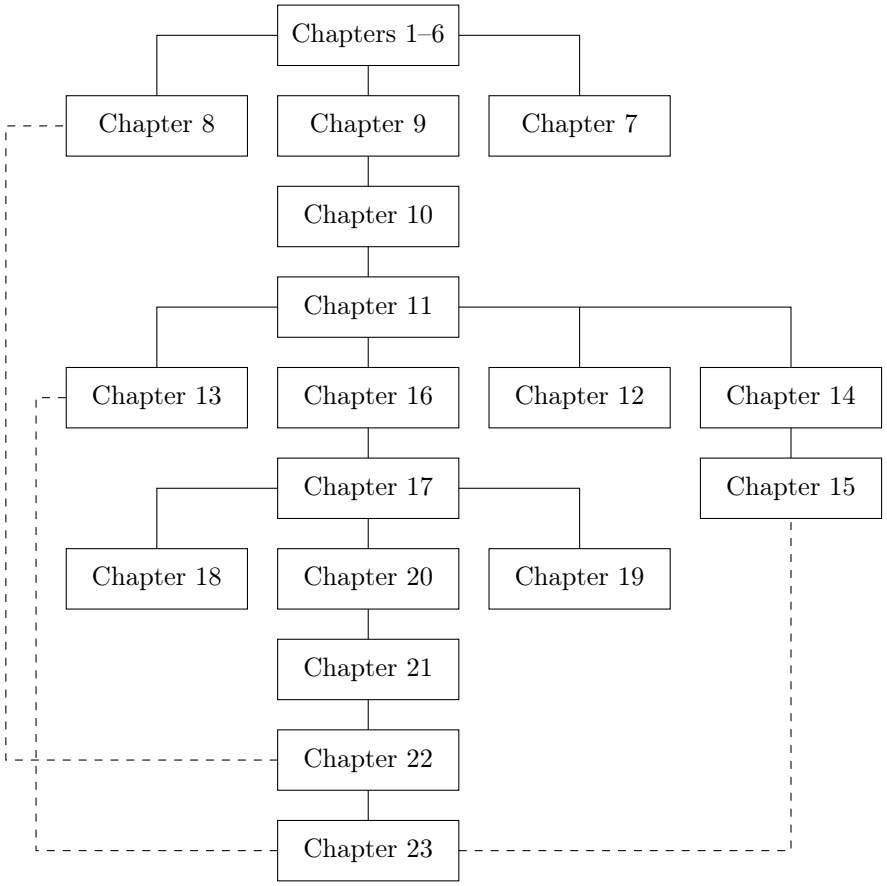
Robert Beezer encouraged me to make *Abstract Algebra: Theory and Applications* available as an open source textbook, a decision that I have never regretted. With his assistance, the book has been rewritten in PreTeXt (http://mathbook.pugetsound.edu), making it possible to quickly output print, web, PDF versions and more from the same source. The open source version of this book has received support from the National Science Foundation (Awards #DUE-1020957 and #DUE–1625223).

Prefacio

This text is intended for a one or two-semester undergraduate course in abstract algebra. Traditionally, these courses have covered the theoretical aspects of groups, rings, and fields. However, with the development of computing in the last several decades, applications that involve abstract algebra and discrete mathematics have become increasingly important, and many science, engineering, and computer science students are now electing to minor in mathematics. Though theory still occupies a central role in the subject of abstract algebra and no student should go through such a course without a good notion of what a proof is, the importance of applications such as coding theory and cryptography has grown significantly.

Until recently most abstract algebra texts included few if any applications. However, one of the major problems in teaching an abstract algebra course is that for many students it is their first encounter with an environment that requires them to do rigorous proofs. Such students often find it hard to see the use of learning to prove theorems and propositions; applied examples help the instructor provide motivation.

This text contains more material than can possibly be covered in a single semester. Certainly there is adequate material for a two-semester course, and perhaps more; however, for a one-semester course it would be quite easy to omit selected chapters and still have a useful text. The order of presentation of topics is standard: groups, then rings, and finally fields. Emphasis can be placed either on theory or on applications. A typical one-semester course might cover groups and rings while briefly touching on field theory, using Chapters 1 through 6, 9, 10, 11, 13 (the first part), 16, 17, 18 (the first part), 20, and 21. Parts of these chapters could be deleted and applications substituted according to the interests of the students and the instructor. A two-semester course emphasizing theory might cover Chapters 1 through 6, 9, 10, 11, 13 through 18, 20, 21, 22 (the first part), and 23. On the other hand, if applications are to be emphasized, the course might cover Chapters 1 through 14, and 16 through 22. In an applied course, some of the more theoretical results could be assumed or omitted. A chapter dependency chart appears below. (A broken line indicates a partial dependency.)



Though there are no specific prerequisites for a course in abstract algebra, students who have had other higher-level courses in mathematics will generally be more prepared than those who have not, because they will possess a bit more mathematical sophistication. Occasionally, we shall assume some basic linear algebra; that is, we shall take for granted an elementary knowledge of matrices and determinants. This should present no great problem, since most students taking a course in abstract algebra have been introduced to matrices and determinants elsewhere in their career, if they have not already taken a sophomore or junior-level course in linear algebra.

Exercise sections are the heart of any mathematics text. An exercise set appears at the end of each chapter. The nature of the exercises ranges over several categories; computational, conceptual, and theoretical problems are included. A section presenting hints and solutions to many of the exercises appears at the end of the text. Often in the solutions a proof is only sketched, and it is up to the student to provide the details. The exercises range in difficulty from very easy to very challenging. Many of the more substantial problems require careful thought, so the student should not be discouraged if the solution is not forthcoming after a few minutes of work.

There are additional exercises or computer projects at the ends of many of the chapters. The computer projects usually require a knowledge of programming. All of these exercises and projects are more substantial in nature and allow the exploration of new results and theory.

Sage (sagemath.org) is a free, open source, software system for advanced mathematics, which is ideal for assisting with a study of abstract algebra. Sage can be used either on your own computer, a local server, or on CoCalc (cocalc.com). Robert Beezer has written a comprehensive introduction to Sage

and a selection of relevant exercises that appear at the end of each chapter, including live Sage cells in the web version of the book. All of the Sage code has been subject to automated tests of accuracy, using the most recent version available at this time: Sage Version 8.0 (released 2017-07-21).

Thomas W. Judson
Nacogdoches, Texas 2016

Índice

1

Preliminares

Se requiere una cierta madurez matemática para encontrar y estudiar aplicaciones del álgebra abstracta. Un conocimiento básico de teoría de conjuntos, inducción matemática, relaciones de equivalencia y matrices es necesario. Aún más importante es la habilidad de leer y entender demostraciones matemáticas. En este capítulo resumiremos los prerrequisitos necesarios para un curso de álgebra abstracta.

1.1 Una Breve Nota sobre Demostraciones

La matemática abstracta es diferente de otras ciencias. En las ciencias de laboratorio como química y física, los científicos hacen experimentos para descubrir nuevos principios y verificar teorías. Si bien las matemáticas están frecuentemente motivadas por experimentos físicos o simulaciones computacionales, se hacen rigurosas mediante el uso de argumentos lógicos. Al estudiar matemáticas abstractas, usamos lo que se llama el método axiomático; es decir, tomamos una colección de objetos $\mathcal{S}$ y suponemos ciertas reglas sobre su estructura. Estas reglas se llaman ***axiomas***. Usando los axiomas para $\mathcal{S}$, queremos deducir otra información sobre $\mathcal{S}$ usando argumentos lógicos. Requerimos que nuestros axiomas sean consistentes; es decir, no debiesen contradecirse entre ellos. También exigimos que no haya demasiados axiomas. Si un sistema de axiomas es demasiado restrictivo, habrá muy pocos ejemplos de la estructura matemática.

Un ***enunciado*** en lógica o matemáticas es una afirmación o frase, en lenguaje natural o usando simbología matemática, que es verdadera o falsa. Considere los siguientes ejemplos:

- $3 + 56 - 13 + 8/2$.
- Todos los gatos son negros.
- $2 + 3 = 5$.
- $2x = 6$ si y solo si $x = 4$.
- If $ax^2 + bx + c = 0$ y $a \neq 0$, then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

- $x^3 - 4x^2 + 5x - 6$.

Todos salvo el primero y el último son enunciados, y deben ser verdaderos o falsos.

Una ***demostración matemática*** no es más ni menos que un argumento convincente de la veracidad de un enunciado. Un tal argumento debiese contener suficiente detalle para convencer a la audiencia; por ejemplo podemos ver que el enunciado "$2x = 6$ si y solo si $x = 4$" es falso evaluando $2 \cdot 4$ y notando que $6 \neq 8$, un argumento que satisfacerá a cualquiera. Por supuesto, las audiencias son muy diversas: demostraciones pueden estar dirigidas a otro estudiante, a un profesor, o al lector de un escrito. Si se presenta más detalle del necesario en una demostración, ésta puede ser muy larga o incluso confusa. Si se omiten demasiados detalles, el argumento puede no ser convincente. Es importante tener en cuenta la audiencia al escribir la demostración. Estudiantes de secundaria requerirán mucho más detalles que estudiantes de post-grado. Una buena regla de oro en un curso introductorio de álgebra abstracta es que la demostración debiese ser escrita pensando en los compañeros de uno, sean estos otros estudiantes o sean lectores del texto.

Examinemos distintos tipos de enunciados. Un enunciado puede ser tan simple como "$10/5 = 2$;" pero, los matemáticos usualmente están interesados en enunciados más complejas tales como "Si p, entonces q," donde p y q son a su vez enunciados. Si cierto enunciado es conocido o suponemos que es cierto, queremos saber lo que podemos decir sobre otros enunciados. Acá p se llama ***hipótesis*** y q se conoce como ***conclusión***. Considere el siguiente enunciado: Si $ax^2 + bx + c = 0$ y $a \neq 0$, entonces

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

La hipótesis es que $ax^2 + bx + c = 0$ y $a \neq 0$; la conclusión es

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Note que el enunciado no dice nada sobre si la hipótesis es verdadera o no. Pero, si el enunciado completo es verdadero y podemos mostrar que $ax^2 + bx + c = 0$ con $a \neq 0$ es verdadero, entonces la conclusión *debe* ser verdadera. Una demostración de este enunciado puede ser simplemente una serie de ecuaciones:

$$\begin{aligned}
ax^2 + bx + c &= 0 \\
x^2 + \frac{b}{a}x &= -\frac{c}{a} \\
x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2 &= \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \\
\left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2} \\
x + \frac{b}{2a} &= \frac{\pm\sqrt{b^2 - 4ac}}{2a} \\
x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.
\end{aligned}$$

Si podemos demostrar la veracidad del enunciado, entonces el enunciado se llama ***proposición***. Una proposición de mayor importancia se llama ***Teorema***. A veces, en lugar de demostrar un teorema o proposición de una sola vez, descomponemos la demostración en módulos; es decir, demostramos varias proposiciones auxiliares, que se llaman ***Lemas***, y usamos los resultados de estas proposiciones para demostrar el resultado principal. Si podemos demostrar

una proposición o teorema, frecuentemente podremos obtener resultados relacionados con muy poco esfuerzo adicional, estos se llaman ***Corolarios***.

Algunas Advertencias y Sugerencias

Existen diversas estrategias para demostrar proposiciones. Además de usar diferentes métodos de demostración, los estudiantes suelen cometer errores comunes cuando recién comienzan a demostrar teoremas. Para ayudar a los estudiantes primerizos de matemáticas abstractas, listamos acá algunas de las dificultades que pueden encontrar y algunas de las estrategias a su disposición. Es una buena idea volver a mirar esta lista como recordatorio. (Otras técnicas de demostración aparecerán a lo largo de este capítulo y en el resto del texto.)

- Un teorema no puede ser demostrado con un ejemplo; pero, el método estándar para demostrar que una proposición no es verdadera, es dar un contraejemplo.
- Los cuantificadores son importantes. Palabras y frases como *único*, *para todos*, *para cada*, y *para algún* tienen significados diferentes.
- Nunca suponga una hipótesis que no se da explícitamente en un teorema. *No puede dar cosas por sabidas.*
- Supongamos que quiere mostrar que un objeto *existe* y es *único*. Primero muestre que el objeto realmente existe. Para demostrar que es único, supongamos que hay dos tales objetos, digamos r y s, y después demuestre que $r = s$.
- A veces es más fácil demostrar el contrapositivo de una proposición. Demostrar la proposición "Si p, entonces q" es exactamente lo mismo que demostrar la proposición "Si no q, entonces no p."
- Si bien usualmente es mejor encontrar una demostración directa de un teorema, esto puede ser difícil. Podría ser más fácil suponer que el teorema que está tratando de demostrar es falso, y esperar que a lo largo de su argumento se vea obligado a deducir un enunciado que no pueda ser verdadero.

Recuerde que uno de los objetivos principales de las matemáticas superiores es demostrar teoremas. Los teoremas son herramientas que permiten nuevas y productivas aplicaciones de las matemáticas. Usamos ejemplos para ilustrar teoremas existentes y para incentivar el desarrollo de la intuición sobre la razón de la posible veracidad de nuevos teoremas. Aplicaciones, ejemplos y demostraciones están fuertemente interconectados—mucho más de lo que puede parecer en primera instancia.

1.2 Conjuntos y Relaciones de Equivalencia

Teoría de Conjuntos

Un ***conjunto*** es una colección bien-definida de objetos; es decir, está definida de manera que para un objeto x cualquiera, podamos determinar si x pertenece o no al conjunto. Los objetos que pertenecen al conjunto se llaman ***elementos*** o ***miembros***. Denotaremos los conjuntos por letras mayúsculas, tales como A o X; si a es un elemento del conjunto A, escribimos $a \in A$.

Un conjunto usualmente se define ya sea listando todos los elementos que contiene entre un par de llaves o indicando la propiedad que determina si un

objeto x pertenece o no al conjunto. Podemos escribir

$$X = \{x_1, x_2, \ldots, x_n\}$$

para un conjunto que contiene los elementos $x_1, x_2, \ldots, x_n$ o

$$X = \{x : x \text{ satisface } \mathcal{P}\}$$

si cada x en X satisface cierta propiedad $\mathcal{P}$. Por ejemplo, si E es el conjunto de enteros pares positivos, podemos describir E escribiendo ya sea

$$E = \{2, 4, 6, \ldots\} \quad \text{o} \quad E = \{x : x \text{ es un entero par y } x > 0\}.$$

Escribimos $2 \in E$ cuando queremos decir que 2 está en el conjunto E, y $-3 \notin E$ para decir que -3 no está en el conjunto E.

Algunos de los conjuntos más importantes que consideraremos son los siguientes:

$$\mathbb{N} = \{n : n \text{ es un número natural}\} = \{1, 2, 3, \ldots\};$$
$$\mathbb{Z} = \{n : n \text{ es un entero}\} = \{\ldots, -1, 0, 1, 2, \ldots\};$$
$$\mathbb{Q} = \{r : r \text{ es un número racional}\} = \{p/q : p, q \in \mathbb{Z} \text{ con } q \neq 0\};$$
$$\mathbb{R} = \{x : x \text{ es un número real}\};$$
$$\mathbb{C} = \{z : z \text{ es un número complejo}\}.$$

Podemos encontrar varias relaciones entre conjuntos y realizar operaciones entre ellos. Un conjunto A es un ***subconjunto*** de B, denotado $A \subset B$ o $B \supset A$, si todo elemento de A también es un elemento de B. Por ejemplo,

$$\{4, 5, 8\} \subset \{2, 3, 4, 5, 6, 7, 8, 9\}$$

y

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Trivialmente, todo conjunto es subconjunto de si mismo. Un conjunto B es un ***subconjunto propio*** de un conjunto A si $B \subset A$ pero $B \neq A$. Si A no es un subconjunto de B, escribimos $A \not\subset B$; por ejemplo, $\{4, 7, 9\} \not\subset \{2, 4, 5, 8, 9\}$. Dos conjuntos son ***iguales***, escrito $A = B$, si contienen los mismos elementos. Esto es equivalente a que $A \subset B$ y $B \subset A$.

Es conveniente tener un conjunto sin elementos. Este conjunto se llama ***conjunto vacío*** y se denota por $\emptyset$. Notemos que el conjunto vacío es un subconjunto de todo conjunto.

Para construir conjuntos nuevos a partir de otros conjuntos, podemos realizar ciertas operaciones: la ***unión*** $A \cup B$ de dos conjuntos A y B se define como

$$A \cup B = \{x : x \in A \text{ o } x \in B\};$$

la ***intersección*** de A y B se define como

$$A \cap B = \{x : x \in A \text{ y } x \in B\}.$$

Si $A = \{1, 3, 5\}$ y $B = \{1, 2, 3, 9\}$, entonces

$$A \cup B = \{1, 2, 3, 5, 9\} \quad \text{y} \quad A \cap B = \{1, 3\}.$$

Podemos considerar la unión y la intersección de más de dos conjuntos. En este caso escribimos

$$\bigcup_{i=1}^{n} A_i = A_1 \cup \ldots \cup A_n$$

y

$$\bigcap_{i=1}^{n} A_i = A_1 \cap \ldots \cap A_n$$

para la unión e intersección, respectivamente de los conjuntos $A_1, \ldots, A_n$. También se pueden definir la unión y la intersección de una colección infinita (o arbitraria) de conjuntos. Si $\mathcal{S} = \{A_i : i \in \mathcal{I}\}$, entonces

$$\bigcup \mathcal{S} = \bigcup_{i \in \mathcal{I}} A_i = \{x : x \in A_i \text{ para algún } A_i \in \mathcal{S}\}$$

y

$$\bigcap \mathcal{S} = \bigcap_{i \in \mathcal{I}} A_i = \{x : x \in A_i \text{ para todo } A_i \in \mathcal{S}\}$$

para la unión e intersección, respectivamente, de los conjuntos en $\mathcal{S}$ indexados por $\mathcal{I}$.

Cuando dos conjuntos no tienen elementos en común, se dice que son ***disjuntos***; por ejemplo, si P es el conjunto de los enteros pares e I es el conjunto de los enteros impares, entonces P e I son disjuntos. Dos conjuntos A y B son disjuntos precisamente cuando $A \cap B = \emptyset$.

En ocasiones trabajaremos con un conjunto fijo U, llamado ***conjunto universal***. Para cualquier conjunto $A \subset U$, podemos definir el ***complemento*** de A, denotado por A', como el conjunto

$$A' = \{x : x \in U \text{ y } x \notin A\}.$$

Definimos la ***diferencia*** de dos conjuntos A y B como

$$A \setminus B = A \cap B' = \{x : x \in A \text{ y } x \notin B\}.$$

Ejemplo 1.1. Sea $\mathbb{R}$ el conjunto universal y supongamos que

$$A = \{x \in \mathbb{R} : 0 < x \leq 3\} \quad \text{y} \quad B = \{x \in \mathbb{R} : 2 \leq x < 4\}.$$

Entonces

$$\begin{aligned} A \cap B &= \{x \in \mathbb{R} : 2 \leq x \leq 3\} \\ A \cup B &= \{x \in \mathbb{R} : 0 < x < 4\} \\ A \setminus B &= \{x \in \mathbb{R} : 0 < x < 2\} \\ A' &= \{x \in \mathbb{R} : x \leq 0 \text{ o } x > 3\}. \end{aligned}$$

Proposición 1.2. *Sean A, B, y C conjuntos. Entonces*

1. *$A \cup A = A$, $A \cap A = A$, y $A \setminus A = \emptyset$;*
2. *$A \cup \emptyset = A$ y $A \cap \emptyset = \emptyset$;*
3. *$A \cup (B \cup C) = (A \cup B) \cup C$ y $A \cap (B \cap C) = (A \cap B) \cap C$;*
4. *$A \cup B = B \cup A$ y $A \cap B = B \cap A$;*
5. *$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;*
6. *$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.*

DEMOSTRACIÓN. Demostraremos (1) y (3) y dejaremos las demostraciones de los demás resultados como ejercicios.

(1) Observe que

$$\begin{aligned} A \cup A &= \{x : x \in A \text{ o } x \in A\} \\ &= \{x : x \in A\} \\ &= A \end{aligned}$$

y

$$\begin{aligned} A \cap A &= \{x : x \in A \text{ y } x \in A\} \\ &= \{x : x \in A\} \\ &= A. \end{aligned}$$

Además, $A \setminus A = A \cap A' = \emptyset$.

(3) Para conjuntos A, B, y C,

$$\begin{aligned} A \cup (B \cup C) &= A \cup \{x : x \in B \text{ o } x \in C\} \\ &= \{x : x \in A \text{ o } x \in B, \text{ o } x \in C\} \\ &= \{x : x \in A \text{ o } x \in B\} \cup C \\ &= (A \cup B) \cup C. \end{aligned}$$

Un argumento similar demuestra que $A \cap (B \cap C) = (A \cap B) \cap C$. □

Teorema 1.3 (Leyes de De Morgan)**.** *Sean A y B conjuntos. Entonces*

1. $(A \cup B)' = A' \cap B'$;
2. $(A \cap B)' = A' \cup B'$.

DEMOSTRACIÓN. (1) Si $A \cup B = \emptyset$, entonces el teorema es inmediato pues tanto A como B son el conjunto vacío. De otra manera, debemos mostrar que $(A \cup B)' \subset A' \cap B'$ y $(A \cup B)' \supset A' \cap B'$. Sea $x \in (A \cup B)'$. Entonces $x \notin A \cup B$. Así x no está en A ni en B, por la definición de la unión de conjuntos. Por la definición del complemento, $x \in A'$ y $x \in B'$. Por lo tanto, $x \in A' \cap B'$ y tenemos $(A \cup B)' \subset A' \cap B'$.

Para mostrar la inclusión inversa, supongamos que $x \in A' \cap B'$. Entonces $x \in A'$ y $x \in B'$, y así $x \notin A$ y $x \notin B$. Luego $x \notin A \cup B$ y así $x \in (A \cup B)'$. Por lo tanto, $(A \cup B)' \supset A' \cap B'$ y así $(A \cup B)' = A' \cap B'$.

La demostración de (2) la dejamos como ejercicio. □

Ejemplo 1.4. Otras relaciones entre conjunto son por ejemplo,

$$(A \setminus B) \cap (B \setminus A) = \emptyset.$$

Para ver que esta es verdadera, observe que

$$\begin{aligned} (A \setminus B) \cap (B \setminus A) &= (A \cap B') \cap (B \cap A') \\ &= A \cap A' \cap B \cap B' \\ &= \emptyset. \end{aligned}$$

Producto Cartesiano y Funciones

Dados dos conjuntos A y B, podemos definir un nuevo conjunto $A \times B$, llamado ***producto Cartesiano*** de A y B, como conjunto de pares ordenados. Esto es,

$$A \times B = \{(a, b) : a \in A \text{ y } b \in B\}.$$

Ejemplo 1.5. Si $A = \{x, y\}$, $B = \{1, 2, 3\}$, y $C = \emptyset$, entonces $A \times B$ es el conjunto

$$\{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$$

y

$$A \times C = \emptyset.$$

Definimos el ***producto Cartesiano de*** n ***conjuntos*** como

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_i \in A_i \text{ para } i = 1, \ldots, n\}.$$

Si $A = A_1 = A_2 = \cdots = A_n$, escribiremos A^n para $A \times \cdots \times A$ (donde A se escribiría n veces). Por ejemplo, el conjunto $\mathbb{R}^3$ consiste de todas las 3-tuplas de números reales.

Subconjuntos de $A \times B$ se llaman ***relaciones***. Definiremos un ***mapeo*** o ***función*** $f \subset A \times B$ de un conjunto A en un conjunto B como el tipo especial de relación donde $(a, b) \in f$ si para todo elemento $a \in A$ existe un único elemento $b \in B$. Otra forma de decir esto es que para cada elemento en A, f asigna un único elemento en B. Usualmente escribimos $f : A \to B$ o $A \xrightarrow{f} B$. En lugar de escribir pares ordenados $(a, b) \in A \times B$, escribimos $f(a) = b$ o $f : a \mapsto b$. El conjunto A se llama ***dominio*** de f y

$$f(A) = \{f(a) : a \in A\} \subset B$$

se llama ***rango*** o ***imagen*** de f. Podemos pensar los elementos del dominio de una función como valores de entrada y los elementos del rango de la función como valores de salida.

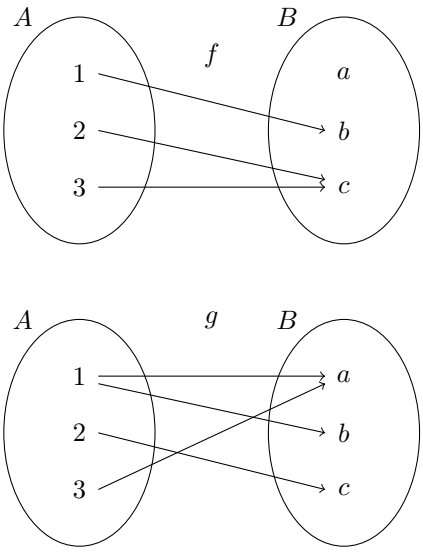


Figura 1.6: Funciones y Relaciones

Ejemplo 1.7. Supongamos $A = \{1, 2, 3\}$ y $B = \{a, b, c\}$. En la Figura 1.6 definimos las relaciones f y g de A en B. La relación f es una función, pero g

no lo es pues a $1 \in A$ no se le asigna una única imagen en B; es decir, $g(1) = a$ y $g(1) = b$.

Dada una función $f : A \to B$, a veces es posible hacer una lista describiendo lo que le hace la función a cada elemento específico del dominio. Pero no todas las funciones pueden ser descritas de esta manera. Por ejemplo, la función $f : \mathbb{R} \to \mathbb{R}$ que envía a cada número real en su cubo es una función que debe ser descrita escribiendo $f(x) = x^3$ o $f : x \mapsto x^3$.

Considere la relación $f : \mathbb{Q} \to \mathbb{Z}$ dada por $f(p/q) = p$. Sabemos que $1/2 = 2/4$, pero es $f(1/2) = 1$ o 2? Esta relación no puede ser una función pues no está bien-definida. Una relación está ***bien-definida*** si a cada elemento en el dominio se le asigna un *único* elemento en el rango.

Si $f : A \to B$ es una función y la imagen de f es B, es decir, $f(A) = B$, entonces f se dice ***sobre*** o ***sobreyectiva***. En otras palabras, si para cada $b \in B$ existe $a \in A$ tal que $f(a) = b$, entonces f es sobre. Una función es ***1-1*** o ***inyectiva*** si $a_1 \neq a_2$ implica $f(a_1) \neq f(a_2)$. Equivalentemente, una función es 1-1 si $f(a_1) = f(a_2)$ implica $a_1 = a_2$. Una función que es 1-1 y sobre se llama ***biyectiva***.

Ejemplo 1.8. Sea $f : \mathbb{Z} \to \mathbb{Q}$ definida como $f(n) = n/1$. Entonces f es 1-1 pero no sobre. Defina $g : \mathbb{Q} \to \mathbb{Z}$ como $g(p/q) = p$ donde p/q es un número racional en su forma reducida con denominador positivo. La función g es sobre pero no 1-1.

Dadas dos funciones, podemos construir una nueva función usando el rango de la primera función como el dominio de la segunda. Sean $f : A \to B$ y $g : B \to C$ funciones. Definimos una nueva función, la ***composición*** de f y g de A en C, como $(g \circ f)(x) = g(f(x))$.

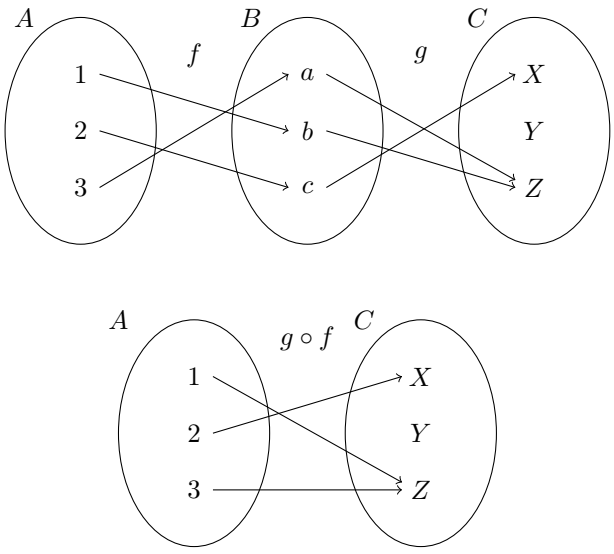


Figura 1.9: Composición de funciones

Ejemplo 1.10. Considere las funciones $f : A \to B$ y $g : B \to C$ que están definidas en la Figura 1.9 (arriba). La composición de estas funciones, $g \circ f : A \to C$, está definida en la Figura 1.9 (abajo).

Ejemplo 1.11. Sean $f(x) = x^2$ y $g(x) = 2x + 5$. Entonces

$$(f \circ g)(x) = f(g(x)) = (2x + 5)^2 = 4x^2 + 20x + 25$$

y

$$(g \circ f)(x) = g(f(x)) = 2x^2 + 5.$$

En general, el orden importa; es decir, en la mayoría de los casos $f \circ g \neq g \circ f$.

Ejemplo 1.12. A veces se cumple que $f \circ g = g \circ f$. Sean $f(x) = x^3$ y $g(x) = \sqrt[3]{x}$. Entonces

$$(f \circ g)(x) = f(g(x)) = f(\sqrt[3]{x}\,) = (\sqrt[3]{x}\,)^3 = x$$

y

$$(g \circ f)(x) = g(f(x)) = g(x^3) = \sqrt[3]{x^3} = x.$$

Ejemplo 1.13. Dada una matriz de 2×2

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

podemos definir una función $T_A : \mathbb{R}^2 \to \mathbb{R}^2$ como

$$T_A(x, y) = (ax + by, cx + dy)$$

para (x, y) en $\mathbb{R}^2$. Esto en realidad es multiplicación de matrices; es decir,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Funciones de $\mathbb{R}^n$ en $\mathbb{R}^m$ dadas por matrices se llaman ***funciones lineales*** o ***transformaciones lineales***.

Ejemplo 1.14. Supongamos que $S = \{1, 2, 3\}$. Definamos una función $\pi : S \to S$ como

$$\pi(1) = 2, \qquad \pi(2) = 1, \qquad \pi(3) = 3.$$

Esta es una función biyectiva. Una forma alternativa de escribir π es

$$\begin{pmatrix} 1 & 2 & 3 \\ \pi(1) & \pi(2) & \pi(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Para cualquier conjunto S, una función biyectiva $\pi : S \to S$ se llama ***permutación*** de S.

Teorema 1.15. *Sean $f : A \to B$, $g : B \to C$, y $h : C \to D$. Entonces*

1. *La composición de funciones es asociativa; es decir, $(h \circ g) \circ f = h \circ (g \circ f)$;*
2. *Si f y g son ambas 1-1, entonces la función $g \circ f$ es 1-1;*
3. *Si f y g son ambas sobre, entonces la función $g \circ f$ es sobre;*
4. *Si f y g son ambas biyectivas, entonces la función $g \circ f$ es biyectiva;*

Demostración. Demostraremos (1) y (3). La parte (2) se deja como ejercicio. La Parte (4) es consecuencia directa de (2) y (3).

(1) Debemos mostrar que

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Para $a \in A$ tenemos

$$(h \circ (g \circ f))(a) = h((g \circ f)(a))$$

$$\begin{aligned} &= h(g(f(a))) \\ &= (h \circ g)(f(a)) \\ &= ((h \circ g) \circ f)(a). \end{aligned}$$

(3) Supongamos que f y g son ambas sobreyectivas. Dado $c \in C$, debemos mostrar que existe $a \in A$ tall que $(g \circ f)(a) = g(f(a)) = c$. Pero, como g es sobre, existe $b \in B$ tal que $g(b) = c$. Similarmente, existe $a \in A$ tal que $f(a) = b$. Por ende,

$$(g \circ f)(a) = g(f(a)) = g(b) = c. \qquad \square$$

Si S es cualquier conjunto, usaremos id_S o id para denotar a la ***función identidad*** de S en si mismo. Definimos esta función como $id(s) = s$ para todo $s \in S$. Una función $g : B \to A$ es una ***función inversa*** de $f : A \to B$ si $g \circ f = id_A$ y $f \circ g = id_B$; en otras palabras, la función inversa de una función simplemente "deshace" lo que hace la función. Una función se dice ***invertible*** si tiene una inversa. Usualmente escribimos f^{-1} para la inversa de f.

Ejemplo 1.16. La función $f(x) = x^3$ tiene inversa $f^{-1}(x) = \sqrt[3]{x}$ por el Ejemplo 1.12.

Ejemplo 1.17. El logaritmo natural y la función exponencial, $f(x) = \ln x$ y $f^{-1}(x) = e^x$, son inversas, la una de la otra, con tal de que seamos cuidadosos en la elección de los dominios. Observe que

$$f(f^{-1}(x)) = f(e^x) = \ln e^x = x$$

y

$$f^{-1}(f(x)) = f^{-1}(\ln x) = e^{\ln x} = x$$

siempre que la composición tenga sentido.

Ejemplo 1.18. Supongamos que

$$A = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}.$$

Entonces A define una función de $\mathbb{R}^2$ en $\mathbb{R}^2$ como

$$T_A(x, y) = (3x + y, 5x + 2y).$$

Podemos encontrar la función inversa de T_A simplemente invirtiendo la matriz A; es decir, $T_A^{-1} = T_{A^{-1}}$. En este ejemplo,

$$A^{-1} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix};$$

luego, la función inversa está dada por

$$T_A^{-1}(x, y) = (2x - y, -5x + 3y).$$

Es fácil verificar que

$$T_A^{-1} \circ T_A(x, y) = T_A \circ T_A^{-1}(x, y) = (x, y).$$

No toda función tiene inversa. Si consideramos la función

$$T_B(x, y) = (3x, 0)$$

dada por la matriz

$$B = \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix},$$

una función inversa tendría que ser de la forma

$$T_B^{-1}(x, y) = (ax + by, cx + dy)$$

y

$$(x, y) = T \circ T_B^{-1}(x, y) = (3ax + 3by, 0)$$

para todo x e y. Claramente esto es imposible pues y podría no ser 0.

Ejemplo 1.19. Dada la permutación

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

en $S = \{1, 2, 3\}$, es fácil ver que la permutación definida por

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

es la inversa de π. De hecho, toda función biyectiva posee una inversa, como veremos en el próximo teorema.

Teorema 1.20. *Una función es invertible si y solo si es biyectiva.*

DEMOSTRACIÓN. Supongamos primero que $f : A \to B$ es invertible con inversa $g : B \to A$. Entonces $g \circ f = id_A$ es la función identidad; es decir, $g(f(a)) = a$. Si $a_1, a_2 \in A$ con $f(a_1) = f(a_2)$, entonces $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$. Así, f es 1-1. Ahora supongamos que $b \in B$. Para mostrar que f es sobre, es necesario encontrar $a \in A$ tal que $f(a) = b$, pero $f(g(b)) = b$ con $g(b) \in A$. Sea $a = g(b)$.

Recíprocamente, sea f una función biyectiva y sea $b \in B$. Como f es sobre, existe $a \in A$ tal que $f(a) = b$. Como f es 1-1, a es único. Defina g como $g(b) = a$. Hemos construído la inversa de f. □

Relaciones de Equivalencia y Particiones

Una noción fundamental en matemáticas es la de igualdad. Podemos generalizar la igualdad por medio de las relaciones de equivalencia y las clases de equivalencia. Una ***relación de equivalencia*** en un conjunto X es una relación $R \subset X \times X$ tal que

- $(x, x) \in R$ para todo $x \in X$ (***propiedad refleja***);
- $(x, y) \in R$ implica $(y, x) \in R$ (***propiedad simétrica***);
- (x, y) y $(y, z) \in R$ implica $(x, z) \in R$ (***propiedad transitiva***).

Dada una relación de equivalencia R en un conjunto X, usualmente escribiremos $x \sim y$ en lugar de $(x, y) \in R$. Si la relación de equivalencia ya tiene asociada una notación como $=$, $\equiv$, o $\cong$, usaremos esa notación.

Ejemplo 1.21. Sean p, q, r, y s enteros, con q y s distintos de cero. Definimos $p/q \sim r/s$ si $ps = qr$. Claramente $\sim$ es refleja y simétrica. Para mostrar que también es transitiva, supongamos que $p/q \sim r/s$ y $r/s \sim t/u$, con q, s, y u todos distintos de cero. Entonces $ps = qr$ y $ru = st$. Por lo tanto,

$$psu = qru = qst.$$

Como $s \neq 0$, $pu = qt$. Así, $p/q \sim t/u$.

Ejemplo 1.22. Supongamos que f y g son funciones diferenciables en $\mathbb{R}$. Podemos definir una relación de equivalencia en el conjunto de tales funciones definiendo $f(x) \sim g(x)$ si $f'(x) = g'(x)$. Es claro que esta relación es refleja y simétrica. Para demostrar la transitividad, supongamos que $f(x) \sim g(x)$ y $g(x) \sim h(x)$. De cálculo sabemos que $f(x) - g(x) = c_1$ y $g(x) - h(x) = c_2$, donde c_1 y c_2 son ambos constantes. Luego,

$$f(x) - h(x) = (f(x) - g(x)) + (g(x) - h(x)) = c_1 - c_2$$

y $f'(x) - h'(x) = 0$. Por lo tanto, $f(x) \sim h(x)$.

Ejemplo 1.23. Para (x_1, y_1) y (x_2, y_2) en $\mathbb{R}^2$, definamos $(x_1, y_1) \sim (x_2, y_2)$ si $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Entonces $\sim$ es una relación de equivalencia en $\mathbb{R}^2$.

Ejemplo 1.24. Sean A y B matrices de 2×2 con coeficientes reales. Podemos definir una relación de equivalencia en el conjunto de la matrices de 2×2, diciendo que $A \sim B$ si existe una matriz invertible P tal que $PAP^{-1} = B$. Por ejemplo, si

$$A = \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} -18 & 33 \\ -11 & 20 \end{pmatrix},$$

entonces $A \sim B$ pues $PAP^{-1} = B$ para

$$P = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}.$$

Sea I la matriz identidad de 2×2; es decir,

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Entonces $IAI^{-1} = IAI = A$; por lo tanto, la relación es refleja. Para demostrar simetría, supongamos que $A \sim B$. Entonces existe una matriz invertible P tal que $PAP^{-1} = B$. Así

$$A = P^{-1}BP = P^{-1}B(P^{-1})^{-1}.$$

Finalmente, supongamos que $A \sim B$ y $B \sim C$. Entonces existen matrices P y Q tales que $PAP^{-1} = B$ y $QBQ^{-1} = C$. Como

$$C = QBQ^{-1} = QPAP^{-1}Q^{-1} = (QP)A(QP)^{-1},$$

la relación es transitiva. Dos matrices equivalente de esta forma se dicen ***similares***.

Una ***partición*** $\mathcal{P}$ de un conjunto X es una colección de conjuntos no vacíos $X_1, X_2, \ldots$ tales que $X_i \cap X_j = \emptyset$ para $i \neq j$ y $\bigcup_k X_k = X$. Sea $\sim$ una relación de equivalencia en un conjunto X y sea $x \in X$. Entonces $[x] = \{y \in X : y \sim x\}$ se llama ***clase de equivalencia*** de x. Veremos que una relación de equivalencia da lugar a una partición via clases de equivalencia. Además, si tenemos una partición de un conjunto, entonces existe una relación de equivalencia subyacente, como demuestra el teorema siguiente.

Teorema 1.25. *Dada una relación de equivalencia $\sim$ en un conjunto X, las clases de equivalencia de X forman una partición de X. Recíprocamente, si $\mathcal{P} = \{X_i\}$ es una partición de un conjunto X, entonces existe una relación de equivalencia en X con clases de equivalencia X_i.*

DEMOSTRACIÓN. Supongamos que existe una relación de equivalencia $\sim$ en el conjunto X. Para cualquier $x \in X$, la propiedad refleja muestra que $x \in [x]$ de manera que $[x]$ no es vacío. Claramente $X = \bigcup_{x \in X} [x]$. Sean $x, y \in X$. Debemos probar que ya sea $[x] = [y]$ o $[x] \cap [y] = \emptyset$. Supongamos que la intersección de $[x]$ y $[y]$ no es vacía y que $z \in [x] \cap [y]$. Entonces $z \sim x$ y $z \sim y$. Por simetría o por transitividad $x \sim y$; luego, $[x] \subset [y]$. Similarmente, $[y] \subset [x]$ y así $[x] = [y]$. Por lo tanto, dos clases de equivalencia pueden ser disjuntas o exactamente la misma.

Recíprocamente, supongamos que $\mathcal{P} = \{X_i\}$ es una partición de un conjunto X. Definamos que dos elementos son equivalentes si y solo si están en el mismo conjunto de la partición. Claramente, la relación es refleja. Si x está en el mismo conjunto que y, entonces y está en el mismo conjunto que x, así $x \sim y$ implica $y \sim x$. Finalmente, si x está en el mismo conjunto que y e y está en el mismo conjunto que z, entonces x debe estar en el mismo conjunto que z, por lo que tenemos transitividad. □

Corolario 1.26. *Dos clases de equivalencia en una relación de equivalencia ya sea son disjuntas o son iguales.*

Examinemos algunas de las particiones dadas por las clases de equivalencia de los últimos ejemplos.

Ejemplo 1.27. En la relación de equivalencia del Ejemplo 1.21, dos pares de enteros, (p, q) y (r, s), están en la misma clase de equivalencia cuando se reducen a la misma fracción reducida.

Ejemplo 1.28. En la relación de equivalencia en el Ejemplo 1.22, dos funciones $f(x)$ y $g(x)$ están en la misma clase cuando difieren por una constante.

Ejemplo 1.29. Hemos definido una clase de equivalencia en $\mathbb{R}^2$ por $(x_1, y_1) \sim (x_2, y_2)$ si $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Dos pares de números reales están en la misma clase cuando representan puntos en una misma circunferencia centrada en el origen.

Ejemplo 1.30. Sean r y s dos enteros y supongamos que $n \in \mathbb{N}$. Diremos que r es ***congruente*** a s ***módulo*** n, o r es congruente a s mód n, si $r - s$ es divisible por n; es decir, $r - s = nk$ para algún $k \in \mathbb{Z}$. En este caso escribimos $r \equiv s \pmod{n}$. Por example, $41 \equiv 17 \pmod{8}$ pues $41 - 17 = 24$ es divisible por 8. Afirmamos que congruencia módulo n es una relación de equivalencia en $\mathbb{Z}$. Ciertamente cualquier entero r es equivalente a si mismo pues $r - r = 0$ es divisible por n. Mostraremos ahora que la relación es simétrica. Si $r \equiv s \pmod{n}$, entonces $r - s = -(s - r)$ es divisible por n. Así $s - r$ es divisible por n y $s \equiv r \pmod{n}$. Ahora supongamos que $r \equiv s \pmod{n}$ y $s \equiv t \pmod{n}$. Entonces existen enteros k y l tales que $r - s = kn$ y $s - t = ln$. Para mostrar la transitividad, es necesario probar que $r - t$ es divisible por n. Pero,

$$r - t = r - s + s - t = kn + ln = (k + l)n,$$

y así $r - t$ es divisible por n.

Si consideramos la relación de equivalencia estabecida por los enteros módulo 3, entonces

$$\begin{aligned}
[0] &= \{\ldots, -3, 0, 3, 6, \ldots\}, \\
[1] &= \{\ldots, -2, 1, 4, 7, \ldots\}, \\
[2] &= \{\ldots, -1, 2, 5, 8, \ldots\}.
\end{aligned}$$

Note que $[0] \cup [1] \cup [2] = \mathbb{Z}$ y también que los conjuntos son disjuntos. Los conjuntos [0], [1], y [2] forman una partición de los enteros.

Los enteros módulo n son ejemplos importantes en el estudio del álgebra abstracta y serán muy útiles en el estudio de diversas estructuras algebraicas tales como grupos y anillos. En nuestra discusión de los enteros módulo n hemos asumido un resultado conocido como algoritmo de división, que será enunciado y demostrado en el Capítulo 2.

1.3 Ejercicios

1. Supongamos que

$$A = \{x : x \in \mathbb{N} \text{ y } x \text{ es par}\},$$
$$B = \{x : x \in \mathbb{N} \text{ y } x \text{ es primo}\},$$
$$C = \{x : x \in \mathbb{N} \text{ y } x \text{ es un múltiplo de } 5\}.$$

Describa cada uno de ls siguientes conjuntos.

(a) $A \cap B$
(b) $B \cap C$
(c) $A \cup B$
(d) $A \cap (B \cup C)$

2. Si $A = \{a, b, c\}$, $B = \{1, 2, 3\}$, $C = \{x\}$, y $D = \emptyset$, liste todos los elementos en cada uno de los siguientes conjuntos.

(a) $A \times B$
(b) $B \times A$
(c) $A \times B \times C$
(d) $A \times D$

3. Encuentre un ejemplo de dos conjuntos no vacíos A y B para los que $A \times B = B \times A$ es verdadero.

4. Demuestre que $A \cup \emptyset = A$ y $A \cap \emptyset = \emptyset$.

5. Demuestre que $A \cup B = B \cup A$ y $A \cap B = B \cap A$.

6. Demuestre que $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

7. Demuestre que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

8. Demuestre que $A \subset B$ si y solo si $A \cap B = A$.

9. Demuestre que $(A \cap B)' = A' \cup B'$.

10. Demuestre que $A \cup B = (A \cap B) \cup (A \setminus B) \cup (B \setminus A)$.

11. Demuestre que $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

12. Demuestre que $(A \cap B) \setminus B = \emptyset$.

13. Demuestre que $(A \cup B) \setminus B = A \setminus B$.

14. Demuestre que $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

15. Demuestre que $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

16. Demuestre que $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

17. ¿Cuál de las siguientes relaciones $f : \mathbb{Q} \to \mathbb{Q}$ define una función? En cada caso, justifique por qué f es o no es una función.

(a) $f(p/q) = \dfrac{p+1}{p-2}$

(b) $f(p/q) = \dfrac{3p}{3q}$

(c) $f(p/q) = \dfrac{p+q}{q^2}$

(d) $f(p/q) = \dfrac{3p^2}{7q^2} - \dfrac{p}{q}$

18. Determine cuáles de las siguientes funciones son 1-1 y cuáles son sobre. Si la función no es sobre, determine su rango.

(a) $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = e^x$

(b) $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(n) = n^2 + 3$

(c) $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = \sin x$

(d) $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x^2$

19. Sean $f : A \to B$ y $g : B \to C$ funciones invertibles; es decir, funciones tales que f^{-1} y g^{-1} existen. Muestre que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

20.

(a) Defina una función $f : \mathbb{N} \to \mathbb{N}$ que sea 1-1 pero no sobre.

(b) Defina una función $f : \mathbb{N} \to \mathbb{N}$ que sea sobre pero no 1-1.

21. Demuestre que la relación definida en $\mathbb{R}^2$ por $(x_1, y_1) \sim (x_2, y_2)$ si $x_1^2 + y_1^2 = x_2^2 + y_2^2$ es una relación de equivalencia.

22. Sean $f : A \to B$ y $g : B \to C$ funciones.

(a) Si f y g son ambas funciones 1-1, muestre que $g \circ f$ es 1-1.

(b) Si $g \circ f$ es dobre, muestre que g es sobre.

(c) Si $g \circ f$ es 1-1, muestre que f es 1-1.

(d) Si $g \circ f$ es 1-1 y f es sobre, muestre que g es 1-1.

(e) Si $g \circ f$ es sobre y g es 1-1, muestre que f es sobre.

23. Defina una función en los números reales como

$$f(x) = \frac{x+1}{x-1}.$$

¿Cuáles son el dominio y el rango de f? ¿cuál es la inversa de f? Calcule $f \circ f^{-1}$ y $f^{-1} \circ f$.

24. Sea $f : X \to Y$ una función con $A_1, A_2 \subset X$ y $B_1, B_2 \subset Y$.

(a) Demuestre que $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

(b) Demuestre que $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$. Dé un ejemplo en que la igualdad falle.

(c) Demuestre que $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, donde

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

(d) Demuestre que $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

(e) Demuestre que $f^{-1}(Y \setminus B_1) = X \setminus f^{-1}(B_1)$.

25. Determine si las siguientes relaciones son relaciones de equivalencia o no. Si la relación es una relación de equivalencia, describa la partición dada por ella. Si no lo es, indique qué es lo que falla.

(a) $x \sim y$ en $\mathbb{R}$ si $x \geq y$

(b) $m \sim n$ en $\mathbb{Z}$ si $mn > 0$

(c) $x \sim y$ en $\mathbb{R}$ si $|x - y| \leq 4$

(d) $m \sim n$ en $\mathbb{Z}$ si $m \equiv n \pmod 6$

26. Defina una relación $\sim$ en $\mathbb{R}^2$ diciendo que $(a, b) \sim (c, d)$ si y solo si $a^2+b^2 \leq c^2 + d^2$. Muestre que $\sim$ es refleja y transitiva pero no simétrica.

27. Muestre que una matriz de $m \times n$ da lugar a una función bien-definida de $\mathbb{R}^n$ en $\mathbb{R}^m$.

28. Encuentre el error en el siguiente argumento mostrando un contraejemplo. "La propiedad refleja es redundante entre los axiomas para una relación de equivalencia. Si $x \sim y$, entonces $y \sim x$ por la propiedad simétrica. Usando la transitividad, podemos deducir que $x \sim x$."

29. (Recta Real Proyectiva) Defina una relación en $\mathbb{R}^2 \setminus \{(0, 0)\}$ haciendo $(x_1, y_1) \sim (x_2, y_2)$ si existe un número real λ distinto de cero tal que $(x_1, y_1) = (\lambda x_2, \lambda y_2)$. Demuestre que $\sim$ define una relación de equivalencia en $\mathbb{R}^2 \setminus (0, 0)$. ¿Cuáles son las correspondientes clases de equivalencia? Esta relación de equivalencia define la recta proyectiva, denotada por $\mathbb{P}(\mathbb{R})$, que es muy importante en geometría.

1.4 Referencias y Lecturas Recomendadas

[1] Artin, M. *Abstract Algebra.* 2nd ed. Pearson, Upper Saddle River, NJ, 2011.

[2] Childs, L. *A Concrete Introduction to Higher Algebra.* 2nd ed. Springer-Verlag, New York, 1995.

[3] Dummit, D. y Foote, R. *Abstract Algebra.* 3rd ed. Wiley, New York, 2003.

[4] Ehrlich, G. *Fundamental Concepts of Algebra.* PWS-KENT, Boston, 1991.

[5] Fraleigh, J. B. *A First Course in Abstract Algebra.* 7th ed. Pearson, Upper Saddle River, NJ, 2003.

[6] Gallian, J. A. *Contemporary Abstract Algebra.* 7th ed. Brooks/Cole, Belmont, CA, 2009.

[7] Halmos, P. *Naive Set Theory.* Springer, New York, 1991. One of the best references for set theory.

[8] Herstein, I. N. *Abstract Algebra.* 3rd ed. Wiley, New York, 1996.

[9] Hungerford, T. W. *Algebra.* Springer, New York, 1974. One of the standard graduate algebra texts.

[10] Lang, S. *Algebra.* 3rd ed. Springer, New York, 2002. Another standard graduate text.

[11] Lidl, R. y Pilz, G. *Applied Abstract Algebra.* 2nd ed. Springer, New York, 1998.

[12] Mackiw, G. *Applications of Abstract Algebra.* Wiley, New York, 1985.

[13] Nickelson, W. K. *Introduction to Abstract Algebra.* 3rd ed. Wiley, New York, 2006.

[14] Solow, D. *How to Read y Do Proofs.* 5th ed. Wiley, New York, 2009.

[15] van der Waerden, B. L. *A History of Algebra.* Springer-Verlag, New York, 1985. An account of the historical development of algebra.

1.5 Sage

Sage es un sistema poderoso para estudiar y explorar diversas áreas de las matemáticas. En este libro, se estudia una variedad de estructuras algebraicas, tales como grupos, anillos y cuerpos. Sage tiene excelentes implementaciones de muchas propiedades de estos objetos como veremos en lo capítulos que vienen. Pero acá y ahora, en este capítulo inicial, nos concentraremos en unas pocas cosas generales para sacarle el mayor provecho posible a Sage.

Usted puede usar Sage de varias formas diferentes. Lo puede usar como un programa de línea de comando si está instalado en su computador, o a través de una aplicación web como SageMathCloud. Este texto supondrá que lo está leyendo como una hoja de cálculo dentro de un Notebook Sage (una interfaz de navegador web), o que esta es una sección del libro completo presentado como páginas web, y usted está usando el Servidor de Sage Cell Server via esas páginas. Después de los primero capítulos las explicaciones debiesen ser igualmente válidas sin importar cómo esté ejecutando los comandos Sage.

Ejecutando Comandos Sage

Su principal interacción será escribir comandos Sage dentro de una *celda de cálculo*. Si está leyendo esto dentro de un Notebook Sage o en la versión web del libro, entonces encontrará una celda de cálculo justo debajo de este párrafo. Pinche una vez dentro de la celda y si está en un Notebook Sage, obtendrá un borde más dintintivo alrededor, y un cursor parpadeante en el interior, además de un enlace "evaluate" debajo.Escriba `2+2` y pinche en el enlace de evaluación. ¿Apareció un `4` debajo de la celda? Si es así, ha tenido éxito en enviar un comando a Sage para su evaluación y ha recibido la respuesta (correcta).

Acá hay otra celda de cálculo. Intente evaluar el comando `factorial(300)`.Hmmmmm. ¡Ese es un entero grande! El resultado debiese tener 615 dígitos en total. Puede que deba usar la barra de navegación para verlo completo o que aparezca cortado y con diagonales al final de cada línea (éstas indican la continuación en la línea siguiente).

Para hacer nuevas celdas de cálculo en el Notebook Sage (solo ahí), pase con el mouse justo arriba de otra celda de cálculo o justo debajo de una celda de salida. Cuando vea una delgada barra azul, pinche y se abrirá una nueva celda lista para ser usada. Note que su hoja de trabajo recordará todas las operaciones que realice, en el orden en que las realice, sin importar dónde estén las celdas por lo que es mejor mantener el orden y agregar celdas abajo.

Intente situar el cursor justo debajo del enorme número que obtuvo para 300! Pinche en la barra azul (no funciona en la versión web del libro) y haga otro cálculo en la nueva celda de cálculo.

Cada celda de cálculo solo mostrará la salida del último comando en la celda. Intente predecir la salida de la siguiente celda antes de ejecutarla.

```
a = 10
b = 6
b = b - 10
a = a + 20
a
```

```
30
```

La siguiente celda de cálculo no producirá nada visible pues el único comando no produce salida. Pero tendrá un efecto, como puede apreciar cuando ejecute la celda siguiente. Note como se usa el valor de `b` de arriba. Ejecute esta celda *una vez*. Exactamente una vez. Aunque *parezca* no hacer nada. Si la ejecuta dos veces, no nos hacemos responsables de lo que pueda suceder.

```
b = b + 50
```

Ahora ejecute esta celda, la que sí producirá una salida.

```
b + 20
```

```
66
```

Así `b` comenzó su existencia como `6`. A continuación le restamos 10. En una celda posterior le sumamos `50`. Esto suponiendo que ejecutó la celda *exactamente* una vez! En la última celda creamos `b+20` (pero no guardamos el resultado) y es ese valor (66) el que se mostró, mientras `b` aún vale 46.

Puede combinar varios comandos en una línea separándolos por punto y coma (;). Esto se puede usar para obtener múltiples salidas de una solo celda. La sintaxis para construir una matriz debiera ser bastante clara cuando vea el resultado, pero si no lo es, no se preocupe, por ahora no es importante.

```
A = matrix([[3, 1], [5,2]]); A
```

```
[3 1]
[5 2]
```

```
print(A); print; print(A.inverse())
```

```
[3 1]
[5 2]
<BLANKLINE>
[ 2 -1]
[-5  3]
```

Ayuda Inmediata

Algunos comandos en Sage son "funciones," un ejemplo es `factorial()` ariba. Otros comandos son "métodos" de un objeto y son características del objeto, un ejemplo `.inverse()` como un método de una matriz. Una vez que sabe como crear un objeto (como una matriz), entonces es fácil ver todos los métodos disponibles. Escriba el nombre del objeto seguido de un punto y presione la tecla TAB. Esto lamentablemente no parece funcionar en la versión web del libro.

Para obtener ayuda en cómo usar un método con un objeto, escriba su nombre después del punto (sin paéntesis) seguido de un signo de interrogación y presione TAB (o evalúe la celda). (Presione la tecla de escape "ESC" para sacar la lista, o presione en el texto para un método.)

```
A.inverse?
```

Con un segundo signo de interrogación es posible ver las instrucciones programadas en Sage que hacen que el método funcione:

```
A.inverse??
```

Vale la pena ver lo que hace Sage cuando hay un error. Seguramente le tocará ver un buen número de estos, e inicialmente pueden resultar bastante intimidantes. Pero con el tiempo, los podrá entender y usar efectivamente, además de ojalá verlos con menos frecuencia. Ejecute la celda de abajo, pide el inverso de una matriz que no es invertible.

```
B = matrix([[2, 20], [5, 50]])
B.inverse()
```

```
Traceback (most recent call last):
...
ZeroDivisionError: Matrix is singular
```

Si está en una celda de un Notebook Sage, verá una versión abreviada del error. Pinchar a la izquierda de éste aumenta el detalle desplegado y pinchando nuevamente desaparece por completo. Finalmente pinchando una tercera vez se vuelve al mensaje abreviado. Lea la parte final del error primero, esa puede ser la mejor explicación. Acá el error `ZeroDivisionError` no es 100% apropiado, pero se acerca. La matriz no es invertible o equivalentemente su determinante es cero por lo que en algún punto Sage intentó dividir por cero. El resto del mensaje comienza con la parte de su código que dio origen al error, seguida de los comandos y funciones intermedias ejecutadas hasta el punto preciso donde se produjo el problema. A veces esta información le dará algunas pistas, otras veces será completamente indescifrable. No se deje asustar si parece misterioso, pero recuerde que conviene leer la última línea primero, después volver atrás y leer las primeras líneas para buscar algo que se parezca a lo que escribió usted.

Comentando su Trabajo

Es fácil comentar el trabajo cuando está usando un Notebook Sage. (Lo siguiente solo es válido en ese contexto. Puede abrir un Notebook Sage y experimentar allí.) Es posible obtener un pequeño procesador de texto en otra celda entre las celdas de cálculo. Una forma de hacer que aparezca es pinchar en a barra azul mencionada antes, pero presionando simultáneamente la tecla SHIFT. Experimente con tipos de letra, colores, listas, etc y luego presione "Save changes" para guardar y salir. Pinche doble en su texto si necesita volver a editarlo.

Apra el procesador de texto nuevamente para escribir algo. Escriba lo siguiente *exactamente,*

```
Teorema de Pitágoras: $c^2=a^2+b^2$
```

y guarde los cambios. Los símbolos entre los signos pesos se interpretan de acuerdo al lenguaje conocido como TEX o LATEX— puede navegar internet para aprender sobre esta útil herramienta. (Al menos entre matemáticos y físicos es muy popular.)

Listas

Gran parte de nuestra interacción con conjuntos será por medio de listas Sage. Estas no son realmente conjuntos — permiten duplicados, y el orden de los elementos es relevante. Pero se parecen a los conjuntos, y son muy poderosas de manera que las usaremos a menudo. Empezaremos con una lista inventada para practicar, las cremillas significan que los elementos son de texto, sin significado especial. Ejecute estas celdas en la medida que avanzamos.

```
zoo = ['snake', 'parrot', 'elephant', 'baboon', 'beetle']
zoo
```

```
['snake', 'parrot', 'elephant', 'baboon', 'beetle']
```

Los corchetes definen los límites de la lista, comas separan sus elementos, y le podemos asignar un nombre a la lista. Para trabajar con un elemento de la lista, usamos el nombre y un par de corchetes conteniendo un índice. Note que las listas usan índices que *comienzan a enumerar desde cero*. Esto parece extraño al principio, pero se acostumbrará.

```
zoo[2]
```

```
'elephant'
```

Podemos agregar un nuevo animal al zoológico, se sitúa al final.

```
zoo.append('ostrich'); zoo
```

```
['snake', 'parrot', 'elephant', 'baboon', 'beetle', 'ostrich']
```

Podemos sacar a un criatura.

```
zoo.remove('parrot')
zoo
```

```
['snake', 'elephant', 'baboon', 'beetle', 'ostrich']
```

Podemos extraer una sublista. Acá comenzamos con el elemento 1 (elephant) y continuamos hasta, *pero sin incluirlo*, el elemento 3 (beetle). Nuevamente un poco extraño, pero parecerá natural a la larga. Por ahora, note que estamos extrayendo dos elementos de la lista, exactamente $3 - 1 = 2$ elementos.

```
mammals = zoo[1:3]
mammals
```

```
['elephant', 'baboon']
```

Querremos saber si dos listas son iguales, o si los conjuntos que representan lo son. Para lograrlo tendremos que ordenar las listas primero. La función `sorted` crea una nueva lista ordenada, sin alterar la lista original. Guardamos la nueva lista con otro nombre.

```
newzoo = sorted(zoo)
newzoo
```

```
['baboon', 'beetle', 'elephant', 'ostrich', 'snake']
```

```
zoo.sort()
zoo
```

```
['baboon', 'beetle', 'elephant', 'ostrich', 'snake']
```

Note que si ejecuta esta última celda su zoológico habrá cambiado y algunos comandos no necesariamente se ejecutarán de la misma forma. Si quiere experimentar, vuelva a la creación original del zoo y ejecute las celdas nuevamente con un zoo renovado.

Una construcción llamada ***list comprehension*** (no he encontrado una buena traducción) es especialmente poderosa, especialmente dado que imita

casi exactamente la notación que usamos para describir conjuntos. Supongamos que queremos formar los plurales de los nombres de las criaturas en nuestro zoo. Construimos una nueva lista, basada en todos los elementos de nuestra lista anterior.

```
plurality_zoo = [animal+'s' for animal in zoo]
plurality_zoo
```

```
['baboons', 'beetles', 'elephants', 'ostrichs', 'snakes']
```

Casi como dice: agregamos una "s" al nombre de cada animal, para cada animal en el zoo, y los ponemos en una nueva lista. Perfecto. (Excepto que el plural de "ostrich" está mal.)

Listas de Enteros

Un tipo final de lista, con números esta vez. La función `srange()` creará una lista de enteros. (La "s" en el nombre se refiere a "Sage" y producirá enteros óptimos para Sage. Muchas de las dificultades iniciales con Sage y teoría de grupos pueden ser aliviadas con solo usar este comando para crear listas de enteros.) En su formal más simple, `srange(12)` creará una lista de 12 enteros, *empezando de cero* y llegando hasta 11. ¿Suena familiar?

```
dozen = srange(12); dozen
```

```
[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]
```

A continuación dos formas adicionales que entenderá estudiando los ejemplos.

```
teens = srange(13, 20); teens
```

```
[13, 14, 15, 16, 17, 18, 19]
```

```
decades = srange(1900, 2000, 10); decades
```

```
[1900, 1910, 1920, 1930, 1940, 1950, 1960, 1970, 1980, 1990]
```

Guardando y Compartiendo su Trabajo

Hay un botón "Save" en la esquina superior derecha del Notebook Sage. Pinchar en él guardará su trabajo de manera que pueda recuperarlo desde el notebook Sage en una ocasión futura, sin embargo deberá volver a ejecutar todas las celdas cuando reabra su hoja de trabajo.

También hay un menú que se despliega donde dice "File", a la izquierda, justo arriba de la primera celda de cálculo (no lo confunda con el menú de su navegador). Verá una opción acá etiquetada "Save worksheet to a file..." Cuando haga esto, creará una copia de su hoja de trabajo en el formato `sws` (abreviación de "Sage WorkSheet"). Puede enviar este archivo por email, o publicarlo en una página web, para que otros usuarios lo vean y lo suban usando el enlace "Upload" en su propio notebook incorporando una copia de su hoja de trabajo en el notebook de ellos.

Hay otras formas de compartir hojas de trabajo con las que puede experimentar, pero esto le da una manera de compartir con cualquier persona.

Hemos visto bastantes cosas en esta sección, así es que vuelva más adelante a repasar y descubrir detalles que no haya notado. Hay muchas otras características del Notebok Sage que no hemos cubierto acá.

1.6 Ejercicios en Sage

1. Este ejercicio es solo para asegurarnos de que sabe cómo usar Sage. Puede que esté usando un Notebook Sage en su propio computador o en el servidor online CoCalc a través de su navegador. En cualquier caso, comience una nueva hoja de trabajo. Haga algún cálculo no trivial, un gráfico o algún cálculo numérico con enorme precisión o con números gigantes. Construya una lista interesante y experimente con ella. Podría incluir algo de texto diagramado o usando TEX en el mini procesador de textos incluido en el Notebook Sage o agregue un comentario en celdas dentro de CoCalc usando ***magics*** `%html` o `%md` en una línea propia seguido de texto con sintaxis HTML o Markdown (respectivamente).
Use el mecanismo que su profesor le haya indicado para entregar su trabajo. O guarde su hoja de trabajo y compártala con un compañero.

2

Los Enteros

El conjunto de los números enteros es un componente básico de las matemáticas. En este capítulo investigaremos las propiedades fundamentales de los enteros, incluyendo el principio de inducción matemática, el algoritmo de división, y el Teorema Fundamental de la Aritmética.

2.1 Principio de Inducción

Supongamos que queremos demostrar que

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

para cualquier número natural n. Esta fórmula se puede verificar fácilmente para números pequeños tales como $n = 1$, 2, 3, o 4, pero es imposible de verificar para todos los número naturales uno por uno. Para demostrar que la fórmula es verdadera en general, se requiere un método más genérico.

Supongamos que hemos verificado la ecuación para los primeros n casos. Intentaremos demostrar que podemos generar una fórmula para el caso $(n+1)$ a partir de este conocimiento. La fórmula es verdadera para $n = 1$ pues

$$1 = \frac{1(1+1)}{2}.$$

Si hemos verificado los primeros n casos, entonces

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n^2 + 3n + 2}{2} \\ &= \frac{(n+1)[(n+1)+1]}{2}. \end{aligned}$$

Esto corresponde exactamente a la fórmula para el caso $(n+1)$.

Este método de demostración se conoce como ***inducción matemática*** o simplemente ***inducción*** si no hay riesgo de confusión. En lugar de intentar verificar una proposición sobre un subconjunto S de los enteros positivos $\mathbb{N}$ uno por uno, una tarea imposible si S es un conjunto infinito, entregamos una demostración directa para el primer entero considerado, seguida de un argumento genérico mostrando que si la proposición se cumple en un cierto caso, entonces también se cumple para el siguiente caso en la sucesión. Resumimos la inducción matemática en el siguiente axioma.

Principio 2.1 (Primer Principio de Inducción)**.** *Sea $S(n)$ una proposición sobre números enteros para $n \in \mathbb{N}$ y supongamos que $S(n_0)$ es verdadera para algún entero n_0. Si para todos los enteros k con $k \geq n_0$, $S(k)$ implica $S(k+1)$, es verdadera, entonces $S(n)$ es verdadera para todos los enteros n mayores o iguales a n_0.*

Ejemplo 2.2. Para todos los enteros $n \geq 3$, $2^n > n + 4$. Como

$$8 = 2^3 > 3 + 4 = 7,$$

la afirmación es verdadera para $n_0 = 3$. Supongamos que $2^k > k + 4$ para $k \geq 3$. Entonces $2^{k+1} = 2 \cdot 2^k > 2(k + 4)$. Pero

$$2(k + 4) = 2k + 8 > k + 5 = (k + 1) + 4$$

pues k es positivo. Luego, por inducción, la afirmación se cumple para todos los enteros $n \geq 3$.

Ejemplo 2.3. El entero $10^{n+1} + 3 \cdot 10^n + 5$ es divisible por 9 para todo $n \in \mathbb{N}$. Para $n = 1$,

$$10^{1+1} + 3 \cdot 10 + 5 = 135 = 9 \cdot 15$$

es divisible por 9. Supongamos que $10^{k+1} + 3 \cdot 10^k + 5$ es divisible por 9 para $k \geq 1$. Entonces

$$\begin{aligned} 10^{(k+1)+1} + 3 \cdot 10^{k+1} + 5 &= 10^{k+2} + 3 \cdot 10^{k+1} + 50 - 45 \\ &= 10(10^{k+1} + 3 \cdot 10^k + 5) - 45 \end{aligned}$$

es divisible por 9.

Ejemplo 2.4. Demostraremos el teorema del binomio por inducción; es decir,

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k},$$

donde a and b son números reales, $n \in \mathbb{N}$, y

$$\binom{n}{k} = \frac{n!}{k!(n - k)!}$$

es el coeficiente binomial. Primero mostraremos que

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Este resultado es consecuencia de

$$\begin{aligned} \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{(n+1)!}{k!(n+1-k)!} \\ &= \binom{n+1}{k}. \end{aligned}$$

Si $n = 1$, el teorema del binomio es fácil de verificar. Ahora supongamos que el resultado es verdadero para n mayor o igual a 1. Entonces

$$(a + b)^{n+1} = (a + b)(a + b)^n$$

$$
\begin{aligned}
&= (a+b)\left(\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}\right)\\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k}\\
&= a^{n+1} + \sum_{k=1}^{n}\binom{n}{k-1}a^k b^{n+1-k} + \sum_{k=1}^{n}\binom{n}{k}a^k b^{n+1-k} + b^{n+1}\\
&= a^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k-1} + \binom{n}{k}\right]a^k b^{n+1-k} + b^{n+1}\\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}.
\end{aligned}
$$

Tenemos una proposición equivalente al Primer Principio de Inducción que en ocasiones será necesaria.

Principio 2.5 (Segundo Principio de Inducción)**.** *Sea $S(n)$ una afirmación sobre enteros para $n \in \mathbb{N}$ y supongamos que $S(n_0)$ es verdadera para algún entero n_0. Si $S(n_0), S(n_0+1), \ldots, S(k)$ implican $S(k+1)$ para $k \geq n_0$, entonces $S(n)$ es verdadera para todos los enteros $n \geq n_0$.*

Un subconjunto S de $\mathbb{Z}$ está ***bien-ordenado*** si todo subconjunto no vacío de S contiene un menor elemento. Note que el conjunto $\mathbb{Z}$ no está bien-ordenado pues no contiene un elemento mínimo. Los números naturales sin ambargo, sí están bien-ordenados.

Principio 2.6 (Principio del Buen-Orden)**.** *El conjunto de los números naturales está bien-ordenado.*

El Principio del Buen-Orden es equivalente al Principio de Inducción.

Lema 2.7. *El principio de Inducción implica que* 1 *es el menor número natural positivo.*

Demostración. Sea $S = \{n \in \mathbb{N} : n \geq 1\}$. Entonces $1 \in S$. Supongamos que $n \in S$. Como $0 < 1$, se debe tener que $n = n + 0 < n + 1$. Por lo tanto, $1 \leq n < n + 1$. Así, si $n \in S$, entonces $n + 1$ también debe estar en S, y por el Principio de Inducción, $S = \mathbb{N}$. □

Teorema 2.8. *El Principio de Inducción implica el Principio del Buen-Orden. Es decir, todo subconjunto no vacío de $\mathbb{N}$ contiene un menor elemento.*

Demostración. Debemos mostrar que si S es un subconjunto no vacío de los números naturales, entonces S contiene un elemento mínimo. Si S contiene a 1, el teorema es verdadero por el Lema 2.7. Supongamos que si S contiene un entero k tal que $1 \leq k \leq n$, entonces S contiene un elemento mínimo. Mostraremos que si un conjunto S contiene un entero menor o igual a $n + 1$, entonces S tiene un elemento mínimo. Si S no contiene un elemento menor a $n+1$, entonces $n+1$ es el menor entero en S. De lo contrario, S debe contener un entero menor o igual a n. En ese caso, por la hipótesis de inducción, S contiene un elemento mínimo. □

La Inducción puede ser muy útil en la formulación de definiciones. Por ejemplo, hay dos formas de definir $n!$, el factorial de un entero positivo n.

- La definición *explícita*: $n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$.

- La definición *inductiva* o *recursiva*: $1! = 1$ y $n! = n(n-1)!$ para $n > 1$.

Mirar un problema de forma recursiva, en lugar de explícita, frecuentemente resulta en una mejor comprensión de situaciones complejas.

2.2 El Algoritmo de División

Una aplicación del Principio del Buen-Orden que usaremos frecuentemente es el algoritmo de división.

Teorema 2.9 (Algoritmo de División)**.** *Sean a y b números enteros, con $b > 0$. Entonces existen enteros únicos q y r tales que*

$$a = bq + r$$

donde $0 \leq r < b$.

Demostración. Este es un ejemplo perfecto de una demostración de existencia y unicidad. Debemos primero demostrar que los números q y r realmente existen. Después debemos mostrar que si q' y r' también son tales números, entonces $q = q'$ y $r = r'$.

Existencia de q y r. Sea

$$S = \{a - bk : k \in \mathbb{Z} \text{ y } a - bk \geq 0\}.$$

Si $0 \in S$, entonces b divide a a, y podemos tomar $q = a/b$ y $r = 0$. Si $0 \notin S$, podemos usar el Principio del Buen-Orden. Debemos primero mostrar que S es no vacío. Si $a > 0$, entonces $a - b \cdot 0 \in S$. Si $a < 0$, entonces $a - b(2a) = a(1 - 2b) \in S$. En cualquier caso $S \neq \emptyset$. Po el Principio del Buen-Orden, S tiene un elemento mínimo, digamos $r = a - bq$. Por lo tanto, $a = bq + r$, $r \geq 0$. Mostremos ahora que $r < b$. Supongamos que $r > b$. Entonces

$$a - b(q + 1) = a - bq - b = r - b > 0.$$

En este caso tendríamos $a - b(q+1)$ en el conjunto S. Pero entonces $a - b(q+1) < a - bq$, lo que llevaría a una contradicción del hecho que $r = a - bq$ es el menor elemento de S. Así $r \leq b$. Como $0 \notin S$, $r \neq b$ y así $r < b$.

Unicidad de q y r. Supongamos que existen enteros r, r', q, y q' tales que

$$a = bq + r, 0 \leq r < b \quad \text{and} \quad a = bq' + r', 0 \leq r' < b.$$

Entonces $bq + r = bq' + r'$. Supongamos que $r' \geq r$. De la última ecuación tenemos $b(q - q') = r' - r$; por lo tanto, b debe dividir a $r' - r$ y $0 \leq r' - r \leq r' < b$. Estos es posible solo si $r' - r = 0$. Luego, $r = r'$ y $q = q'$. □

Sean a y b enteros. Si $b = ak$ para algún entero k, escribiremos $a \mid b$. Un entero d se llama ***divisor común*** de a y b si $d \mid a$ y $d \mid b$. El ***máximo común divisor*** de los enteros a y b es un entero positivo d tal que d es un divisor común de a y b y si d' es cualquier otro divisor común de a y b, entonces $d' \mid d$. Escribiremos $d = \text{mcd}(a, b)$; por ejemplo, $\text{mcd}(24, 36) = 12$ y $\text{mcd}(120, 102) = 6$. Decimos que dos enteros a y b son ***relativamente primos*** si $\text{mcd}(a, b) = 1$.

Teorema 2.10. *Sean a y b enteros distintos de cero. Entonces existen enteros r y s tales que*

$$\text{mcd}(a, b) = ar + bs.$$

Más aún, el máximo común divisor de a y b es único.

DEMOSTRACIÓN. Sea

$$S = \{am + bn : m, n \in \mathbb{Z} \text{ and } am + bn > 0\}.$$

Claramente, el conjunto S es no-vacío; luego, por el Principio del Buen-Orden S tiene un elemento mínimo, digamos $d = ar + bs$. Afirmamos que $d = \text{mcd}(a, b)$. Escriba $a = dq + r'$ con $0 \leq r' < d$. Si $r' > 0$, entonces

$$\begin{aligned} r' &= a - dq \\ &= a - (ar + bs)q \\ &= a - arq - bsq \\ &= a(1 - rq) + b(-sq), \end{aligned}$$

que está en S. Pero esto estaría en contradicción con el hecho de que d es el menor miembro de S. Luego, $r' = 0$ y d divide a a. Un argumento similar muestra que d divide a b. Por lo tanto, d es un divisor común de a y b.

Supongamos que d' es otro divisor común de a y b, y queremos mostrar que $d' \mid d$. Si $a = d'h$ y $b = d'k$, entonces

$$d = ar + bs = d'hr + d'ks = d'(hr + ks).$$

Es decir d' divide a d. Luego, d es el único máximo común divisor de a y b. □

Corolario 2.11. *Sean a y b enteros relativamente primos. Entonces existen enteros r y s tales que $ar + bs = 1$.*

El Algoritmo de Euclides

Entre otras cosas, el Teorema 2.10 nos permite calcular el máximo común divisor de dos enteros.

Ejemplo 2.12. Calculemos el máximo común divisor de 945 y 2415. Primero observemos que

$$\begin{aligned} 2415 &= 945 \cdot 2 + 525 \\ 945 &= 525 \cdot 1 + 420 \\ 525 &= 420 \cdot 1 + 105 \\ 420 &= 105 \cdot 4 + 0. \end{aligned}$$

Usando los pasos de atrás para adelante, 105 divide a 420, 105 divide a 525, 105 divide a 945, y 105 divide a 2415. Luego, 105 divide tanto a 945 como a 2415. Si d fuese otro divisor común de 945 y 2415, entonces d también dividiría a 105. Por lo tanto, $\text{mcd}(945, 2415) = 105$.

Volviendo a recorrer las ecuaciones anteriores de abajo para arriba, podemos obtener números enteros r y s tales que $945r + 2415s = 105$. Note que

$$\begin{aligned} 105 &= 525 + (-1) \cdot 420 \\ &= 525 + (-1) \cdot [945 + (-1) \cdot 525] \\ &= 2 \cdot 525 + (-1) \cdot 945 \\ &= 2 \cdot [2415 + (-2) \cdot 945] + (-1) \cdot 945 \\ &= 2 \cdot 2415 + (-5) \cdot 945. \end{aligned}$$

Así $r = -5$ y $s = 2$. Note que r y s no son únicos, pues por ejemplo $r = 41$ y $s = -16$ también funcionarían.

Para calcular $\text{mcd}(a,b) = d$, estamos usando sucesivas divisiones para obtener una sucesión decreciente de enteros positivos $r_1 > r_2 > \cdots > r_n = d$; es decir,

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n+1}. \end{aligned}$$

Para encontrar r y s tales que $ar + bs = d$, empezamos con la última ecuación y sustituímos los resultados obtenidos de las ecuaciones anteriores:

$$\begin{aligned} d &= r_n \\ &= r_{n-2} - r_{n-1}q_n \\ &= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\ &= -q_nr_{n-3} + (1 + q_nq_{n-1})r_{n-2} \\ &\vdots \\ &= ra + sb. \end{aligned}$$

El algoritmo que acabamos de usar para encontrar el máximo común divisor d de dos enteros a y b y escribir d como combinación lineal de a y b se conoce como el ***algoritmo de Euclides***.

Números Primos

Sea p un entero tal que $p > 1$. Decimos que p es un ***número primo***, o simplemente p es ***primo***, si y solo si los únicos números enteros positivos que dividen a p son 1 y el mismo p. Un entero $n > 1$ que no es primo se llama ***compuesto***.

Lema 2.13 (Euclides)**.** *Sean a y b enteros y p un número primo. Si $p \mid ab$, entonces ya sea $p \mid a$ o $p \mid b$.*

Demostración. Supongamos que p no divide a a. Debemos mostrar que $p \mid b$. Como $\text{mcd}(a,p) = 1$, existen enteros r y s tales que $ar + ps = 1$. Así

$$b = b(ar + ps) = (ab)r + p(bs).$$

Como p divide tanto a ab como a si mismo, p divide a $b = (ab)r + p(bs)$. □

Teorema 2.14 (Euclides)**.** *Existe una cantidad infinita de números primos.*

Demostración. Demostraremos este teorema por contradicción. Supongamos que existe solo una cantidad finita de primos, digamos $p_1, p_2, \ldots, p_n$. Sea $P = p_1p_2 \cdots p_n + 1$. Entonces P debe ser divisible por algún p_i con $1 \leq i \leq n$. En este caso, p_i debe dividir a $P - p_1p_2 \cdots p_n = 1$, lo que es una contradicción. Luego, ya sea P es primo o existe un primo adicional $p \neq p_i$ que divide a P. □

Teorema 2.15 (Teorema Fundamental de la Aritmética)**.** *Sea n un entero tal que $n > 1$. Entonces*

$$n = p_1p_2 \cdots p_k,$$

con $p_1, \ldots, p_k$ primos (no necesariamente distintos). Más aún, esta factorización es única; es decir, si

$$n = q_1 q_2 \cdots q_l,$$

entonces $k = l$ y los q_i son iguales a los p_i posiblemente en otro orden.

DEMOSTRACIÓN. *Unicidad.* Para demostrar la unicidad procederemos por inducción en n. El teorema es claramente verdadero para $n = 2$ pues en este caso n es primo. Ahora supongamos que el resultado se cumple para todos los enteros m tales que $1 \leq m < n$, y

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l,$$

con $p_1 \leq p_2 \leq \cdots \leq p_k$ y $q_1 \leq q_2 \leq \cdots \leq q_l$. Por el Lema 2.13, $p_1 \mid q_i$ para ciertos $i = 1, \ldots, l$ y $q_1 \mid p_j$ para ciertos $j = 1, \ldots, k$. Como todos los p_i y los q_i son primos, $p_1 = q_i$ y $q_1 = p_j$. Luego, $p_1 = q_1$ pues $p_1 \leq p_j = q_1 \leq q_i = p_1$. Por la hipótesis de inducción,

$$n' = p_2 \cdots p_k = q_2 \cdots q_l$$

tiene una factorización única. Luego, $k = l$ y $q_i = p_i$ para $i = 1, \ldots, k$.

Existencia. Para demostrar la existencia, supongamos que existe algún entero que no puede ser escrito como producto de primos. Sea S el conjunto de tales números. Por el Principio del Buen-Orden, S contiene un elemento mínimo, digamos a. Si los únicos factores positivos de a son a y 1, entonces a es primo, lo que es una contradicción. Luego, $a = a_1 a_2$ con $1 < a_1 < a$ y $1 < a_2 < a$. Ni $a_1 \in S$ ni $a_2 \in S$, pues a es el menor elemento de S. Así

$$a_1 = p_1 \cdots p_r$$
$$a_2 = q_1 \cdots q_s.$$

Por lo tanto,

$$a = a_1 a_2 = p_1 \cdots p_r q_1 \cdots q_s.$$

Así $a \notin S$, lo que es una contradicción. □

Nota Histórica

Los números primos ya fueron estudiados por los antiguos Griegos. Dos resultados importantes de la Antigüedad son la demostración de Euclides de que existe una infinidad de primos y la criba de Ertóstenes, un método para calcular todos los números primos menores a un entero positivo dado. Un problema en teoría de números es encontrar una función f tal que $f(n)$ es primo para cada entero n. Pierre Fermat (1601?–1665) conjeturó que $2^{2^n} + 1$ era primo para todo n, pero posteriormente Leonhard Euler (1707–1783) demostró que

$$2^{2^5} + 1 = 4{,}294{,}967{,}297$$

es un número compuesto. Una de las muchas conjeturas no demostradas sobre números primos es la conjetura de Goldbach. En una carta a Euler en 1742, Christian Goldbach enunció la conjetura que todo entero positivo con la excepción de 2 parecía ser suma de dos primos: $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, ... Si bien la conjetura ha sido verificada para todos los números hasta 4×10^{18}, aún no ha sido demostrada en general. Como los números primos tienen un rol importante en la criptografía de llave pública, hay actualmente gran interés en determinar si un número grande es primo o no.

Sage El objetivo inicial de Sage fue de apoyar la investigación en teoría de números, de manera que funciona muy bien para los tipos de cálculos con enteros que tenemos en este capítulo.

2.3 Ejercicios

1. Demuestre que

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

para $n \in \mathbb{N}$.

2. Demuestre que

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

para $n \in \mathbb{N}$.

3. Demuestre que $n! > 2^n$ para $n \geq 4$.

4. Demuestre que

$$x + 4x + 7x + \cdots + (3n-2)x = \frac{n(3n-1)x}{2}$$

para todo $n \in \mathbb{N}$.

5. Demuestre que $10^{n+1} + 10^n + 1$ es divisible por 3 para todo $n \in \mathbb{N}$.

6. Demuestre que $4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5$ es divisible por 99 para todo $n \in \mathbb{N}$.

7. Muestre que

$$\sqrt[n]{a_1 a_2 \cdots a_n} \leq \frac{1}{n} \sum_{k=1}^{n} a_k.$$

8. Demuestre la regla de Leibniz para $f^{(n)}(x)$, donde $f^{(n)}$ es la n-ésima derivada de f; es decir, muestre que

$$(fg)^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x).$$

9. Use inducción para demostrar que $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ para todo $n \in \mathbb{N}$.

10. Demuestre que

$$\frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

para todo $n \in \mathbb{N}$.

11. Si x es un número real no negativo, demuestre que $(1+x)^n - 1 \geq nx$ para $n = 0, 1, 2, \ldots$.

12. (Conjunto Potencia) Sea X un conjunto. Defina el ***conjunto potencia*** de X, denotado $\mathcal{P}(X)$, como el conjunto de todos los subconjuntos de X. Por ejemplo,

$$\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

Para todo entero positivo n, muestre que un conjunto con exactamente n elementos tiene un conjunto potencia con exactamente 2^n elementos.

13. Demuestre que que los dos Principios de Inducción enunciados en la Sección2.1 son equivalentes.

14. Muestre que el Principio del Buen-Orden para los números naturales implica que 1 es el menor número natural. Use este resultado para mostrar que el Principio del Buen-Orden implica el Principio de Inducción; es decir, muestre que si $S \subset \mathbb{N}$ tal que $1 \in S$ y $n+1 \in S$ cada vez que $n \in S$, entonces $S = \mathbb{N}$.

15. Para cada uno de los siguientes pares de números a y b, calcule $\text{mcd}(a, b)$ y encuentre enteros r y s tales que $\text{mcd}(a, b) = ra + sb$.

(a) 14 y 39
(b) 234 y 165
(c) 1739 y 9923
(d) 471 y 562
(e) 23771 y 19945
(f) -4357 y 3754

16. Sean a y b enteros distintos de cero. Si existen enteros r y s tales que $ar + bs = 1$, muestre que a y b son relativamente primos.

17. (Números de Fibonacci) Los Números de Fibonacci son

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots.$$

Podemos definirlos recursivamente como $f_1 = 1$, $f_2 = 1$, y $f_{n+2} = f_{n+1} + f_n$ para $n \in \mathbb{N}$.

(a) Demuestre que $f_n < 2^n$.
(b) Demuestre que $f_{n+1}f_{n-1} = f_n^2 + (-1)^n$, $n \geq 2$.
(c) Demuestre que $f_n = [(1+\sqrt{5}\,)^n - (1-\sqrt{5}\,)^n]/2^n\sqrt{5}$.
(d) Muestre que $\lim_{n\to\infty} f_n/f_{n+1} = (\sqrt{5}-1)/2$.
(e) Demuestre que f_n y f_{n+1} son relativamente primos.

18. Sean a y b enteros tales que $\text{mcd}(a, b) = 1$. Sean r y s enteros tales que $ar + bs = 1$. Demuestre que

$$\text{mcd}(a, s) = \text{mcd}(r, b) = \text{mcd}(r, s) = 1.$$

19. Sean $x, y \in \mathbb{N}$ relativamente primos. Si xy es un cuadrado perfecto, demuestre que x e y son ambos cuadrados perfectos.

20. Usando el algoritmo de división, muestre que todo cuadrado perfecto es de la forma $4k$ o $4k+1$ para algún entero no negativo k.

21. Supongamos que a, b, r, s son relativamente primos de a pares y que

$$a^2 + b^2 = r^2$$
$$a^2 - b^2 = s^2.$$

Demuestre que a, r, y s son impares y que b es par.

22. Sea $n \in \mathbb{N}$. Use el algoritmo de división para demostrar que todo entero es congruente mód n a exactamente uno de los enteros $0, 1, \ldots, n-1$. Concluya que si r es un entero, entonces hay exactamente un s en $\mathbb{Z}$ tal que $0 \leq s < n$ y $[r] = [s]$. Luego, los enteros están efectivamente particionados por la relación de congruencia mód n.

23. Defina el ***mínimo común múltiplo*** de dos enteros distintos de cero a y b, denotado por $\text{mcm}(a, b)$, como el entero positivo m tal que tanto a como b dividen a m, y si a y b dividen a otro entero n, entonces m también divide a n. Demuestre que existe un único mínimo común múltiplo para cualquiera dos enteros a y b distintos de cero.

24. Si $d = \text{mcd}(a, b)$ y $m = \text{mcm}(a, b)$, demuestre que $dm = |ab|$.

25. Muestre que $\text{mcm}(a, b) = ab$ si y solo si $\text{mcd}(a, b) = 1$.

26. Demuestre que $\text{mcd}(a, c) = \text{mcd}(b, c) = 1$ si y solo si $\text{mcd}(ab, c) = 1$ para todos los enteros a, b, y c.

27. Sean $a, b, c \in \mathbb{Z}$. Demuestre que si $\text{mcd}(a, b) = 1$ y $a \mid bc$, entonces $a \mid c$.

28. Sea $p \geq 2$. Demuestre que si $2^p - 1$ es primo, entonces p también es primo.

29. Demuestre que hay infinitos primos de la forma $6n + 5$.

30. Demuestre que hay infinitos primos de la forma $4n - 1$.

31. Usando el hecho que 2 es primo, muestre que no existen enteros p y q tales que $p^2 = 2q^2$. Demuestre que por lo tanto $\sqrt{2}$ no puede ser un número racional.

2.4 Ejercicios de Programación

1. (La Criba de Eratóstenes) Un método para calcular todos los números primos menores a un cierto entero positivo dado N es listar todos los números n tales que $1 < n < N$. Comience eleminando todos los múltiplos de 2. Después elimine todos los múltiplos de 3. Ahora elimine todos los múltiplos de 5. Note que 4 ya ha sido eliminado. Continúe de esta manera, notando que no es necesario llegar hasta N; es suficiente con parar en $\sqrt{N}$. Usando este método, calcule todos los números primos menores a $N = 250$. También podemos usar este método para encontrar todos los enteros que son relativamente primos a un entero N. Simplemente elimine los factores primos de N y todos sus múltiplos. Usando este método, encuentre todos los números que son relativamente primos con $N = 120$. Usando la Criba de Eratóstenes, escriba un programa que calcule todos los primos menores que un entero N.

2. Sea $\mathbb{N}^0 = \mathbb{N} \cup \{0\}$. La función de Ackermann es la función $A : \mathbb{N}^0 \times \mathbb{N}^0 \to \mathbb{N}^0$ definida por las ecuaciones

$$\begin{aligned} A(0, y) &= y + 1, \\ A(x + 1, 0) &= A(x, 1), \\ A(x + 1, y + 1) &= A(x, A(x + 1, y)). \end{aligned}$$

Use esta definición para calcular $A(3, 1)$. Escriba un programa para evaluar la función de Ackermann. Modifique el programa para que cuente el número de comandos ejecutados en el programa cuando se evalúa la función de Ackermann. ¿Cuántos comandos se ejecutan en la evaluación de $A(4, 1)$? ¿$A(5, 1)$?

3. Escriba un programa que implemente el algoritmo de Euclides. El programa debiese aceptar dos enteros positivos a y b como entrada y la salida debiese ser tanto $\text{mcd}(a, b)$ como enteros r y s tales que

$$\text{mcd}(a, b) = ra + sb.$$

2.5 Referencias y Lecturas Recomendadas

[1] Brookshear, J. G. *Theory of Computation: Formal Languages, Automata, and Complexity*. Benjamin/Cummings, Redwood City, CA, 1989. Shows the relationships of the theoretical aspects of computer science to set theory and the integers.

[2] Hardy, G. H. and Wright, E. M. *An Introduction to the Theory of Numbers*. 6th ed. Oxford University Press, New York, 2008.

[3] Niven, I. and Zuckerman, H. S. *An Introduction to the Theory of Numbers*. 5th ed. Wiley, New York, 1991.

[4] Vanden Eynden, C. *Elementary Number Theory*. 2nd ed. Waveland Press, Long Grove IL, 2001.

2.6 Sage

Muchas de las propiedades de los objetos algebraicos que estudiaremos se pueden determinar a partir de propiedades de los enteros asociados. Sage tiene muchas y poderosas funciones para trabajar con enteros.

Algoritmo de División

La instrucción `a % b` entregará el resto de la división de a entre b. En otras palabras, el resultado es el entero r (único) tal que (1) $0 \leq r < b$, y (2) $a = bq+r$ para algún entero q (el cociente), como está garantizado por el Algoritmo de la División (Teorema 2.9). Entonces $(a - r)/b$ será igual a q. Por ejemplo,

```
r = 14 % 3
r
```

```
2
```

```
q = (14 - r)/3
q
```

```
4
```

También es posible obtener el cociente y el resto de forma simultánea con el método `.quo_rem()` (cociente y resto).

```
a = 14
b = 3
a.quo_rem(b)
```

```
(4, 2)
```

Un resto cero indica divisibilidad. Así `(a % b)== 0` resulta `True` (verdadero) si b divide a a, y de otro modo resultará `False` (falso).

```
(20 % 5) == 0
```

```
True
```

```
(17 % 4) == 0
```

```
False
```

El método `.divides()` es otra opción.

```
c = 5
c.divides(20)
```

```
True
```

```
d = 4
d.divides(17)
```

```
False
```

Máximo Común Divisor

El máximo común divisor de a y b se obtiene con el comando `gcd(a, b)`, donde por ahora, a y b son enteros. Más tarde, a y b podrán ser otros objetos con una noción de divisibilidad y "tamaño," tales como los polinomios. Por ejemplo,

```
gcd(2776, 2452)
```

```
4
```

Podemos usar el comando `gcd` para determinar si un par de enteros son relativamente primos.

```
a = 31049
b = 2105
gcd(a, b) == 1
```

```
True
```

```
a = 3563
b = 2947
gcd(a, b) == 1
```

```
False
```

El comando `xgcd(a,b)` ("eXtended GCD") entrega un trío donde el primer elemento es el máximo común divisor de a y b (como con el comando `gcd(a,b)`), y los siguientes dos elementos son valores de r y s tales que $ra + sb = \text{mcd}(a, b)$.

```
xgcd(633,331)
```

```
(1, -137, 262)
```

Partes del trío pueden ser extraídas usando `[ ]` ("indexando") para acceder a los elementos del trío, empezando con el primero como índice `0`. Por ejemplo, Lo siguiente siempre debiese resultar en `True`, aunque usted cambie los valores de `a` y `b`. Intente cambiando los valores de `a` y `b` abajo, para ver que el resultado siempre es `True`.

```
a = 633
b = 331
extended = xgcd(a, b)
g = extended[0]
r = extended[1]
s = extended[2]
g == r*a + s*b
```

```
True
```

Estudiar este bloque de código le permitirá descubrir formas de beneficiarse de las respuestas entregadas por Sage. Note que = es la forma de *asignar* un valor a una variable, mientras que en la última línea, == es la forma de comparar si dos objetos son *iguales*.

Primos y Factorización

El método `.is_prime()` determinará si un entero es primo o no.

```
a = 117371
a.is_prime()
```

```
True
```

```
b = 14547073
b.is_prime()
```

```
False
```

```
b == 1597 * 9109
```

```
True
```

El comando `random_prime(a, proof=True)` generará un número primo aleatorio entre 2 y a. Experimente ejecutando las celdas siguientes varias veces. (Reemplazando `proof=True` por `proof=False` acelerará la búsqueda, pero existirá una pequeñísima probabilidad de que el resultado no sea primo.)

```
a = random_prime(10^21, proof=True)
a
```

```
424729101793542195193
```

```
a.is_prime()
```

```
True
```

El comando `prime_range(a, b)` entrega una lista ordenada de todos los primos entre a y $b-1$, incluyendo posiblemente los extremos. Por ejemplo,

```
prime_range(503, 550)
```

```
[503, 509, 521, 523, 541, 547]
```

Los comandos `next_prime(a)` y `previous_prime(a)` son otras formas de obtener un primo de un tamaño deseado. Experimente en la celda siguiente (si la hay). (El símbolo `#`, se usa para indicar un "comentario", que no será evaluado por Sage. Puede borrar esta línea o empezar en la línea siguiente.)Además de verificar si un entero es primo, o generar números primos, Sage también puede descomponer un número entero en sus factores primos, como se decribe en el Teorema Fundamental de la Aritmética (Teorema 2.15).

```
a = 2600
a.factor()
```

```
2^3 * 5^2 * 13
```

Así $2600 = 2^3 \times 5^2 \times 13$ y esta es la única forma de escribir 2600 como producto de números primos (aparte de reordenar los primos en el producto).

Si bien Sage muestra la factorización de una forma que entendemos fácilmente, internamente la guarda como una lista de pares de enteros, consistiendo cada par de una base (un primo) y un exponente (entero positivo). Analice detalladamente los siguientes comandos, pues es un buen ejemplo para entender los resultados de Sage en forma de listas.

```
a = 2600
factored = a.factor()
first_term = factored[0]
first_term
```

```
(2, 3)
```

```
second_term = factored[1]
second_term
```

```
(5, 2)
```

```
third_term = factored[2]
third_term
```

```
(13, 1)
```

```
first_prime = first_term[0]
first_prime
```

```
2
```

```
first_exponent = first_term[1]
first_exponent
```

```
3
```

La siguiente celda revela la estructura interna de la factorización pidiendo la lista como tal. y mostramos como puede determinar el número de términos en la factorización usando el comando `len()` (largo).

```
list(factored)
```

```
[(2, 3), (5, 2), (13, 1)]
```

```
len(factored)
```

```
3
```

¿Puede extraer de `a` los siguientes dos primos y sus exponentes?

2.7 Ejercicios en Sage

Estos ejercicios se tratan de investigar propiedades básicas de los enteros, algo que frecuentemente haremos al investigar grupos. Las hojas de trabajo de Sage tienen extensas capacidades para hacer celdas con texto cuidadosamente formateado, incluyendo la posibilidad de usar comandos LaTeX para expresar matemáticas. Así si una pregunta pide explicaciones o comentarios, haga una nueva celda y comuníquese claramente con su audiencia.

1. Use el comando `next_prime()` para construir dos primos diferentes de 8 dígitos cada uno y guárdelos en variables llamadas `a` y `b`.

2. Use el método `.is_prime()` para veriicar que sus primos `a` y `b` son realmente primos.

3. Verifique que 1 es el máximo común divisor de los dos primos de los ejercicios anteriores.

4. Encuentre dos enteros que formen una "combinación lineal" entera de los dos primos que sea igual a 1. Incluya una verificación de su resultado.

5. Determine una factorización en potencias de primos para $c = 4\,598\,037\,234$.

6. Escriba una celda que defina nuevamente el mismo valor de `c`, y luego defina un candidato a divisor de `c` llamado `d`. La tercera línea de la celda debiera retornar `True` si y solo si `d` es un divisor de `c`. Ilustre el uso de su celda testeando su código con $d = 7$ y en una nueva copia de la celda, testeando su código con $d = 11$.

3

Grupos

Comenzaremos nuestro estudio de estructuras algebraicas investigando conjuntos dotados de una operación que satisfaga ciertos axiomas razonables; es decir, queremos definir una operación en un conjunto de forma de generalizar estructuras familiares como los enteros $\mathbb{Z}$ con la operación única de suma, o matrices invertibles de 2×2 con la operación única de multiplicación de matrices. Los enteros y las matrices de 2×2, junto con sus respectivas operaciones únicas, son ejemplos de estructuras algebraicas conocidas como grupos.

La teoría de grupos ocupa una posición central en matemáticas. La teoría moderna de grupos surgió del intento de encontrar las raíces de un polinomio en términos de sus coeficientes. Los grupos tienen hoy un rol central en áreas tales como teoría de códigos, conteo, y el estudio de simetrías; muchas áreas de la biología, la química, y la física se han visto beneficiadas por la teoría de grupos.

3.1 Clases de Equivalencia de Enteros y Simetrías

Investiguemos ahora ciertas estructuras matemáticas que pueden ser vistas como conjuntos con una sola operación.

Los Enteros módulo n

Los enteros mód n se han vuelto indispensables en la teoría y las aplicaciones del álgebra. En matemáticas se usan en criptografía, teoría de códigos, y la detección de errores en códigos de identificación.

Ya hemos visto que dos enteros a y b son equivalentes mód n si n divide a $a - b$. Los enteros mód n también particionan $\mathbb{Z}$ en n distintas clases de equivalencia; denotaremos el conjunto de estas clases de equivalencia por $\mathbb{Z}_n$. Considere los enteros módulo 12 y la correspondiente partición de los enteros:

$$\begin{aligned}
[0] &= \{\ldots, -12, 0, 12, 24, \ldots\}, \\
[1] &= \{\ldots, -11, 1, 13, 25, \ldots\}, \\
&\vdots \\
[11] &= \{\ldots, -1, 11, 23, 35, \ldots\}.
\end{aligned}$$

Cuando no haya posibilidad de confusión, usaremos $0, 1, \ldots, 11$ para indicar las clases de equivalencia $[0], [1], \ldots, [11]$ respectivamente. Podemos hacer aritmética en $\mathbb{Z}_n$. Para dos enteros a y b, definimos adición módulo n como $(a+b) \pmod{n}$; es decir, el resto de la división de $a + b$ entre n. Similarmente, la multiplicación módulo n se define como $(ab) \pmod{n}$, el resto de la división de ab entre n.

Ejemplo 3.1. Los siguiente ejemplos ilustran la aritméticas de los enteros módulo n:

$$\begin{aligned} 7+4 &\equiv 1 \pmod 5 & \qquad 7\cdot 3 &\equiv 1 \pmod 5 \\ 3+5 &\equiv 0 \pmod 8 & \qquad 3\cdot 5 &\equiv 7 \pmod 8 \\ 3+4 &\equiv 7 \pmod{12} & \qquad 3\cdot 4 &\equiv 0 \pmod{12}. \end{aligned}$$

En particular, notemos que es posible que el producto de dos números no equivalentes a 0 módulo n sea equivalente a 0 módulo n.

Ejemplo 3.2. La mayoría, pero no todas, las reglas usuales de la aritmética se cumplen para la adición y la multiplicación en $\mathbb{Z}_n$. Por ejemplo, no es necesariamente cierto que haya un inverso multiplicativo. Considere la tabla de multiplicación para $\mathbb{Z}_8$ en el Cuadro 3.3. Note que 2, 4, y 6 no tienen inversos multiplicativos; es decir, para $n = 2$, 4, o 6, no hay un entero k tal que $kn \equiv 1 \pmod 8$.

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Cuadro 3.3: Tabla de multiplicación para $\mathbb{Z}_8$

Proposición 3.4. *Sea $\mathbb{Z}_n$ el conjunto de clases de equivalencia de los enteros mód n y sean $a, b, c \in \mathbb{Z}_n$.*

1. *Adición y multiplicación son conmutativas:*

$$\begin{aligned} a+b &\equiv b+a \pmod n \\ ab &\equiv ba \pmod n. \end{aligned}$$

2. *Adición y multiplicación son asociativas:*

$$\begin{aligned} (a+b)+c &\equiv a+(b+c) \pmod n \\ (ab)c &\equiv a(bc) \pmod n. \end{aligned}$$

3. *Hay neutros para ambas operaciones:*

$$\begin{aligned} a+0 &\equiv a \pmod n \\ a\cdot 1 &\equiv a \pmod n. \end{aligned}$$

4. *La multiplicación distribuye sobre la adición:*

$$a(b+c) \equiv ab+ac \pmod n.$$

5. *Para cada entero a hay un inverso aditivo $-a$:*

$$a + (-a) \equiv 0 \pmod{n}.$$

6. *Sea a un entero no nulo. Entonces* $\mathrm{mcd}(a, n) = 1$ *si y solo si hay un inverso multiplicativo b para $a \pmod{n}$; es decir, un entero no nulo b tal que*

$$ab \equiv 1 \pmod{n}.$$

DEMOSTRACIÓN. Demostraremos (1) y (6) y dejaremos las demás propiedades para ser demostradas en los ejercicios.

(1) Adición y multiplicación son conmutativas módulo n pues el resto obtenido al dividir $a + b$ entre n es el mismo que el resto obtenido al dividir $b + a$ entre n.

(6) Supongamos que $\mathrm{mcd}(a, n) = 1$. Entonces existen enteros r y s tales que $ar + ns = 1$. Como $ns = 1 - ar$, se cumple que $ar \equiv 1 \pmod{n}$. Si b es la clase de equivalencia de r, $ab \equiv 1 \pmod{n}$.

Recíprocamente, supongamos que hay un entero b tal que $ab \equiv 1 \pmod{n}$. Entonces n divide a $ab - 1$, de manera que hay un entero k tal que $ab - nk = 1$. Sea $d = \mathrm{mcd}(a, n)$. Como d divide a $ab - nk$, d también divide a 1; luego, $d = 1$. □

Simetrías

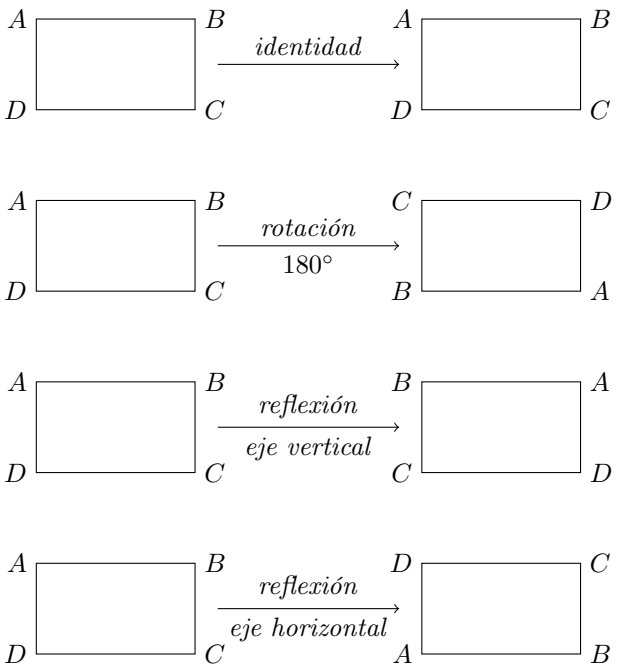
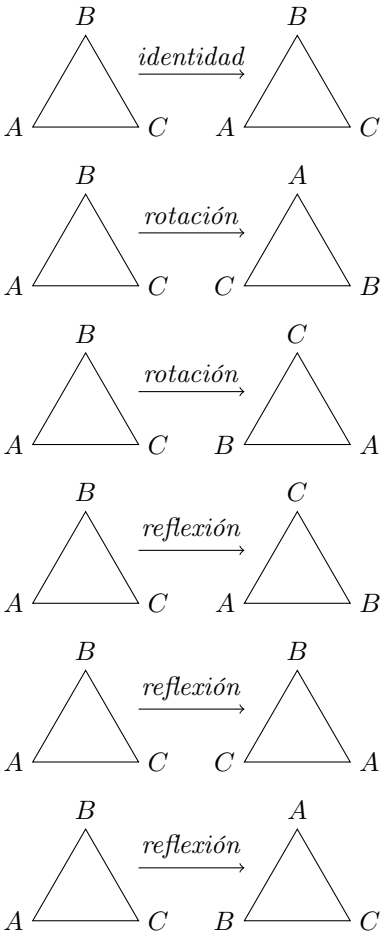


Figura 3.5: Movimientos rígidos de un rectángulo

Una ***simetría*** de una figura geométrica es un reposicionamiento de la figura que preserva las relaciones entre sus lados y vértices tal como las distancias y los ángulos. Una función del plano en sí mismo que preserva la simetría de un objeto se llama ***movimiento rígido***. Por ejemplo, si miramos el rectángulo de la Figura 3.5, es fácil ver que una rotación en 180° o 360° devuelve un rectángulo en el plano con la misma orientación como el rectángulo original

y la misma relación entre sus vértices. Una reflexión del rectángulo por su eje vertical o su eje horizontal también puede ser reconocida como simetría de éste. Sin embargo, una rotación en 90° en cualquier dirección no puede ser una simetría del rectángulo a menos que sea un cuadrado.



$$id = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

$$\mu_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$

$$\mu_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

Figura 3.6: Simetrías de un triángulo

Encontremos las simetrías de un triángulo equilátero $\triangle ABC$. Para encontrar las simetrías de $\triangle ABC$, debemos primero examinar las permutaciones de los vértices A, B, y C para luego preguntarnos si una permutación se extiende a una simetría del triángulo. Recuerde que una ***permutación*** de un conjunto S es una función biyectiva $\pi : S \to S$. Los tres vértices tienen $3! = 6$ permutaciones, de manera que el triángulo tiene a lo más seis simetrías. Para ver que hay seis permutaciones, observe que hay tres diferentes elecciones para el primer vértice, y dos para el segundo, y que el vértice restante está determinado por la posición de los primeros dos. Así tenemos $3 \cdot 2 \cdot 1 = 3! = 6$ arreglos diferentes. Para describir una permutación de los vértices de un triángulo equilátero que envía A en B, B en C, y C en A, escribiremos el arreglo

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}.$$

Note que esta permutación en particular corresponde al movimiento rígido de rotar el triángulo en 120° en dirección horaria. De hecho, cada permutación

produce una simetría del triángulo. Todas estas simetría se muestran en la Figura 3.6.

Es natural preguntarse qué pasa si un movimiento del triángulo $\triangle ABC$ es seguido por otro. ¿Qué simetría es $\mu_1\rho_1$; es decir, si realizamos la permutación ρ_1 y luego la permutación μ_1? *Recuerde que acá estamos componiendo funciones. A pesar de que usualmente multiplicamos de izquierda a derecha, componemos funciones de derecha a izquierda.* Tenemos

$$\begin{aligned}(\mu_1\rho_1)(A) &= \mu_1(\rho_1(A)) = \mu_1(B) = C\\ (\mu_1\rho_1)(B) &= \mu_1(\rho_1(B)) = \mu_1(C) = B\\ (\mu_1\rho_1)(C) &= \mu_1(\rho_1(C)) = \mu_1(A) = A.\end{aligned}$$

Esta es la misma simetría que μ_2. Supongamos que hacemos estas mismas operaciones en el orden opuesto, $\rho_1\mu_1$. Es fácil determinar que esto es lo mismo que la simetría μ_3; luego, $\rho_1\mu_1 \neq \mu_1\rho_1$. Una tabla de multiplicación de simetrías de un triángulo equilátero $\triangle ABC$ se encuentra en el Cuadro 3.7.

Note que en la tabla de multiplicación para las simetrías de un triángulo equilátero, para cada movimiento α del triángulo, hay otro movimiento β tal que $\alpha\beta = \mathrm{id}$; es decir, para cada movimiento hay otro movimiento que devuelve al triángulo a su orientación original.

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

Cuadro 3.7: Simetrías de un triángulo equilátero

3.2 Definiciones y Ejemplos

Los enteros mód n y las simetrías de un triángulo o un rectángulo son ejemplos de grupos. Una ***operación binaria*** o ***ley de composición*** en un conjunto G es una función $G \times G \to G$ que asigna a cada par $(a, b) \in G \times G$ un único elemento $a \circ b$, o ab en G, llamado composición de a y b. Un ***grupo*** $(G, \circ)$ es un conjunto G junto a una ley de composición $(a, b) \mapsto a \circ b$ que satisface los siguientes axiomas.

- La ley de composición es ***asociativa***. Es decir,

  $$(a \circ b) \circ c = a \circ (b \circ c)$$

  para $a, b, c \in G$.

- Existe un elemento $e \in G$, llamado ***elemento identidad***, tal que para cualquier elemento $a \in G$

  $$e \circ a = a \circ e = a.$$

- Para cada elemento $a \in G$, existe un ***elemento inverso*** en G, denotado por a^{-1}, tal que

  $$a \circ a^{-1} = a^{-1} \circ a = e.$$

Un grupo G con la propiedad que $a \circ b = b \circ a$ para todo $a, b \in G$ se llama ***abeliano*** o ***conmutativo***. Grupos que no satisfacen esta propiedad se dicen ***no abelianos*** o ***no conmutativos***.

Ejemplo 3.8. Los enteros $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$ forman un grupo bajo la operación de adición. La operación binaria en dos enteros $m, n \in \mathbb{Z}$ es simplemente su suma. Como la suma de enteros tiene una notación bien establecida, usaremos el operador $+$ en lugar de $\circ$; es decir, escribiremos $m+n$ en lugar de $m \circ n$. La identidad es 0, y el inverso de $n \in \mathbb{Z}$ se escribe como $-n$ en lugar de n^{-1}. Note que el conjunto de los enteros bajo adición tiene la propiedad adicional de que $m + n = n + m$ y por lo tanto forma un grupo abeliano.

La mayor parte de las veces escribiremos ab en lugar de $a \circ b$; sin embargo, si el grupo ya tiene una operación natural, como la suma en los enteros, usaremos aquella operación. Esto es, si estamos sumando dos enteros, aún escribiremos $m+n$, $-n$ para el inverso, y 0 para la identidad como de costumbre. También escribiremos $m - n$ en lugar de $m + (-n)$.

Frecuentemente es conveniente describir un grupo en términos de su tabla de adición o de multiplicación. Una tal tabla se llama ***tabla de Cayley***.

Ejemplo 3.9. Los enteros mód n forman un grupo bajo adición módulo n. Considere $\mathbb{Z}_5$, que consiste de las clases de equivalencia de los enteros 0, 1, 2, 3, y 4. Definimos la operación de grupo en $\mathbb{Z}_5$ por adición módulo 5. Escribimos esta operación binaria en el grupo de forma aditiva, es decir, escribimos $m+n$. El elemento 0 es la identidad del grupo y cada elemento en $\mathbb{Z}_5$ tiene un inverso. Por ejemplo, $2+3 = 3+2 = 0$. El Cuadro 3.10 es una tabla de Cayley para $\mathbb{Z}_5$. Por la Proposición 3.4, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ es un grupo bajo la operación binaria de adición mód n.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Cuadro 3.10: Tabla de Cayley para $(\mathbb{Z}_5, +)$

Ejemplo 3.11. No todo conjunto con una operación binaria es un grupo. Por ejemplo, si tomamos como operación binaria la multiplicación modular en $\mathbb{Z}_n$, entonces $\mathbb{Z}_n$ no es un grupo. El elemento 1 actúa como una identidad de grupo pues $1 \cdot k = k \cdot 1 = k$ para cualquier $k \in \mathbb{Z}_n$; sin embargo, no existe un inverso multiplicativo para 0 pues $0 \cdot k = k \cdot 0 = 0$ para todo k en $\mathbb{Z}_n$. Incluso si consideramos el conjunto $\mathbb{Z}_n \setminus \{0\}$, aún es posible que no tengamos un grupo. Por ejemplo, $2 \in \mathbb{Z}_6$ no tiene inverso multiplicativo pues

$$\begin{aligned} 0 \cdot 2 &= 0 & 1 \cdot 2 &= 2 \\ 2 \cdot 2 &= 4 & 3 \cdot 2 &= 0 \\ 4 \cdot 2 &= 2 & 5 \cdot 2 &= 4. \end{aligned}$$

Por la Proposición 3.4, todo elemento no nulo k tiene un inverso multiplicativo en $\mathbb{Z}_n$ si k es relativamente primo con n. Denotemos el conjunto de tales elementos en $\mathbb{Z}_n$ por $U(n)$. Entonces $U(n)$ es un grupo llamado el ***grupo de unidades*** de $\mathbb{Z}_n$. El Cuadro 3.12 es una tabla de Cayley para el grupo $U(8)$.

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Cuadro 3.12: Tabla de multiplicación para $U(8)$

Ejemplo 3.13. Las simetrías de un triángulo equilátero descritas en la Sección 3.1 forman un grupo no abeliano. Como observamos, no es necesariamente cierto que $\alpha\beta = \beta\alpha$ para dos simetrías α y β. Usando el Cuadro 3.7, que es una tabla de Cayley para este grupo, podemos fácilmente verificar que las simetrías de un triángulo equilátero forman efectivamente un grupo. Denotaremos este grupo como S_3 o D_3, por razones que explicaremos más adelante.

Ejemplo 3.14. Usaremos $\mathbb{M}_2(\mathbb{R})$ para denotar al conjunto de todas las matrices de 2×2. Sea $GL_2(\mathbb{R})$ el subconjunto de $\mathbb{M}_2(\mathbb{R})$ que consiste de las matrices invertibles; es decir, una matriz

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

está en $GL_2(\mathbb{R})$ si existe una matriz A^{-1} tal que $AA^{-1} = A^{-1}A = I$, donde I la matriz identidad de 2×2. Que A tenga una inversa es equivalente a que el determinante de A no sea cero; es decir, $\det A = ad - bc \neq 0$. El conjunto de las matrices invertibles forma un grupo llamado el ***grupo lineal general***. La identidad del grupo es la matriz identidad.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

La inversa de $A \in GL_2(\mathbb{R})$ es

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

El producto de dos matrices invertibles es nuevamente invertible. La multiplicación de matrices es asociativa, satisfaciendo así el otro axioma de grupos. Para las matrices en general no se cumple que $AB = BA$; por lo tanto, $GL_2(\mathbb{R})$ es otro ejemplo de un grupo no abeliano.

Ejemplo 3.15. Sean

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
$$J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \qquad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

con $i^2 = -1$. Entonces las relaciones $I^2 = J^2 = K^2 = -1$, $IJ = K$, $JK = I$, $KI = J$, $JI = -K$, $KJ = -I$, y $IK = -J$ se satisfacen. El conjunto $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$ es un grupo llamado ***grupo de cuaterniones***. Note que Q_8 es no conmutativo.

Ejemplo 3.16. Sea $\mathbb{C}^*$el conjunto de los números complejos no nulos. $\mathbb{C}^*$ forma un grupo bajo la operación de multiplicación. La identidad es 1. Si $z = a + bi$ es un número complejo no nulo, entonces

$$z^{-1} = \frac{a - bi}{a^2 + b^2}$$

es el inverso de z. Es fácil verificar que se cumplen los demás axiomas de grupo.

Un grupo es ***finito***, o tiene ***orden finito***, si contiene un número finito de elementos; de otro modo, el grupo se dice ***infinito*** o que tiene ***orden infinito***. El ***orden*** de un grupo finito es el número de elementos que contiene. Si G es un grupo que contiene n elementos, escribiremos $|G| = n$. El grupo $\mathbb{Z}_5$ es un grupo finito de orden 5; los enteros $\mathbb{Z}$ forman un grupo infinito bajo la adición, y en ocasiones escribiremos $|\mathbb{Z}| = \infty$.

Propiedades básicas de los Grupos

Proposición 3.17. *El elemento identidad en un grupo G es único; es decir, hay solo un elemento $e \in G$ tal que $eg = ge = g$ para todo $g \in G$.*

Demostración. Supongamos que e y e' son ambas identidades en G. Entonces $eg = ge = g$ y $e'g = ge' = g$ para todo $g \in G$. Debemos demostrar que $e = e'$. Si pensamos en e como la identidad, entonces $ee' = e'$; pero si e' es la identidad, entonces $ee' = e$. Combinando estas dos ecuaciones, tenemos $e = ee' = e'$. □

Los inversos en un grupo también son únicos. Si g' y g'' son ambos inversos de un elemento g en un grupo G, entonces $gg' = g'g = e$ y $gg'' = g''g = e$. Queremos mostrar que $g' = g''$, pero $g' = g'e = g'(gg'') = (g'g)g'' = eg'' = g''$. Resumimos este hecho en la siguiente proposición.

Proposición 3.18. *Si g es un elemento en un grupo G, entonces el inverso de g, denotado por g^{-1}, es único.*

Proposición 3.19. *Sea G un grupo. Si $a, b \in G$, entonces $(ab)^{-1} = b^{-1}a^{-1}$.*

Demostración. Sean $a, b \in G$. Entonces $abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$. Similarmente, $b^{-1}a^{-1}ab = e$. Por la proposición anterior, los inversos son únicos; luego, $(ab)^{-1} = b^{-1}a^{-1}$. □

Proposición 3.20. *Sea G un grupo. Para cualquier $a \in G$, $(a^{-1})^{-1} = a$.*

Demostración. Notemos que $a^{-1}(a^{-1})^{-1} = e$. Por lo tanto, multiplicando ambos lados de esta ecuación por a, tenemos

$$(a^{-1})^{-1} = e(a^{-1})^{-1} = aa^{-1}(a^{-1})^{-1} = ae = a.$$ □

Tiene sentido escribir ecuaciones con elementos y operaciones de un grupo. Si a y b son dos elementos en un grupo G, ¿existe un elemento $x \in G$ tal que $ax = b$? ¿Si tal x existe, es único? La siguiente proposición entrega una respuesta afirmativa a ambas preguntas.

Proposición 3.21. *Sea G un grupo y sean a y b dos elementos cualquiera en G. Entonces las ecuaciones $ax = b$ y $xa = b$ tienen una única solución en G.*

Demostración. Supongamos que $ax = b$. Debemos demostrar que tal x existe. Podemos multiplicar ambos lados de $ax = b$ por a^{-1} para encontrar $x = ex = a^{-1}ax = a^{-1}b$.

Para demostrar la unicidad, supongamos que x_1 y x_2 son ambas soluciones de $ax = b$; entonces $ax_1 = b = ax_2$. Luego $x_1 = a^{-1}ax_1 = a^{-1}ax_2 = x_2$. La demostración de la existencia y unicidad de la solución de $xa = b$ es similar. □

Proposición 3.22. *Si G es un grupo y $a, b, c \in G$, entonces $ba = ca$ implica $b = c$ y $ab = ac$ implica $b = c$.*

Esta proposición nos dice que las ***leyes de cancelación derecha e izquierda*** se cumple para grupos. Dejamos la demostración como ejercicio.

Podemos utilizar la notación exponencial en grupos de la forma en que estamos acostumbrados. Si G es un grupo y $g \in G$, definimos $g^0 = e$. Para $n \in \mathbb{N}$, definimos

$$g^n = \underbrace{g \cdot g \cdots g}_{n \text{ times}}$$

y

$$g^{-n} = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}.$$

Teorema 3.23. *En un grupo, se cumplen las reglas usuales de los exponentes; es decir, para todo $g, h \in G$,*

1. *$g^m g^n = g^{m+n}$ para todo $m, n \in \mathbb{Z}$;*
2. *$(g^m)^n = g^{mn}$ para todo $m, n \in \mathbb{Z}$;*
3. *$(gh)^n = (h^{-1}g^{-1})^{-n}$ para todo $n \in \mathbb{Z}$. Más aún, si G es abeliano, entonces $(gh)^n = g^n h^n$.*

Dejaremos la demostración de este teorema como un ejercicio. Note que $(gh)^n \neq g^n h^n$ en general, pues el grupo puede no ser abeliano. Si el grupo es $\mathbb{Z}$ o $\mathbb{Z}_n$, escribiremos la operación del grupo de forma aditiva y la operación exponencial como multiplicación; es decir, escribimos ng en lugar de g^n. Las leyes de los exponentes ahora son

1. $mg + ng = (m + n)g$ para todo $m, n \in \mathbb{Z}$;
2. $m(ng) = (mn)g$ para todo $m, n \in \mathbb{Z}$;
3. $m(g + h) = mg + mh$ para todo $n \in \mathbb{Z}$.

Es importante notar que esto solo es posible dado que $\mathbb{Z}$ y $\mathbb{Z}_n$ son grupos conmutativos.

Nota Histórica

Si bien la primera definición axiomática clara de grupo recién fue dada a finales del siglo XIX, los métodos de teoría de grupos ya habían sido usados anteriormente en el desarrollo de muchas áreas de las matemáticas, incluyendo la geometría y la teoría de ecuaciones algebraicas.

Joseph-Louis Lagrange usó teoría de grupos en una memoria de 1770–1771 para estudiar métodos de resolución de ecuaciones polinomiales. Más tarde, Évariste Galois (1811–1832) desarrolló con éxito las matemáticas necesarias para determinar exactamente cuáles ecuaciones polinomiales podían ser resueltas en términos de los coeficientes del polinomio en cuestión. La herramienta principal que usó Galois' fue la teoría de grupos.

El estudio de la geometría sufrió cambios revolucionarios en 1872 cuando Felix Klein propuso que los espacios geométricos debían ser estudiados examinando aquellas propiedades que son invariantes bajo una trasformación del espacio. Sophus Lie, coetáneo de Klein, usó teoría de grupos para estudiar las soluciones de ecuaciones diferenciales parciales. Uno de los primeros libros en tratar la teoría de grupos en forma moderna es el de William Burnside *The Theory of Groups of Finite Order* [1], publicado originalmente en 1897.

3.3 Subgrupos

Definiciones y Ejemplos

En ocasiones necesitaremos estudiar grupos más pequeños dentro de un grupo mayor. El conjunto de los enteros pares $2\mathbb{Z} = \{\ldots, -2, 0, 2, 4, \ldots\}$ es un grupo bajo la operación de adición. Este grupo está naturalmente contenido en el grupo de enteros bajo adición. Definimos un ***subgrupo*** H de un grupo G como un subconjunto H de G tal que con la operación de G restringida a H, H es un grupo. Observe que todo grupo G con al menos dos elementos siempre tiene al menos dos subgrupos, el subgrupo que consiste únicamente del elemento identidad y el grupo completo. El subgrupo $H = \{e\}$ de un grupo G se llama ***subgrupo trivial***. Un subgrupo que es un subconjunto propio de G se llama ***subgrupo propio***. En muchos de los ejemplos que hemos considerado hasta ahora, existen otros subgrupos aparte de los subgrupos trivial e impropio.

Ejemplo 3.24. Considere el conjunto de los números reales no nulos, $\mathbb{R}^*$, con la operación de multiplicación para formar un grupo. La identidad de este grupo es 1 y el inverso de cualquier elemento $a \in \mathbb{R}^*$ es simplemente $1/a$. Mostraremos que

$$\mathbb{Q}^* = \{p/q : p \text{ y } q \text{ son enteros no nulos}\}$$

es un subgrupo de $\mathbb{R}^*$. La identidad de $\mathbb{R}^*$ es 1; sin embargo, $1 = 1/1$ es el cociente de dos enteros no nulos. Por lo tanto, la identidad de $\mathbb{R}^*$ está en $\mathbb{Q}^*$. Dados dos elementos en $\mathbb{Q}^*$, digamos p/q y r/s, su producto pr/qs también está en $\mathbb{Q}^*$. El inverso de cualquier elemento $p/q \in \mathbb{Q}^*$ está nuevamente en $\mathbb{Q}^*$ pues $(p/q)^{-1} = q/p$. Como la multiplicación en $\mathbb{R}^*$ es asociativa, multiplicación en $\mathbb{Q}^*$ es asociativa.

Ejemplo 3.25. Recuerde que $\mathbb{C}^*$ es el grupo multiplicativo de los números complejo no nulos. Sea $H = \{1, -1, i, -i\}$. Entonces H es un subgrupo de $\mathbb{C}^*$. Es fácil verificar que H es un grupo con la operación de multiplicación y que $H \subset \mathbb{C}^*$.

Ejemplo 3.26. Sea $SL_2(\mathbb{R})$ el subconjunto de $GL_2(\mathbb{R})$ que contiene las matrices de determinante uno; es decir, una matriz

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

está en $SL_2(\mathbb{R})$ precisamente cuando $ad - bc = 1$. Para mostrar que $SL_2(\mathbb{R})$ es un subgrupo del grupo lineal general, debemos demostrar que también es un grupo con la operación de multiplicación de matrices. La matriz identidad de 2×2 está en $SL_2(\mathbb{R})$, así como la inversa de la matriz A:

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Falta mostrar que la multiplicación es cerrada; es decir, que el producto de dos matrices de determinante uno también tiene determinante uno. Dejaremos esta tarea como ejercicio. El grupo $SL_2(\mathbb{R})$ se llama ***grupo lineal especial***.

Ejemplo 3.27. Es importante notar que un subconjunto H de un grupo G puede ser un grupo sin ser un subgrupo de G. Para que H sea un subgrupo de G debe heredar la operación binaria de G. El conjunto de todas las matrices de 2×2, $\mathbb{M}_2(\mathbb{R})$, forma un grupo con la operación de adición. El grupo lineal

general $GL_2(\mathbb{R})$ es un subconjunto de $\mathbb{M}_2(\mathbb{R})$ y es un grupo con la operación de multiplicación de matrices, pero no es un subgrupo de $\mathbb{M}_2(\mathbb{R})$. Si sumamos dos matrices invertibles no necesariamente obtendremos otra matriz invertible. Observe que

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

pero la matriz cero no está en $GL_2(\mathbb{R})$.

Ejemplo 3.28. Una manera de saber si dos grupos son el mismo grupo, es examinando sus subgrupos. Aparte del subgrupo trivial y del grupo mismo, el grupo $\mathbb{Z}_4$ tiene exactamente un subgrupo adicional que consiste de los elementos 0 y 2. A partir del grupo $\mathbb{Z}_2$, podemos formar otro grupo de cuatro elementos como sigue. Como conjunto, este grupo es $\mathbb{Z}_2 \times \mathbb{Z}_2$. Realizamos las operacioens coordenada a coordenada; es decir, $(a, b) + (c, d) = (a + c, b + d)$. El Cuadro 3.29 es una tabla de sumas para $\mathbb{Z}_2 \times \mathbb{Z}_2$. Como hay tres subgrupos propios no triviales de $\mathbb{Z}_2 \times \mathbb{Z}_2$, $H_1 = \{(0, 0), (0, 1)\}$, $H_2 = \{(0, 0), (1, 0)\}$, y $H_3 = \{(0, 0), (1, 1)\}$, $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$ deben ser grupos diferentes.

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Cuadro 3.29: Tabla de sumas para $\mathbb{Z}_2 \times \mathbb{Z}_2$

Algunos Teoremas para Subgrupos

Examinemos algunos criterios para determinar exactamente cuándo un subconjunto de un grupo es un subgrupo.

Proposición 3.30. *Un subconjunto H de G es un subgrupo si y solo si satiface las siguientes condiciones.*

1. *La identidad e de G está en H.*
2. *Si $h_1, h_2 \in H$, entonces $h_1 h_2 \in H$.*
3. *Si $h \in H$, entonces $h^{-1} \in H$.*

Demostración. Primero supongamos que H es un subgrupo de G. Debemos mostrar que se cumplen las tres condiciones. Como H es un grupo, debe tener una identidad e_H. Debemos demostrar que $e_H = e$, donde e es la identidad de G. Sabemos que $e_H e_H = e_H$ y que $ee_H = e_H e = e_H$; por lo tanto, $ee_H = e_H e_H$. Por cancelación a la derecha, $e = e_H$. La segunda condición se cumple pues un subgrupo de H es un grupo. Para demostrar la tercera condición, sea $h \in H$. Como H es un grupo, hay un elemento $h' \in H$ tal que $hh' = h'h = e$. Por la unicidad del inverso en G, $h' = h^{-1}$.

Recíprocamente, si se cumplen la tres condiciones, debemos demostrar que H es un grupo con la misma operación que G; pero, estas tres condiciones más la asociatividad de la operación binaria son exactamente las condiciones de la definición de grupo. □

Proposición 3.31. *Sea H un subconjunto de un grupo G. Entonces H es un subgrupo de G si y solo si $H \neq \emptyset$, y para todo $g, h \in H$ se tiene que gh^{-1} está en H.*

DEMOSTRACIÓN. Supongamos primero que H es un subgrupo de G. Queremos mostrar que $gh^{-1} \in H$ cada vez que g y h están en H. Como h está en H, su inverso h^{-1} también debe estar en H. Por la clausura de la operación de grupo, $gh^{-1} \in H$.

Recíprocamente, supongamos que $H \subset G$ tal que $H \neq \emptyset$ y $gh^{-1} \in H$ cada vez que $g, h \in H$. Si $g \in H$, entonces $gg^{-1} = e$ está en H. Si $g \in H$, entonces $eg^{-1} = g^{-1}$ también está en H. Sean ahora $h_1, h_2 \in H$. Debemos demostrar que su producto está también en H. pero, $h_1(h_2^{-1})^{-1} = h_1 h_2 \in H$. Luego, H es un subgrupo de G. □

Sage La primera mitad de este libro es sobre teoría de grupos. Sage incluye Grupos, Algoritmos y Programación en (GAP), un programa diseñado principalmente para la teoría de grupos, y que ha estado en constante desarrollo desde 1986. Muchos de los cálculos con grupos hechos en Sage en realidad son realizados por GAP.

3.4 Ejercicios

1. Encuentre todos los $x \in \mathbb{Z}$ que satisfagan cada una de las siguientes ecuaciones.

(a) $3x \equiv 2 \pmod 7$

(b) $5x + 1 \equiv 13 \pmod{23}$

(c) $5x + 1 \equiv 13 \pmod{26}$

(d) $9x \equiv 3 \pmod 5$

(e) $5x \equiv 1 \pmod 6$

(f) $3x \equiv 1 \pmod 6$

2. ¿Cuál(es) de las siguientes tablas de multiplicación definidas en el conjunto $G = \{a, b, c, d\}$ forma(n) un grupo? Justifique su respuesta en cada caso.

(a)

$\circ$	a	b	c	d
a	a	c	d	a
b	b	b	c	d
c	c	d	a	b
d	d	a	b	c

(b)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

(c)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

(d)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

3. Complete tablas de Cayley para los grupos formados por las simetrías de un rectángulo y para $(\mathbb{Z}_4, +)$. ¿Cuántos elementos hay en cada grupo? ¿Son iguales estos grupos? ¿Por qué o por qué no?

4. Describa las simetrías de un rombo y demuestre que el conjunto de simetrías forma un grupo. Complete tablas de Cayley tanto para las simetrías de un rectángulo como para las simetrías de un rombo. ¿Son iguales estos grupos?

5. Describa las simetrías de un cuadrado y demuestre que el conjunto de tales simetrías es un grupo. Complete una tabla de Cayley para las simetrías. ¿De cuántas maneras es posible permutar los vértices de un cuadrado? ¿Corresponde cada una de estas permutaciones a una simetría del cuadrado? El grupo de simetrías del cuadrado se denota por D_4.

6. Complete una tabla de multiplicación para el grupo $U(12)$.

7. Sea $S = \mathbb{R} \setminus \{-1\}$ y defina una operación binaria en S por $a * b = a + b + ab$. Demuestre que $(S, *)$ es un grupo abeliano.

8. Dé un ejemplo de dos elementos A y B en $GL_2(\mathbb{R})$ con $AB \neq BA$.

9. Demuestre que el producto de dos matrices en $SL_2(\mathbb{R})$ tiene determinante uno.

10. Demuestre que el conjunto de matrices de la forma

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

es un grupo con la operación de multiplicación de matrices. Este grupo, conocido como el ***grupo de Heisenberg***, es importante en mecánica cuántica. La multiplicación de matrices en el grupo de Heisenberg se define por

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x + x' & y + y' + xz' \\ 0 & 1 & z + z' \\ 0 & 0 & 1 \end{pmatrix}.$$

11. Demuestre que $\det(AB) = \det(A)\det(B)$ en $GL_2(\mathbb{R})$. Use este resultado para mostrar que la operación binaria en el grupo $GL_2(\mathbb{R})$ es cerrada; es decir, si A y B están en $GL_2(\mathbb{R})$, entonces $AB \in GL_2(\mathbb{R})$.

12. Sea $\mathbb{Z}_2^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{Z}_2\}$. Defina una operación binaria en $\mathbb{Z}_2^n$ por

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Demuestre que $\mathbb{Z}_2^n$ es un grupo con esta operación. Este grupo es importante en la teoría de códigos algebraicos.

13. Muestre que $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ es un grupo con la operación de multiplicación.

14. Dados dos grupos $\mathbb{R}^*$ y $\mathbb{Z}$, sea $G = \mathbb{R}^* \times \mathbb{Z}$. Defina una operación binaria $\circ$ en G por $(a, m) \circ (b, n) = (ab, m + n)$. Muestre que G es un grupo con esta operación.

15. Demuestre o refute que todo grupo con seis elementos es abeliano.

16. Dé un ejemplo explícito de algún grupo G y elementos $g, h \in G$ con $(gh)^n \neq g^n h^n$.

17. Dé un ejemplo de tres grupos diferentes con ocho elementos. ¿Por qué son diferentes estos grupos?

18. Muestre que hay $n!$ permutaciones de un conjunto de n elementos.

19. Muestre que

$$0 + a \equiv a + 0 \equiv a \pmod{n}$$

para todo $a \in \mathbb{Z}_n$.

20. Demuestre que existe una identidad multiplicativa para los enteros módulo n:

$$a \cdot 1 \equiv a \pmod{n}.$$

21. Para cada $a \in \mathbb{Z}_n$ encuentre un elemento $b \in \mathbb{Z}_n$ tal que

$$a + b \equiv b + a \equiv 0 \pmod{n}.$$

22. Muestre que la suma y el producto mód n son operaciones bien definidas. Es decir, muestre que no dependen de la elección de representantes de las clases de equivalencia mód n.

23. Muestre que la suma y el producto mód n son operaciones asociativas.

24. Muestre que la multiplicación distribuye sobre la suma módulo n:

$$a(b + c) \equiv ab + ac \pmod{n}.$$

25. Sean a y b elementos en un grupo G. Demuestre que $ab^n a^{-1} = (aba^{-1})^n$ para $n \in \mathbb{Z}$.

26. Sea $U(n)$ el grupo de unidades en $\mathbb{Z}_n$. Si $n > 2$, demuestre que hay un elemento $k \in U(n)$ tal que $k^2 = 1$ y $k \neq 1$.

27. Demuestre que el inverso de $g_1 g_2 \cdots g_n$ es $g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}$.

28. Complete la demostración de la Proposición 3.21: si G es un grupo y $a, b \in G$, entonces la ecuación $xa = b$ tiene una única solución en G.

29. Demuestre el Teorema 3.23.

30. Demuestre las leyes de cancelación izquierda y derecha para un grupo G; es decir, demuestre que en el grupo G, $ba = ca$ implica $b = c$ y $ab = ac$ implica $b = c$ para elementos cualquiera $a, b, c \in G$.

31. Demuestre que si $a^2 = e$ para todos los elementos a en un grupo G, entonces G debe ser abeliano.

32. Demuestre que si G es un grupo finito de orden par, entonces existe un $a \in G$ tal que a no es la identidad y $a^2 = e$.

33. Sea G un grupo y supongamos que $(ab)^2 = a^2 b^2$ para todo a y b en G. Demuestre que G es un grupo abeliano.

34. Encuentre todos los subgrupos de $\mathbb{Z}_3 \times \mathbb{Z}_3$. Use esta información para demostrar que $\mathbb{Z}_3 \times \mathbb{Z}_3$ no es el mismo grupo que $\mathbb{Z}_9$. (Vea el Ejemplo 3.28 para una descripción resumida del producto de grupos.)

35. Encuentre todos los subgrupos del grupo de simetrías de un triángulo equilátero.

36. Encuentre los subgrupos del grupo de simetrías de un cuadrado.

37. Sea $H = \{2^k : k \in \mathbb{Z}\}$. Demuestre que H es un subgrupo de $\mathbb{Q}^*$.

38. Sea $n = 0, 1, 2, \ldots$ y sea $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Demuestre que $n\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$. Muestre que estos son los únicos subgrupos de $\mathbb{Z}$.

39. Sea $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. Demuestre que $\mathbb{T}$ es un subgrupo de $\mathbb{C}^*$.

40. Sea G el conjunto de matrices de 2×2 de la forma

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$

con $\theta \in \mathbb{R}$. Demuestre que G es un subgrupo de $SL_2(\mathbb{R})$.

41. Demuestre que

$$G = \{a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ y } a \text{ y } b \text{ no ambos cero}\}$$

es un subgrupo de $\mathbb{R}^*$ con la operación de multiplicación.

42. Sea G el grupo de matrices de 2×2 con la operción de suma y sea

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}.$$

Demuestre que H es un subgrupo de G.

43. Demuestre o refute: $SL_2(\mathbb{Z})$, el conjunto de matrices de 2×2 con coeficientes enteros y determinante 1, es un subgrupo de $SL_2(\mathbb{R})$.

44. Liste los subgrupos del grupo de cuaterniones, Q_8.

45. Demuestre que la intersección de dos subgrupos de un grupo G también es un subgrupo de G.

46. Demuestre o refute: Si H y K son subgrupos de un grupo G, entonces $H \cup K$ es un subgrupo de G.

47. Demuestre o refute: Si H y K son subgrupos de un grupo G, entonces $HK = \{hk : h \in H \text{ and } k \in K\}$ es un subgrupo de G. ¿Qué pasa si G es abeliano?

48. Sea G un grupo y sea $g \in G$. Demuestre que

$$Z(G) = \{x \in G : gx = xg \text{ para todo } g \in G\}$$

es un subgrupo de G. Este subgrupo se llama ***centro*** de G.

49. Sean a y b elementos de un grupo G. Si $a^4b = ba$ y $a^3 = e$, demuestre que $ab = ba$.

50. Dé un ejemplo de un grupo infinito en que todo subgrupo no trivial es infinito.

51. Si $xy = x^{-1}y^{-1}$ para todo x e y en G, demuestre que G debe ser abeliano.

52. Demuestre o refute: Todo subgrupo propio de un grupo no abeliano es no abeliano.

53. Sea H un subgrupo de G y sea

$$C(H) = \{g \in G : gh = hg \text{ para todo } h \in H\}.$$

Demuestre que $C(H)$ es un subgrupo de G. Este subgrupo se llama ***centralizador*** de H en G.

54. Sea H un subgrupo de G. Si $g \in G$, muestre que $gHg^{-1} = \{ghg^{-1} : h \in H\}$ también es un subgrupo de G.

3.5 Ejercicios Adicionales: Detectando Errores

1. (Códigos UPC) El Código Universal de Productos (UPC por su sigla en inglés) se encuentra en la mayoría de los productos de supermercados y tiendas del retail. El UPC es un código de 12 dígitos que identifica al fabricante de un producto y al producto mismo (Figura 3.32). Los primeros 11 dígitos contienen información sobre el producto; el último dígito se usa para la detección de errores. Si $d_1 d_2 \cdots d_{12}$ es un número UPC válido, entonces

$$3 \cdot d_1 + 1 \cdot d_2 + 3 \cdot d_3 + \cdots + 3 \cdot d_{11} + 1 \cdot d_{12} \equiv 0 \pmod{10}.$$

(a) Muestre que el número UPC 0-50000-30042-6, que aparece en la Figura 3.32, es un número UPC válido.

(b) Muestre que el número 0-50000-30043-6 no es un número UPC válido.

(c) Escriba una fórmula para calcular el dígito verificador, d_{12}, de un número UPC.

(d) El método de detección de errores del UPC puede detectar la mayor parte de los errores de transposición; es decir, puede tereminar si dos dígitos fueron intercambiados. Muestre que el error de transposición 0-05000-30042-6 no es detectado. Encuentre un error de transposición que sí sea detectado. ¿Puede encontrar una regla general sobre cuáles son los errores de transposición que son detectados?

(e) Escriba un programa que determina si un número UPC es válido.

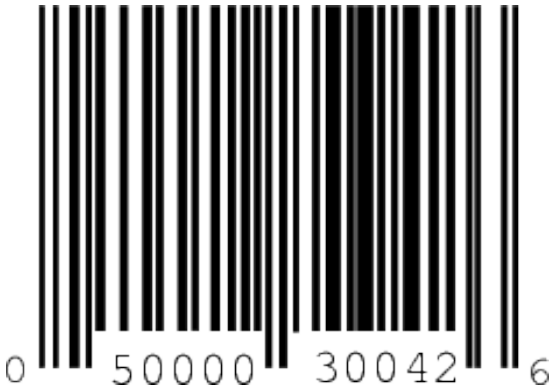


Figura 3.32: Un código UPC

2. Con frecuencia es útil usar la notación de producto interno para este método de detección de errores; de manera que usaremos la notación

$$(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$$

para decir que

$$d_1 w_1 + d_2 w_2 + \cdots + d_k w_k \equiv 0 \pmod{n}.$$

Supongamos que $(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$ es un método de detección de errores para el número de identificación de k dígitos $d_1 d_2 \cdots d_k$, donde $0 \leq d_i < n$. Demuestre que todos los errores en un solo dígito son detectados si y solo si $\text{mcd}(w_i, n) = 1$ para $1 \leq i \leq k$.

3. Sea $(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$ un método de detección de errores para el número de identificación de k dígitos $d_1 d_2 \cdots d_k$, donde $0 \leq d_i < n$. Demuestre que todas las transposiciones de dos dígitos d_i y d_j son detectadas si y solo si $\text{mcd}(w_i - w_j, n) = 1$ para i y j entre 1 y k.

4. (Códigos ISBN) Todo libro tiene un International Standard Book Number (ISBN). Este es un código de 10 dígitos que indica la editorial y el título del libro. El décimo dígito es un dígito verificador que satisface

$$(d_1, d_2, \ldots, d_{10}) \cdot (10, 9, \ldots, 1) \equiv 0 \pmod{11}.$$

Un problema es que d_{10} puede tener que ser 10 para que el producto interno sea cero; en ese caso, se requieren 11 dígitos para que funcione el método. Por lo tanto se usa una X como undécimo dígito para representar el 10. Así el ISBN 3-540-96035-X es un código ISBN válido.

(a) ¿Es el ISBN 0-534-91500-0 un código ISBN válido? ¿Y el ISBN 0-534-91700-0 o el ISBN 0-534-19500-0?

(b) ¿Sirve este método para detectar todos los errores en un solo dígito? ¿y todos los errores de transposición?

(c) ¿Cuántos códigos ISBN diferentes hay?

(d) Escriba un programa que permita calcular el dígito verificador para los primeros nueve dígitos de un código ISBN.

(e) Una editorial tiene sedes en Alemania y Estados Unidos. Su prefijo alemán es 3-540. Si su prefijo en Estados Unidos es 0-`abc`, encuentre `abc` tal que el resto del código ISBN sea el mismo para un libro impreso en Alemania y los Estados Unidos. Bajo el método de codificación ISBN el primer dígito identifica el idioma; alemán es 3 y e inglés es 0. El siguiente grupo de número identifica a la editorial, y el último grupo identifica el libro específico.

3.6 Referencias y Lecturas Recomendadas

[1] Burnside, W. *Theory of Groups of Finite Order*. 2nd ed. Cambridge University Press, Cambridge, 1911; Dover, New York, 1953. A classic. Also available at books.google.com.

[2] Gallian, J. A. and Winters, S. "Modular Arithmetic in the Marketplace," *The American Mathematical Monthly* **95** (1988): 548–51.

[3] Gallian, J. A. *Contemporary Abstract Algebra*. 7th ed. Brooks/Cole, Belmont, CA, 2009.

[4] Hall, M. *Theory of Groups*. 2nd ed. American Mathematical Society, Providence, 1959.

[5] Kurosh, A. E. *The Theory of Groups*, vols. I and II. American Mathematical Society, Providence, 1979.

[6] Rotman, J. J. *An Introduction to the Theory of Groups*. 4th ed. Springer, New York, 1995.

3.7 Sage

Muchos de los grupos discutidos en este capítulo están disponibles para ser estudiados en Sage. Es importante entender que los conjuntos que forman

objetos algebraicos (grupos en este capítulo) se llaman "parents" en Sage, y elementos de estos objetos se llaman "elements." Así cada element pertenece a un parent (en otras palabras, está contenido en algún conjunto). Podemos preguntar por propiedades de los conjuntos (¿finito? ¿orden? ¿abeliano?), y podemos preguntar sobre propiedades de los elementos individuales (¿identidad? inverso?). En lo que sigue mostraremos como crear algunos de estos grupos comunes y empezaremos a explorar sus propiedades con Sage.

Enteros mód n

```
Z8 = Integers(8)
Z8
```

```
Ring of integers modulo 8
```

```
Z8.list()
```

```
[0, 1, 2, 3, 4, 5, 6, 7]
```

```
a = Z8.an_element(); a
```

```
0
```

```
a.parent()
```

```
Ring of integers modulo 8
```

Queremos trabajar con elementos de `Z8`. Si escribimos `6` en una celda Sage, ¿qué significará? ¿El entero 6, el número racional $\frac{6}{1}$, el número real 6.00000, o el número complejo $6.00000+0.00000i$? ¿O quizás lo que realmente queremos es el entero 6 mód 8? Sage no tiene idea sobre lo que queremos. Para aclarárselo a Sage, lo que podemos hacer es "coercionar" `6` a `Z8` con la sintaxis `Z8(6)`. Sin esto, Sage tratará una entrada como `6` como un entero, que en algún sentido es la interpretación más sencilla. Analice lo siguiente cuidadosamente, primero trabajamos con enteros "normales" y luego con enteros mód 8.

```
a = 6
a
```

```
6
```

```
a.parent()
```

```
Integer Ring
```

```
b = 7
c = a + b; c
```

```
13
```

```
d = Z8(6)
d
```

```
6
```

```
d.parent()
```

```
Ring of integers modulo 8
```

```
e = Z8(7)
f = d+e; f
```

```
5
```

```
g = Z8(85); g
```

```
5
```

```
f == g
```

```
True
```

`Z8` es un poco extraño como un primer ejemplo, ya que tiene dos operaciones definidas, tanto suma como producto, con la suma forma un grupo, pero no así con el producto. Aún así, podemos trabajar con la parte aditiva, formando acá la tabla de las sumas.

```
Z8.addition_table(names='elements')
```

```
+  0 1 2 3 4 5 6 7
 +----------------
0| 0 1 2 3 4 5 6 7
1| 1 2 3 4 5 6 7 0
2| 2 3 4 5 6 7 0 1
3| 3 4 5 6 7 0 1 2
4| 4 5 6 7 0 1 2 3
5| 5 6 7 0 1 2 3 4
6| 6 7 0 1 2 3 4 5
7| 7 0 1 2 3 4 5 6
```

Cuando n es un número primo, la estructura multiplicativa (sin el cero), también forma un grupo.

Los enteros mód n son muy importantes, y Sage implementa tanto la multiplicación como la adición en ellos. Grupos de simetrías son un mejor ejemplo de como Sage implementa grupos, pues hay solo una operación presente.

Grupos de simetrías

Los grupos de simetrías de algunos objetos geométricos ya están definidos en Sage, aunque con nombres diferentes. Están implementados como "grupos de permutaciones (permutation groups)" los que empezaremos a estudiar cuidadosamente en el Capítulo 5.

Sage usa enteros para etiquetar los vértices, empezando a contar desde `1`, en lugar de letras. Los elementos normalmente se muestran en "notación cíclica (cycle notation)" que veremos descrita en detalle en el Capítulo 5. Acá hay un ejemplo, que incluye tanto matemáticas como Sage. Para la parte de Sage, construimos el grupo de simetrías y luego creamos la simetría ρ_2 por coerción, desplegando a continuación el elemento en notación cíclica. Después creamos la *fila inferior* de la notación que hemos usado para las permutaciones.

$$\rho_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

```
triangle = SymmetricGroup(3)
rho2 = triangle([3,1,2])
rho2
```

```
(1,3,2)
```

```
[rho2(x) for x in triangle.domain()]
```

```
[3, 1, 2]
```

La última lista merece un comentario. El método `.domain()` entrega una lista de los símbolos usados para el grupo de permutaciones `triangle` y luego `rho2` se usa como si fuera una función (lo *es*) para crear las imágenes que ocuparían la fila inferior.

Con una lista doble podemos listar los seis elementos del grupo en el formato de "fila inferior". Un buen ejercicio es identificar cada elemento con el nombre que le dimos en la Figura 3.6.

```
[[a(x) for x in triangle.domain()] for a in triangle]
```

```
[[1, 2, 3], [2, 1, 3], [2, 3, 1], [3, 1, 2], [1, 3, 2], [3,
    2, 1]]
```

Diferentes libros, diferentes autores, diferentes programas de computadora todos tienen ideas diferentes sobre el orden en que se deben escribir las permutaciones para componerlas. Este libro se basa en la idea tradicional de composición de funciones, de manera que fg es la composición $(fg)(x) = f(g(x))$ y es natural aplicar g primero. Sage toma el punto de vista opuesto y por fg, Sage entenderá que queremos hacer f primero. Ninguna de las dos postura es incorrecta y ninguna es necesariamente superior, son simplemente diferentes y hay buenas razones para preferir una o la otra. Cuando lea otros libros que trabajan con grupos de permutaciones, deberá determinar primero cuál es la elección utilizada. (Note que esta discusión sobre la composición de funciones en Sage, se limita a la composición de permutaciones, pues las funciones —"regulares", Sage las compone de la forma en que estamos acostumbrados.)

La traducción hecha acá entre el texto y Sage es una práctica valiosa. Reanudaremos la discusión al final de la Sección 3.1, pero revierta el orden de cada producto para calcular como lo haría Sage imitando lo que hace el texto.

```
mu1 = triangle([1,3,2])
mu2 = triangle([3,2,1])
mu3 = triangle([2,1,3])
rho1 = triangle([2,3,1])
product = rho1*mu1
product == mu2
```

```
True
```

```
[product(x) for x in triangle.domain()]
```

```
[3, 2, 1]
```

```
rho1*mu1 == mu1*rho1
```

```
False
```

```
mu1*rho1 == mu3
```

```
True
```

Ahora que entendemos que Sage calcula los productos al revés, podemos obtener la tabla de multiplicación para este grupo. El comportamiento por defecto es usar letras para referirse a los elementos de un grupo, `a, b, c, \dots{}` en el mismo orden que les daría el comando `.list()` al listar los elementos del grupo. Pero también es posible mostrar explícitamente los elementos en la tabla (con notación cíclica en este caso), puede darle los nombres que desee a los elementos. Usaremos `u` como abreviación de μ y `r` para ρ.

```
triangle.cayley_table()
```

```
*  a b c d e f
 +------------
a| a b c d e f
b| b a f e d c
c| c e d a f b
d| d f a c b e
e| e c b f a d
f| f d e b c a
```

```
triangle.cayley_table(names='elements')
```

```
      *       ()   (1,2) (1,2,3) (1,3,2)   (2,3)   (1,3)
       +-----------------------------------------------
     ()|       ()   (1,2) (1,2,3) (1,3,2)   (2,3)   (1,3)
  (1,2)|   (1,2)       ()   (1,3)   (2,3) (1,3,2) (1,2,3)
(1,2,3)| (1,2,3)   (2,3) (1,3,2)       ()   (1,3)   (1,2)
(1,3,2)| (1,3,2)   (1,3)       () (1,2,3)   (1,2)   (2,3)
  (2,3)|   (2,3) (1,2,3)   (1,2)   (1,3)       () (1,3,2)
  (1,3)|   (1,3) (1,3,2)   (2,3)   (1,2) (1,2,3)       ()
```

```
triangle.cayley_table(names=['id','u3','r1','r2','u1','u2'])
```

```
 *  id u3 r1 r2 u1 u2
  +------------------
id| id u3 r1 r2 u1 u2
u3| u3 id u2 u1 r2 r1
r1| r1 u1 r2 id u2 u3
r2| r2 u2 id r1 u3 u1
u1| u1 r1 u3 u2 id r2
u2| u2 r2 u1 u3 r1 id
```

Usted debiera verificar que esta tabla está correcta, así como la tabla en el Cuadro 3.7 está correcta. Recuerde que la convención es multiplicar la etiqueta de la columna por la de la fila, en ese orden. Pero, para hacer una verificación entre las tablas, deberá recordar la diferencia de orden entre el texto y Sage.

Cuaterniones

Sage implementa los cuaterniones, pero los elementos no son matrices, sino permutaciones. A pesar de las apariencias, la estructura es idéntica. No debería importar que versión tiene en mente (matrices o permutaciones) si construye la tabla de Cayley usando letras para etiquetar los elementos. Como permutaciones, o como letras, ¿puede identificar -1, I, J y K?

```
Q = QuaternionGroup()
[[a(x) for x in Q.domain()] for a in Q]
```

```
[[1, 2, 3, 4, 5, 6, 7, 8], [2, 3, 4, 1, 6, 7, 8, 5],
 [5, 8, 7, 6, 3, 2, 1, 4], [3, 4, 1, 2, 7, 8, 5, 6],
 [6, 5, 8, 7, 4, 3, 2, 1], [8, 7, 6, 5, 2, 1, 4, 3],
 [4, 1, 2, 3, 8, 5, 6, 7], [7, 6, 5, 8, 1, 4, 3, 2]]
```

```
Q.cayley_table()
```

```
*  a b c d e f g h
 +----------------
a| a b c d e f g h
b| b d f g c h a e
c| c e d h g b f a
d| d g h a f e b c
e| e h b f d a c g
f| f c g e a d h b
g| g a e b h c d f
h| h f a c b g e d
```

Debiera ser bastante obvio que `a` es el elemento identidad del grupo (1), ya sea por su comportamiento en la tabla, o por su representación de "fila inferior" como el primer elemento de la lista anterior. Y si lo prefiere, puede pedirle a Sage una lista de sus imágenes cuando es considerado como una función.

```
id = Q.identity()
[id(x) for x in Q.domain()]
```

```
[1, 2, 3, 4, 5, 6, 7, 8]
```

Ahora -1 debería tener la propiedad de que $-1 \cdot -1 = 1$. Vemos que el elemento identidad `a` está en la diagonal de la tabla de Cayley solo cuando calculamos `d*d`. Esto lo podemos verificar fácilmente, tomado la cuarta "fila inferior" de la lista anterior. Con esta información, una vez que hemos localizado I, podemos fácilmente calcular $-I$, y así sucesivamente.

```
minus_one = Q([3, 4, 1, 2, 7, 8, 5, 6])
minus_one*minus_one == Q.identity()
```

```
True
```

Vea si es capaz de identificar las letras con los ocho elementos de los cuaterniones. Tenga un poco de cuidado con los nombres que use, pues el símbolo `I` is es usado por Sage para el número imaginario $i = \sqrt{-1}$ (que utilizaremos más adelante), pero Sage le permitirá redefinirlo como cualquier cosa que quiera, sin una advertencia. Lo mismo vale para el uso de la `i` minúscula en Sage. De manera que mejor llame algo como `QI, QJ, QK` a los elementos de los cuaterniones para evitar confusión.

En la medida en que empezamos a trabajar con grupos, es instructivo trabajar con sus elementos. Pero muchas propiedades de los grupos son independientes del orden usado para la multiplicación, y de los nombres o representaciones que usemos para los elementos. Aquí mencionaremos algunos hechos sobre los cuaterniones que podemos calcular directamente sin tener información alguna sobre cómo se escriben los elementos o cómo se multiplican.

```
Q.is_finite()
```

```
True
```

```
Q.order()
```

```
8
```

```
Q.is_abelian()
```

```
False
```

Subgrupos

Las mejores técnicas para la creación de subgrupos vendrán en capítulos posteriores, pero ya ahora podemos crear algunos grupos que son naturalmente subgrupos de otros.

Los elementos de los cuaterniones fueron representados por ciertas permutaciones de los enteros del 1 al 8. Podemos también crear el grupo de *todas* las permutaciones de estos ocho enteros. Esto se hace bastante grande, así es que no los liste a menos que desee obtener una respuesta muy larga! (Lo desafío a hacerlo.)

```
S8 = SymmetricGroup(8)
a = S8.random_element()
[a(x) for x in S8.domain()]     # random
```

```
[5, 2, 6, 4, 1, 8, 3, 7]
```

```
S8.order()
```

```
40320
```

El grupo de los cuaterniones, `Q`, es un subgrupo del grupo de todas las permutaciones, el grupo simétrico S_8 o `S8`, y Sage considera esto como una propiedad de `Q`.

```
Q.is_subgroup(S8)
```

```
True
```

En Sage los números complejos se conocen por el nombre `CC`. Podemos crear una lista de los elementos en el subgrupodescrito en el Ejemplo 3.16. Podemos luego verificar que este conjunto es un subgrupo examinando la tabla de Cayley, usando la multiplicación como operación.

```
H = [CC(1), CC(-1), CC(I), CC(-I)]
CC.multiplication_table(elements=H,
                        names=['1', '-1', 'i', '-i'])
```

```
*   1 -1  i -i
  +------------
 1|  1 -1  i -i
-1| -1  1 -i  i
 i|  i -i -1  1
-i| -i  i  1 -1
```

3.8 Ejercicios en Sage

El objetivo de estos ejercicios es familiariarizarle con el trabajo con grupos en Sage. Las hojas de trabajo de Sage le permiten formar cuadros de textos con una extensa capacidad de formato, incluyendo la posibilidad de usar LaTeX para expresar matemáticas. De manera que si una pregunta requiere de una explicación o un comentario, cree una nueva celda y comuníquese claramente con su audiencia.

1. Cree los grupos `CyclicPermutationGroup(8)` y `DihedralGroup(4)` y nómbrelos `C` y `D`, respectivamente. Pronto entenderemos mejor esta construcciones, pero por ahora acepte que ambos objetos creados son de hecho grupos.

2. Verifique que `C` y `D` tienen el mismo tamaño usando el método `.order()`. Determine cuál de ellos es abeliano, y cuál no lo es, usando el método `.is_abelian()`.

3. Use el método `.cayley_table()` para crear la tabla de Cayley de cada grupo.

4. Escriba una discusión elegantemente formateada explicando las diferencias entre estos dos grupos que sean discernibles de las propiedades de sus tablas de Cayley. En otras palabras, ¿qué es *diferente* entre estos dos grupos que se pueda "ver" en las tablas de Cayley? (En notebook Sage, hacer Shift-click en una barra azúl producirá un mini-procesador de texto, y puede usar signos peso para insertar matemáticas usando LaTeX.)

5. Para `C` encuentre un subgrupo de orden 4. El grupo `D` tiene tres subgrupos de orden 4. Escoja uno de estos tres subgrupos de `D` que tenga una estructura diferente del obtenido en `C`.
El método `.subgroups()` le dará una lista de todos los subgrupos para ayudarle a comenzar. Una tabla de Cayley le ayudará a detectar la diferencia entre los dos subgrupos. ¿Qué propiedades de estas tablas le sirvieron para establecer la diferencia en la estructura de los subgrupos?

6. El método `.subgroup(elt_list)` construirá el menor subgrupo que contenga los elementos especificados del grupo, cuando estos son entregados como una lista `elt_list`. Use este comando para descubrir la menor lista de elementos necesaria para recrear los subgrupos encontrados en el ejercicios anterior. La comparación de igualdad `==`, puede ser usada para verificar si dos subgrupos son iguales.

4

Grupos Cíclicos

Los grupos $\mathbb{Z}$ y $\mathbb{Z}_n$, que están entre los grupos más familiares y fáciles de comprender, son ambos ejemplos de grupos cíclicos. En este capítulo estudiaremos las propiedades de grupos cíclicos y subgrupos cíclicos, los que juegan un papel clave en la clasificación de los grupos abelianos.

4.1 Subgrupos Cíclicos

Con frecuencia un subgrupo dependerá exclusivamente de un elemento de un grupo; es decir, el conocimiento de ese elemento en particular nos permitirá calcular cualquier elemento del subgrupo.

Ejemplo 4.1. Supongamos que escogemos $3 \in \mathbb{Z}$ y consideremos todos los múltiplos (tanto positivos como negativos) de 3. Como conjunto, tenemos

$$3\mathbb{Z} = \{\ldots, -3, 0, 3, 6, \ldots\}.$$

Es fácil ver que $3\mathbb{Z}$ es un subgrupo de los enteros. Este subgrupo está completamente determinado por el elemento 3 pues podemos obtener todos los otros elementos del grupo tomando los múltiplos de 3. Todo elemento en el subgrupo es "generado" por 3.

Ejemplo 4.2. Si $H = \{2^n : n \in \mathbb{Z}\}$, entonces H es un subgrupo del grupo multiplicativo de los números racionales no nulos, $\mathbb{Q}^*$. Si $a = 2^m$ y $b = 2^n$ están en H, entonces $ab^{-1} = 2^m 2^{-n} = 2^{m-n}$ también está en H. Por la Proposición 3.31, H es un subgrupo de $\mathbb{Q}^*$ determinada por el elemento 2.

Teorema 4.3. *Sea G un grupo y sea a un elemento en G. Entonces el conjunto*

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

es un subgrupo de G. Más aún, $\langle a \rangle$ es el menor subgrupo de G que contiene a a.

Demostración. La identidad está en $\langle a \rangle$ pues $a^0 = e$. Si g y h son dos elementos cualquiera en $\langle a \rangle$, entonces por la definición de $\langle a \rangle$ podemos escribir $g = a^m$ y $h = a^n$ con m y n enteros. Así $gh = a^m a^n = a^{m+n}$ está nuevamente en $\langle a \rangle$. Finalmente, si $g = a^n$ está en $\langle a \rangle$, entonces el inverso $g^{-1} = a^{-n}$ también está en $\langle a \rangle$. Claramente, cualquier subgrupo H de G que contenga a debe contener todas las potencias de a por clausura; luego, H contiene a $\langle a \rangle$. Por lo tanto, $\langle a \rangle$ es el menor subgrupo de G que contiene a a. □

Nota 4.4. Si usamos la notación "+", como en el caso de los enteros con la operación de suma, escribimos $\langle a \rangle = \{na : n \in \mathbb{Z}\}$.

Para $a \in G$, llamamos a $\langle a \rangle$ el ***subgrupo cíclico*** generado por a. Si G contiene algún elemento a tal que $G = \langle a \rangle$, entonces G es un ***grupo cíclico***. En ese caso a es un ***generador*** de G. Si a es un elemento de un grupo G, definimos el ***orden*** de a como el menor entero positivo n tal que $a^n = e$, y escribimos $|a| = n$. Si no hay tal entero n, decimos que el orden de a es infinito y escribimos $|a| = \infty$ para denotar el orden de a.

Ejemplo 4.5. Note que un grupo cíclico puede tener más que un generador. Tanto 1 como 5 generan $\mathbb{Z}_6$; por lo tanto, $\mathbb{Z}_6$ es un grupo cíclico. No todo elemento en un grupo cíclico es un generador del grupo. El orden de $2 \in \mathbb{Z}_6$ es 3. El subgrupo cíclico generado por 2 es $\langle 2 \rangle = \{0, 2, 4\}$.

Los grupos $\mathbb{Z}$ y $\mathbb{Z}_n$ son grupos cíclicos. Los elementos 1 y -1 son generadores para $\mathbb{Z}$. Siempre podemos generar $\mathbb{Z}_n$ con 1 pero puede haber otros generadores de $\mathbb{Z}_n$, como en el caso de $\mathbb{Z}_6$.

Ejemplo 4.6. El grupo de unidades, $U(9)$, en $\mathbb{Z}_9$ es un grupo cíclico. Como conjunto, $U(9)$ es $\{1, 2, 4, 5, 7, 8\}$. El elemento 2 es un generador para $U(9)$ pues

$$\begin{aligned} 2^1 &= 2 & 2^2 &= 4 \\ 2^3 &= 8 & 2^4 &= 7 \\ 2^5 &= 5 & 2^6 &= 1. \end{aligned}$$

Ejemplo 4.7. No todo grupo es un grupo cíclico. Considere el grupo de simetrías de un triángulo equilátero S_3. La tabla de multiplicación para este grupo es la Tabla 3.7. Los subgrupos de S_3 se muestran en la Figura 4.8. Note que todo subgrupo propio es cíclico; sin embargo, ningún elemento por si solo genera el grupo completo.

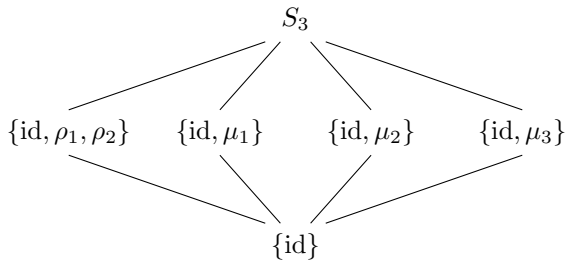


Figura 4.8: Subgrupos de S_3

Teorema 4.9. *Todo grupo cíclico es abeliano.*

Demostración. Sea G un grupo cíclico y sea $a \in G$ un generador para G. Si g y h están en G, entonces pueden ser escritos como potencias de a, digamos $g = a^r$ y $h = a^s$. Como

$$gh = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = hg,$$

G es abeliano. □

Subgrupos de Grupos Cíclicos

Podemos hacer algunas preguntas interesantes sobre subgrupos cíclicos de un grupo y sobre subgrupos de un grupo cíclico. Si G es un grupo, qué subgrupos de G son cíclicos? Si G es un grupo cíclico, que tipo de subgrupos tiene G?

Teorema 4.10. *Todo subgrupo de un grupo cíclico es cíclico.*

DEMOSTRACIÓN. Las principales herramientas usadas en esta demostración son el algoritmo de división y el principio del buen orden. Sea G un grupo cíclico generado por a y supongamos que H es un subgrupo de G. Si $H = \{e\}$, entonces H es cíclico trivialmente. Supongamos que H contiene algún otro elemento g distinto de la identidad. Entonces g puede ser escrito como a^n para algún entero n. Como H es un subgrupo, $g^{-1} = a^{-n}$ también debe estar en H. Como n o $-n$ es positivo, podemos suponer que H contiene potencias positivas de a y que $n > 0$. Sea m el menor número natural tal que $a^m \in H$. Tal m existe por por el principio del buen orden.

Afirmamos que $h = a^m$ es un generador para H. Debemos demostrar que todo $h' \in H$ puede ser escrito como una potencia de h. Como $h' \in H$ y H es un subgrupo de G, $h' = a^k$ para algún entero k. Usando el algoritmo de la división, podemos encontrar q y r tales que $k = mq + r$ con $0 \leq r < m$; luego,

$$a^k = a^{mq+r} = (a^m)^q a^r = h^q a^r.$$

Así $a^r = a^k h^{-q}$. Como a^k y h^{-q} están en H, a^r también debe estar en H. Pero m era el menor número positivo tal que a^m está en H; por lo tanto, $r = 0$ y $k = mq$. Luego,

$$h' = a^k = a^{mq} = h^q$$

y H está generado por h. □

Corolario 4.11. *Los subgrupos de $\mathbb{Z}$ son exactamente $n\mathbb{Z}$ con $n = 0, 1, 2, \ldots$.*

Proposición 4.12. *Sea G un grupo cíclico de orden n y supongamos que a es un generador para G. Entonces $a^k = e$ si y solo si n divide a k.*

DEMOSTRACIÓN. Supongamos primero que $a^k = e$. Por el algoritmo de la división, $k = nq + r$ con $0 \leq r < n$; luego,

$$e = a^k = a^{nq+r} = a^{nq} a^r = e a^r = a^r.$$

Como el menor entero m tal que $a^m = e$ es n, $r = 0$.

Recíprocamente, si n divide a k, entonces $k = ns$ para algún entero s. Por lo tanto,

$$a^k = a^{ns} = (a^n)^s = e^s = e.$$ □

Teorema 4.13. *Sea G un grupo cíclico de orden n y supongamos que $a \in G$ es un generador del grupo. Si $b = a^k$, entonces el orden de b es n/d, con $d = \text{mcd}(k, n)$.*

DEMOSTRACIÓN. Buscamos el menor entero positivo m tal que $e = b^m = a^{km}$. Por la Proposición 4.12, este es el menor entero positivo m tal que n divide a km o, equivalentemente, n/d divide a $m(k/d)$. Como d es el máximo común divisor de n y k, n/d y k/d son relativamente primos. Luego, para que n/d divida a $m(k/d)$ debe dividir a m. El menor tal m es n/d. □

Corolario 4.14. *Los generadores de $\mathbb{Z}_n$ son los enteros r tales que $1 \leq r < n$ y $\text{mcd}(r, n) = 1$.*

Ejemplo 4.15. Consideremos el grupo $\mathbb{Z}_{16}$. Los números 1, 3, 5, 7, 9, 11, 13, y 15 son los elementos de $\mathbb{Z}_{16}$ que son relativamente primos con 16. Cada uno de estos elementos genera $\mathbb{Z}_{16}$. Por ejemplo,

$$1 \cdot 9 = 9 \qquad 2 \cdot 9 = 2 \qquad 3 \cdot 9 = 11$$

$$\begin{array}{lll} 4 \cdot 9 = 4 & 5 \cdot 9 = 13 & 6 \cdot 9 = 6 \\ 7 \cdot 9 = 15 & 8 \cdot 9 = 8 & 9 \cdot 9 = 1 \\ 10 \cdot 9 = 10 & 11 \cdot 9 = 3 & 12 \cdot 9 = 12 \\ 13 \cdot 9 = 5 & 14 \cdot 9 = 14 & 15 \cdot 9 = 7. \end{array}$$

4.2 Grupo multiplicativo de los números complejos

Los ***números complejos*** están definidos como

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\},$$

con $i^2 = -1$. Si $z = a + bi$, entonces a es la ***parte real*** de z y b es la ***parte imaginaria*** de z.

Para sumar dos números complejos $z = a + bi$ y $w = c + di$, debemos simplemente sumar las partes reales y las imaginarias respectivamente:

$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i.$$

Recordando que $i^2 = -1$, podemos multiplicar los números complejos como si fueran polinomios. El producto de z y w es

$$(a + bi)(c + di) = ac + bdi^2 + adi + bci = (ac - bd) + (ad + bc)i.$$

Todo número complejo no nulo $z = a + bi$ tiene un inverso multiplicativo; es decir, existe un $z^{-1} \in \mathbb{C}^*$ tal que $zz^{-1} = z^{-1}z = 1$. Si $z = a + bi$, entonces

$$z^{-1} = \frac{a - bi}{a^2 + b^2}.$$

El ***conjugado*** de un número complejo $z = a + bi$ se define como $\overline{z} = a - bi$. El ***valor absoluto*** o ***módulo*** de $z = a + bi$ es $|z| = \sqrt{a^2 + b^2}$.

Ejemplo 4.16. Sean $z = 2 + 3i$ y $w = 1 - 2i$. Entonces

$$z + w = (2 + 3i) + (1 - 2i) = 3 + i$$

y

$$zw = (2 + 3i)(1 - 2i) = 8 - i.$$

Además,

$$\begin{aligned} z^{-1} &= \frac{2}{13} - \frac{3}{13}i \\ |z| &= \sqrt{13} \\ \overline{z} &= 2 - 3i. \end{aligned}$$

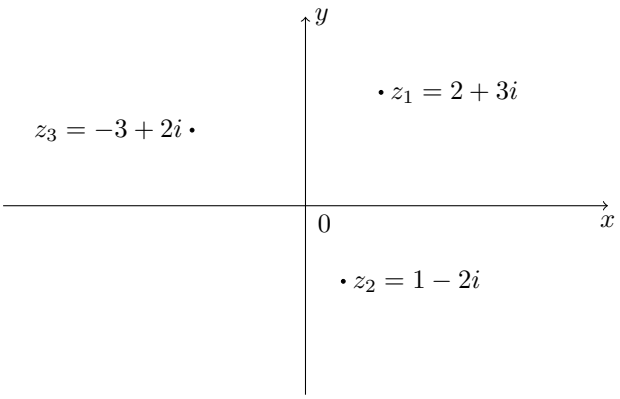


Figura 4.17: Coordenadas cartesianas de un número complejo

Existen varias formas de representar gráficamente a los números complejos. Podemos representar un número complejo $z = a + bi$ como un par ordenado en el plano xy donde a es la coordenada x (o real) y b coordenada y y (o imaginaria). Esta se llama representación ***rectangular*** o ***cartesiana*** . Las representaciones cartesianas de $z_1 = 2 + 3i$, $z_2 = 1 - 2i$, y $z_3 = -3 + 2i$ se ilustran en la Figura 4.17.

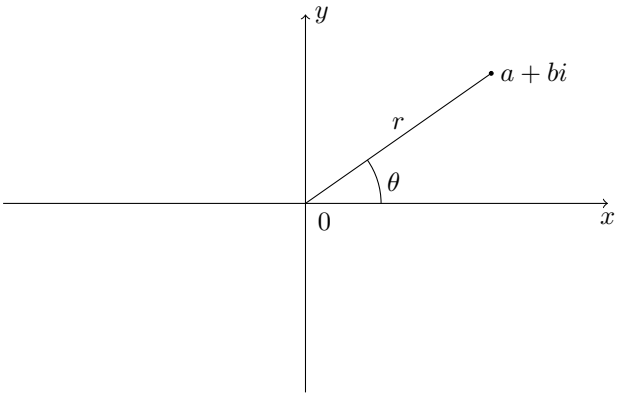


Figura 4.18: Coordenadas polares de un número complejo

Número complejos no nulos se pueden representar también con sus ***coordenadas polares***. Para especificar un punto no cero en el plano, basta con dar un ángulo θ desde el eje x positivo en dirección antihoraria y una distancia r desde el origen, como en la Figura 4.18. Podemos ver que

$$z = a + bi = r(\cos\theta + i\sin\theta).$$

Luego,

$$r = |z| = \sqrt{a^2 + b^2}$$

y

$$a = r\cos\theta$$
$$b = r\sin\theta.$$

A veces abreviarems $r(\cos\theta + i\sin\theta)$ as $r\,\mathrm{cis}\,\theta$. Para garantizar que la representación de z esté bien definida, también pediremos que $0° \leq \theta < 360°$. Si la medida está en radianes, entonces $0 \leq \theta < 2\pi$.

Ejemplo 4.19. Supongamos que $z = 2\operatorname{cis}60°$. Entonces

$$a = 2\cos 60° = 1$$

y

$$b = 2\sin 60° = \sqrt{3}.$$

Luego, la representación cartesiana es $z = 1 + \sqrt{3}\,i$.

Recíprocamente, si no entregan la representación cartesiana de un número complejo, puede ser útil conocer su representación polar. Si $z = 3\sqrt{2} - 3\sqrt{2}\,i$, entonces

$$r = \sqrt{a^2 + b^2} = \sqrt{36} = 6$$

y

$$\theta = \arctan\left(\frac{b}{a}\right) = \arctan(-1) = 315°,$$

aí $3\sqrt{2} - 3\sqrt{2}\,i = 6\operatorname{cis}315°$.

La representación polar de un número complejo facilita el cálculo de productos y potencias de números complejos. La demostración de la siguiente proposición es directa y la dejamos como ejercicio.

Proposición 4.20. *Sean $z = r\operatorname{cis}\theta$ y $w = s\operatorname{cis}\phi$ dos números complejos. Entonces*

$$zw = rs\operatorname{cis}(\theta + \phi).$$

Ejemplo 4.21. Si $z = 3\operatorname{cis}(\pi/3)$ y $w = 2\operatorname{cis}(\pi/6)$, entonces $zw = 6\operatorname{cis}(\pi/2) = 6i$.

Teorema 4.22 (DeMoivre)**.** *Sea $z = r\operatorname{cis}\theta$ un número complejo distinto de cero. Entonces*

$$[r\operatorname{cis}\theta]^n = r^n\operatorname{cis}(n\theta)$$

para $n = 1, 2, \ldots$.

Demostración. Procederemos por inducción en n. Para $n = 1$ el teorema es trivial. Supongamos que el teorema es verdadero para todo k tal que $1 \leq k \leq n$. Entonces

$$\begin{aligned}
z^{n+1} &= z^n z \\
&= r^n(\cos n\theta + i\sin n\theta)r(\cos\theta + i\sin\theta) \\
&= r^{n+1}[(\cos n\theta\cos\theta - \sin n\theta\sin\theta) + i(\sin n\theta\cos\theta + \cos n\theta\sin\theta)] \\
&= r^{n+1}[\cos(n\theta + \theta) + i\sin(n\theta + \theta)] \\
&= r^{n+1}[\cos(n+1)\theta + i\sin(n+1)\theta].
\end{aligned}$$

□

Ejemplo 4.23. Supongamos que $z = 1 + i$ y queremos calcular z^{10}. En lugar de calcular $(1 + i)^{10}$ directamente, es mucho más fácil pasar a coordenadas polares y calcular z^{10} usando el Teorema de DeMoivre:

$$\begin{aligned}
z^{10} &= (1 + i)^{10} \\
&= \left(\sqrt{2}\operatorname{cis}\left(\frac{\pi}{4}\right)\right)^{10} \\
&= (\sqrt{2}\,)^{10}\operatorname{cis}\left(\frac{5\pi}{2}\right) \\
&= 32\operatorname{cis}\left(\frac{\pi}{2}\right) \\
&= 32i.
\end{aligned}$$

El grupo de la circunferencia y las raíces de la unidad

El grupo multiplicativo de los números complejos, $\mathbb{C}^*$, posee algunos subgrupos interesantes. Mientras $\mathbb{Q}^*$ y $\mathbb{R}^*$ no tienen subgrupos interesantes de orden finito, $\mathbb{C}^*$ tiene muchos. Consideremos primero el ***grupo de la circunferencia***,

$$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}.$$

La siguiente proposición es consecuencia directa de la Proposición 4.20.

Proposición 4.24. *El grupo de la circunferencia es un subgrupo de* $\mathbb{C}^*$.

Si bien el grupo de la circunferencia tiene orden infinito, tiene muchos subgrupos finitos interesantes. Supongamos que $H = \{1, -1, i, -i\}$. Entonces H es un subgrupo del grupo de la circunferencia. También, 1, -1, i, y $-i$ son precisamente los números complejos que satisfacen la ecuación $z^4 = 1$. Los números comlejos que satisfacen la ecuación $z^n = 1$ se llaman raíces ***n-ésimas de la unidad***.

Teorema 4.25. *Si $z^n = 1$, entonces las raíces n-ésima de uno son*

$$z = \operatorname{cis}\left(\frac{2k\pi}{n}\right),$$

con $k = 0, 1, \ldots, n-1$. Más aún, la raíces n-ésimas de uno forman un subgrupo cíclico de $\mathbb{T}$ de orden n

Demostración. Por el Teorema de DeMoivre's,

$$z^n = \operatorname{cis}\left(n\frac{2k\pi}{n}\right) = \operatorname{cis}(2k\pi) = 1.$$

Las z's son distintas entre sí pues los números $2k\pi/n$ son todos distintos y mayores o iguales a 0 pero menores que 2π. El hecho de que estas sean todas las raíces de la ecuación $z^n = 1$ es consecuencia del Corolario 17.9, que dice que un polinomio de grado n puede tener a lo más n raíces. Dejaremos al lector la demostración de que las raíces n-ésimas de uno forman un subgrupo cíclico de $\mathbb{T}$. □

Un generador para el grupo de las raíces n-ésimas de unno se llama ***raíz n-ésima primitiva de la unidad***.

Ejemplo 4.26. Las raíces octavas de la unidad se pueden representar como ocho puntos equidistantes en el círculo unitario (Figura 4.27). Las raíces octavas primitivas de la unidad son

$$\begin{aligned}
\omega &= \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\
\omega^3 &= -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\
\omega^5 &= -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \\
\omega^7 &= \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i.
\end{aligned}$$

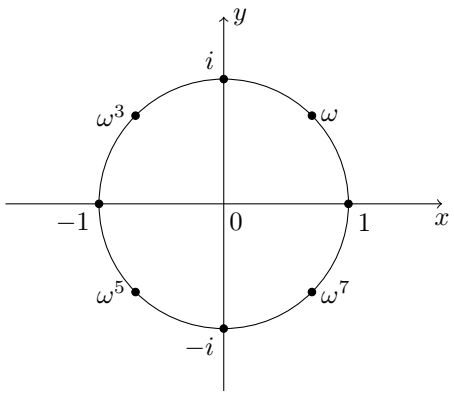


Figura 4.27: Raíces octavas de la unidad

4.3 El método de los cuadrados repetidos

Calcular potencias grandes puede tomar mucho tiempo. Así como cualquiera puede calcular 2^2 o 2^8, cualquiera sabe como calcular

$$2^{2^{1000000}}.$$

Sin embargo, tales número son tan grandes que no quisiéramos siquiera intentar hacer los cálculos; Más aún, después de cierto punto, el cálculo no sería realizable aunque tuviéramos a nuestra disposición todos los computadores del mundo. Incluso escribir la representación decimal de un número demasiado grande puede no ser práctico. Podría tener miles o incluso millones de dígitos. Sin embargo, si pudiéramos calcular algo como

$$2^{37398332} \pmod{46389},$$

podríamos fácilmente escribir el resultado pues sería un número entre 0 y 46,388. Si queremos calcular potencias módulo n rápida y eficientemente, deberemos ser astutos.[1]

Lo primero que debemos notar es que cualquier número a se puede escribir como una suma de potencias de 2 distintas; es decir, podemos escribir

$$a = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_n},$$

con $k_1 < k_2 < \cdots < k_n$. Esto es simplemente la representación binaria de a. Por ejemplo, la representación binaria de 57 es 111001, pues $57 = 2^0 + 2^3 + 2^4 + 2^5$.

La reglas de los exponentes se cumplen en $\mathbb{Z}_n$; es decir, si $b \equiv a^x \pmod{n}$ y $c \equiv a^y \pmod{n}$, entonces $bc \equiv a^{x+y} \pmod{n}$. Podemos calcular $a^{2^k} \pmod{n}$ en k pasos calculando

$$\begin{aligned} &a^{2^0} \pmod{n} \\ &a^{2^1} \pmod{n} \\ &\vdots \\ &a^{2^k} \pmod{n}. \end{aligned}$$

Cada paso corresponde a elevar al cuadrado el resultado obtenido en el paso anterior, dividir por n, y dejar el resto.

[1] Los resultados de esta sección solo serán necesarios en el Capítulo 7

Ejemplo 4.28. Calcularemos $271^{321} \pmod{481}$. Note que

$$321 = 2^0 + 2^6 + 2^8;$$

luego, calcular $271^{321} \pmod{481}$ es lo mismo que calcular

$$271^{2^0+2^6+2^8} \equiv 271^{2^0} \cdot 271^{2^6} \cdot 271^{2^8} \pmod{481}.$$

Será suficiente con calcular $271^{2^i} \pmod{481}$ con $i = 0, 6, 8$. Es muy fácil ver que

$$271^{2^1} = 73{,}441 \equiv 329 \pmod{481}.$$

Podemos elevar al cuadrado este resultado, obteniéndo un valor para $271^{2^2} \pmod{481}$:

$$\begin{aligned} 271^{2^2} &\equiv (271^{2^1})^2 \pmod{481} \\ &\equiv (329)^2 \pmod{481} \\ &\equiv 108{,}241 \pmod{481} \\ &\equiv 16 \pmod{481}. \end{aligned}$$

Estamos usando el hecho que $(a^{2^n})^2 \equiv a^{2\cdot 2^n} \equiv a^{2^{n+1}} \pmod{n}$. Continuando, podemos calcular

$$271^{2^6} \equiv 419 \pmod{481}$$

y

$$271^{2^8} \equiv 16 \pmod{481}.$$

Por lo tanto,

$$\begin{aligned} 271^{321} &\equiv 271^{2^0+2^6+2^8} \pmod{481} \\ &\equiv 271^{2^0} \cdot 271^{2^6} \cdot 271^{2^8} \pmod{481} \\ &\equiv 271 \cdot 419 \cdot 16 \pmod{481} \\ &\equiv 1{,}816{,}784 \pmod{481} \\ &\equiv 47 \pmod{481}. \end{aligned}$$

El método de los cuadrado repretido resultará ser una herramienta muy útil cuando exploremos la criptografía RSA en el Capítulo 7. Para codificar y decodificar mensaje de forma razonable, será necesario poder calcular grandes potencia de enteros mód n de forma rápida.

Sage La implementación de los grupos cíclicos en Sage es algo débil — pero igual podemos hacer uso provechoso de Sage y quizás esta situación cambie pronto.

4.4 Ejercicios

1. Demuestre o refute cada una de las siguientes proposiciones.

(a) Todos los generadores de $\mathbb{Z}_{60}$ son primos.

(b) $U(8)$ es cíclico.

(c) $\mathbb{Q}$ es cíclico.

(d) Si todo subgrupo propio de un grupo G es cíclico, entonces G es un grupo cíclico.

(e) Un grupo con un número finito de subgrupos es finito.

2. Encuentre el orden de cada uno de los siguientes elementos.

(a) $5 \in \mathbb{Z}_{12}$
(b) $\sqrt{3} \in \mathbb{R}$
(c) $\sqrt{3} \in \mathbb{R}^*$
(d) $-i \in \mathbb{C}^*$
(e) 72 in $\mathbb{Z}_{240}$
(f) 312 in $\mathbb{Z}_{471}$

3. Liste todos los elementos en cada uno de los siguientes subgrupos.

(a) El subgrupo de $\mathbb{Z}$ generado por 7
(b) El subgrupo de $\mathbb{Z}_{24}$ generado por 15
(c) Todos los subgrupos de $\mathbb{Z}_{12}$
(d) Todos los subgrupos de $\mathbb{Z}_{60}$
(e) Todos los subgrupos de $\mathbb{Z}_{13}$
(f) Todos los subgrupos de $\mathbb{Z}_{48}$
(g) El subgrupo generado por 3 en $U(20)$
(h) El subgrupo generado por 5 en $U(18)$
(i) El subgrupo de $\mathbb{R}^*$ generado por 7
(j) El subgrupo de $\mathbb{C}^*$ generado por i con $i^2 = -1$
(k) El subgrupo de $\mathbb{C}^*$ generado por $2i$
(l) El subgrupo de $\mathbb{C}^*$ generado por $(1+i)/\sqrt{2}$
(m) El subgrupo de $\mathbb{C}^*$ generado por $(1+\sqrt{3}\,i)/2$

4. Encuentre los subgrupos de $GL_2(\mathbb{R})$ generados por cada una de la siguientes matrices.

(a) $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
(b) $\begin{pmatrix} 0 & 1/3 \\ 3 & 0 \end{pmatrix}$
(c) $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$
(d) $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$
(e) $\begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}$
(f) $\begin{pmatrix} \sqrt{3}/2 & 1/2 \\ -1/2 & \sqrt{3}/2 \end{pmatrix}$

5. Encuentre el orden de cada elemento en $\mathbb{Z}_{18}$.

6. Encuentre el orden de cada elemento en el grupo de simetrías del cuadrado, D_4.

7. ¿Cuáles son todos los subgrupos cíclicos del grupo de los cuaterniones, Q_8?

8. Liste todos los subgrupos cíclicos de $U(30)$.

9. Liste todos los generadores de cada subgrupo de orden 8 en $\mathbb{Z}_{32}$.

10. Encuentre todos los elementos de orden finito en cada uno de los siguientes grupos. Acá el "$*$" indica el conjunto sin el cero.

(a) $\mathbb{Z}$
(b) $\mathbb{Q}^*$
(c) $\mathbb{R}^*$

11. Si $a^{24} = e$ en un grupo G, ¿cuáles son los posibles órdenes de a?

12. Encuentre un grupo cíclico con exactamente un generador. ¿Puede encontrar grupos cíclicos con exactamente dos generadores? ¿Cuatro generadores? ¿Con exactamente n generadores?

13. Para $n \leq 20$, ¿cuáles grupos $U(n)$ son cíclicos? Conjeture qué se cumple en general. ¿Puede demostrar su conjetura?

14. Sean

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

elementos en $GL_2(\mathbb{R})$. Muestre que A y B tienen orden finito pero que AB tiene orden infinito.

15. Evalúe.

(a) $(3-2i)+(5i-6)$
(b) $(4-5i)-\overline{(4i-4)}$
(c) $(5-4i)(7+2i)$
(d) $(9-i)\overline{(9-i)}$
(e) i^{45}
(f) $(1+i)+\overline{(1+i)}$

16. Convierta los siguientes números complejos a la forma $a+bi$.

(a) $2\,\mathrm{cis}(\pi/6)$
(b) $5\,\mathrm{cis}(9\pi/4)$
(c) $3\,\mathrm{cis}(\pi)$
(d) $\mathrm{cis}(7\pi/4)/2$

17. Escriba la representación polar de los siguientes números complejos.

(a) $1-i$
(b) -5
(c) $2+2i$
(d) $\sqrt{3}+i$
(e) $-3i$
(f) $2i+2\sqrt{3}$

18. Calcule cada una de las siguientes expresiones.

(a) $(1+i)^{-1}$
(b) $(1-i)^6$
(c) $(\sqrt{3}+i)^5$
(d) $(-i)^{10}$
(e) $((1-i)/2)^4$
(f) $(-\sqrt{2}-\sqrt{2}\,i)^{12}$
(g) $(-2+2i)^{-5}$

19. Demuestre cada una de las siguientes proposiciones.

(a) $|z| = |\overline{z}|$
(b) $z\overline{z} = |z|^2$
(c) $z^{-1} = \overline{z}/|z|^2$
(d) $|z+w| \leq |z|+|w|$
(e) $|z-w| \geq ||z|-|w||$
(f) $|zw| = |z||w|$

20. Liste y grafique las raíces sextas de la unidad. ¿Cuáles son los generadores de este grupo? ¿Cuáles son las raíces sextas primitivas de la unidad?

21. Liste y grafique las raíces quintas de la unidad. ¿Cuáles son los generadores de este grupo? ¿Cuáles son las raíces quintas primitivas de la unidad?

22. Calcule cada uno de los siguientes.

(a) $292^{3171} \pmod{582}$
(b) $2557^{341} \pmod{5681}$
(c) $2071^{9521} \pmod{4724}$
(d) $971^{321} \pmod{765}$

23. Sean $a, b \in G$. Demuestre las siguientes proposiciones.

(a) El orden de a es el mismo que el orden de a^{-1}.

(b) Para todo $g \in G$, $|a| = |g^{-1}ag|$.

(c) El orden de ab es el mismo que el orden de ba.

24. Sean p y q primos distintos. ¿Cuántos generadores tiene $\mathbb{Z}_{pq}$?

25. Sea p primo y r un entero positivo. ¿Cuántos generadores tiene $\mathbb{Z}_{p^r}$?

26. Demuestre que $\mathbb{Z}_p$ no tiene subgrupos propios no triviales si p es primo.

27. Si g y h tienen orden 15 y 16 respectivamente en un grupo G, ¿Cuál es el orden de $\langle g \rangle \cap \langle h \rangle$?

28. Sea a un elemento en un grupo G. ¿Qué elemento genera el subgrupo $\langle a^m \rangle \cap \langle a^n \rangle$?

29. Demuestre que $\mathbb{Z}_n$ tiene un número par de generadores para $n > 2$.

30. Supongamos que G es un grupo y sean $a, b \in G$. Demuestre que si $|a| = m$ y $|b| = n$ con $\text{mcd}(m, n) = 1$, entonces $\langle a \rangle \cap \langle b \rangle = \{e\}$.

31. Sea G un grupo abeliano. Demuestre que los elementos de orden finito en G forman un subgrupo. Este subgrupo se llama ***subgrupo de torsión*** de G.

32. Sea G un grupo cíclico finito de orden n generado por x. Muestre que si $y = x^k$ con $\text{mcd}(k, n) = 1$, entonces y también es un generador de G.

33. Si G es un grupo abeliano que contiene dos subgrupos cíclicos de orden 2, muestre que G debe contener un subgrupo de orden 4. ¿Es necesariamente cíclico este subgrupo?

34. Sea G un grupo abeliano de orden pq con $\text{mcd}(p, q) = 1$. Si G contiene elementos a y b de orden p y q respectivamente, entonces demuestre que G es cíclico.

35. Demuestre que los subgrupos de $\mathbb{Z}$ son exactamente $n\mathbb{Z}$ para $n = 0, 1, 2, \ldots$.

36. Demuestre que los generadores de $\mathbb{Z}_n$ son los enteros r tales que $1 \leq r < n$ y $\text{mcd}(r, n) = 1$.

37. Demuestre que si G no tiene subgrupos propios no triviales, entonces G es un grupo cíclico.

38. Demuestre que el orden de un elemento en un grupo cíclico finito G debe dividir el orden del grupo.

39. Demuestre que si G es un grupo cíclico de orden m y $d \mid m$, entonces G tiene un subgrupo de orden d.

40. ¿Para qué enteros n es -1 una raíz n-ésima de la unidad?

41. Si $z = r(\cos\theta + i\sin\theta)$ y $w = s(\cos\phi + i\sin\phi)$ son dos números complejos no nulos, muestre que

$$zw = rs[\cos(\theta + \phi) + i\sin(\theta + \phi)].$$

42. Demuestre que el grupo de la circunferencia es un subgrupo de $\mathbb{C}^*$.

43. Demuestre que las raíces n-ésimas de la unidad forman un subgrupo cíclico de $\mathbb{T}$ de orden n.

44. Sea $\alpha \in \mathbb{T}$. Demuestre que $\alpha^m = 1$ y $\alpha^n = 1$ si y solo si $\alpha^d = 1$ para $d = \text{mcd}(m, n)$.

45. Sea $z \in \mathbb{C}^*$. Si $|z| \neq 1$, demuestre que el orden de z es infinito.

46. Sea $z = \cos\theta + i \sin\theta$ en $\mathbb{T}$ con $\theta \in \mathbb{Q}$. Demuestre que el orden de z es infinito.

4.5 Ejercicios de programación

1. Escriba un programa que escriba cualquier número entero como suma de potencias distintas de 2. ¿Cuál es el mayor entero para el que funciona su programa?

2. Escriba un programa para calcular $a^x \pmod{n}$ con el método de los cuadrados repetidos. ¿Cuáles son los mayores valores de n y x aceptados por su programa?

4.6 Referencias y Lecturas recomendadas

[1] Koblitz, N. *A Course in Number Theory y Cryptography.* 2nd ed. Springer, New York, 1994.

[2] Pomerance, C. "Cryptology y Computational Number Theory—An Introduction," in *Cryptology y Computational Number Theory*, Pomerance, C., ed. Proceedings of Symposia in Applied Mathematics, vol. 42, American Mathematical Society, Providence, RI, 1990. This book gives an excellent account of how the method of repeated squares is used in cryptography.

4.7 Sage

Los grupos cíclicos son muy importantes, así es que no es una sorpresa que aparezcan en diferentes formas en Sage. Cada una de estas es ligeramente diferente, y ninguna de ellas es ideal para una introducción, pero juntas pueden ilustrar la mayor parte de las ideas importantes. Aquí hay una guía a las diferentes formas de construir, y estudiar, un grupo cíclico en Sage.

Grupos Cíclicos de Orden Infinito

En Sage, los enteros $\mathbb{Z}$ se construyen con `ZZ`. Para construir un grupo cíclico infinito tal como $3\mathbb{Z}$ del Ejemplo 4.1, simplemente use `3*ZZ`. Como conjunto infinito, no es mucho lo que se pueda hacer con esto. Se puede determinar si un entero está en el conjunto o no. También es posible recuperar el generador con el comando `.gen()`.

```
G = 3*ZZ
-12 in G
```

```
True
```

```
37 in G
```

```
False
```

```
G.gen()
```

```
3
```

Grupos Cíclicos Aditivos

El grupo cíclico aditivo $\mathbb{Z}_n$ se puede construir como un caso especial de una construcción más general en Sage. Primer definimos $\mathbb{Z}_{14}$ y capturamos su generador. En lo que sigue, preste especial atención al uso de paréntesis y corchetes para cuando realice sus propios ensayos.

```
G = AdditiveAbelianGroup([14])
G.order()
```

```
14
```

```
G.list()
```

```
[(0), (1), (2), (3), (4), (5), (6), (7),
 (8), (9), (10), (11), (12), (13)]
```

```
a = G.gen(0)
a
```

```
(1)
```

Se puede calcular en este grupo, usando el generador, usando elementos nuevos obtenidos de coercionar enteros a pertenecer al grupo, o tomando el resultado de operaciones con otros elementos. Podemos obtener el orden de los elementos en este grupo. Note que podemos abreviar la suma repetida de elementos usando la multiplicación de un elemento por un número entero.

```
a + a
```

```
(2)
```

```
a + a + a + a
```

```
(4)
```

```
4*a
```

```
(4)
```

```
37*a
```

```
(9)
```

Podemos crear, y después calcular con, elementos del grupo obtenidos a partir de la coerción de un entero (en una lista de largo 1) al grupo. Es posible que obtenga una advertencia `DeprecationWarning` la primera vez que use esta sintaxis para crear un nuevo elemento. Esta misteriosa advertencia puede ser ignorada sin problemas.

```
G([2])
```

```
doctest:...: DeprecationWarning: The default behaviour
    changed! If you
*really* want a linear combination of smith generators, use
.linear_combination_of_smith_form_gens.
See http://trac.sagemath.org/16261 for details.
(2)
```

```
b = G([2]); b
```

```
(2)
```

```
b + b
```

```
(4)
```

```
2*b == 4*a
```

```
True
```

```
7*b
```

```
(0)
```

```
b.order()
```

```
7
```

```
c = a - 6*b; c
```

```
(3)
```

```
c + c + c + c
```

```
(12)
```

```
c.order()
```

```
14
```

Es posible crear subgrupos cíclicos, a partir de un elemento designado como nuevo generador. Desafortunadamente, hacer esto requiere usar el método `.submodule()` (que debiera ser renombrado en Sage).

```
H = G.submodule([b]); H
```

```
Additive abelian group isomorphic to Z/7
```

```
H.list()
```

```
[(0), (2), (4), (6), (8), (10), (12)]
```

```
H.order()
```

```
7
```

```
e = H.gen(0); e
```

```
(2)
```

```
3*e
```

```
(6)
```

```
e.order()
```

```
7
```

El subgrupo cíclico `H` recién creado tiene más de un generador. Podemos verificar esto construyendo un nuevo subgrupo y comparando ambos subgrupos.

```
f = 12*a; f
```

```
(12)
```

```
f.order()
```

```
7
```

```
K = G.submodule([f]); K
```

```
Additive abelian group isomorphic to Z/7
```

```
K.order()
```

```
7
```

```
K.list()
```

```
[(0), (2), (4), (6), (8), (10), (12)]
```

```
K.gen(0)
```

```
(2)
```

```
H == K
```

```
True
```

Ciertamente la lista de elementos, y el generador común `(2)` nos hacen pensar que `H` y `K` son el mismo, pero la comparación en la última línea no deja lugar a dudas.

Los resultados en en esta sección, especialmente el Teorema 4.13 y el Corolario 4.14, pueden ser investigados creando generadores de subgrupos a partir de un generador de un grupo cíclico aditivo, creando los subgrupos, y calculando los órdenes tanto de los elementos como de los grupos.

Grupos Multiplicativos Abstractos

Podemos crear un grupo cíclico abstracto al estilo de los Teoremas 4.3, 4.9, 4.10. En la sintaxis que sigue `a` es un nombre para el generador, y `14` es el orden del elemento. Note que la notación es ahora multiplicativa, así es que multiplicamos los elementos, y los productos repetidos pueden ser escritos como potencias.

```
G.<a> = AbelianGroup([14])
G.order()
```

```
14
```

```
G.list()
```

```
(1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^10, a^11,
    a^12, a^13)
```

```
a.order()
```

```
14
```

Los cálculos en el grupo son similares a como eran antes, solo con una notación diferente. Ahora son productos, con productos repetidos escritos como potencias.

```
b = a^2
b.order()
```

```
7
```

```
b*b*b
```

```
a^6
```

```
c = a^7
c.order()
```

```
2
```

```
c^2
```

```
1
```

```
b*c
```

```
a^9
```

```
b^37*c^42
```

```
a^4
```

Subgrupos se pueden formar con el comando `.subgroup()`. Pero no intente listar los elementos del subgrupo, se verán algo extraños. Tampoco está implementada la comparación de subgrupos.

```
H = G.subgroup([a^2])
H.order()
```

```
7
```

```
K = G.subgroup([a^12])
K.order()
```

```
7
```

```
L = G.subgroup([a^4])
H == L
```

```
False
```

Una ventaja de esta implementación es la posibilidad de crear todos los posibles subgrupos. Acá crearemos la lista de subgrupos, extraemos uno en particular (el tercero) y obtenemos su orden.

```
allsg = G.subgroups(); allsg
```

```
[Multiplicative Abelian subgroup isomorphic to C2 x C7
    generated by {a},
 Multiplicative Abelian subgroup isomorphic to C7 generated
     by {a^2},
 Multiplicative Abelian subgroup isomorphic to C2 generated
     by {a^7},
 Trivial Abelian subgroup]
```

```
sub = allsg[2]
sub.order()
```

```
2
```

Grupos Cíclicos de Permutaciones

Aprenderemos más sobre los grupos de permutaciones en el siguiente capítulo. Pero acá mencionaremos que es fácil crear grupos cíclicos como grupos de permutaciones, y diversos métodos para trabajar con ellos están disponibles, aunque los elementos en sí se tornan algo incómodos para trabajar. Tal como antes, observemos que la notación es multiplicativa.

```
G=CyclicPermutationGroup(14)
a = G.gen(0); a
```

```
(1,2,3,4,5,6,7,8,9,10,11,12,13,14)
```

```
b = a^2
b = a^2; b
```

```
(1,3,5,7,9,11,13)(2,4,6,8,10,12,14)
```

```
b.order()
```

```
7
```

```
a*a*b*b*b
```

```
(1,9,3,11,5,13,7)(2,10,4,12,6,14,8)
```

```
c = a^37*b^26; c
```

```
(1,6,11,2,7,12,3,8,13,4,9,14,5,10)
```

```
c.order()
```

```
14
```

Podemos crear subgrupos, obtener sus órdenes, y listar sus elementos.

```
H = G.subgroup([a^2])
H.order()
```

```
7
```

```
H.gen(0)
```

```
(1,3,5,7,9,11,13)(2,4,6,8,10,12,14)
```

```
H.list()
```

```
[(),
 (1,3,5,7,9,11,13)(2,4,6,8,10,12,14),
 (1,5,9,13,3,7,11)(2,6,10,14,4,8,12),
 (1,7,13,5,11,3,9)(2,8,14,6,12,4,10),
 (1,9,3,11,5,13,7)(2,10,4,12,6,14,8),
 (1,11,7,3,13,9,5)(2,12,8,4,14,10,6),
 (1,13,11,9,7,5,3)(2,14,12,10,8,6,4)]
```

Puede ser de ayuda visualizar este grupo, y el subgrupo, como rotaciones de un dodecágono regular con vértices etiquetados con los enteros del 1 al 12. Este no es el grupo completo de simetrías, pues no incluye las reflexiones, solamente las 12 rotaciones.

Tablas de Cayley

Como grupos, cada uno de los ejemplos anteriores (grupos y subgrupos) tienen implementadas sus tablas de Cayley en Sage. Como los grupos son cíclicos, y por ende también lo son sus subgrupos, las tablas de Cayley deberían seguir un patrón similarmente "cíclico". Note que las letras usadas en la tabla obtenida por defecto son genéricas, y no están relacionadas a las letras usadas antes para elementos específicos — solo corresponden a los elementos del grupo en el orden dado por `.list()`.

```
G.<a> = AbelianGroup([14])
G.cayley_table()
```

```
*  a b c d e f g h i j k l m n
 +----------------------------
a| a b c d e f g h i j k l m n
b| b c d e f g h i j k l m n a
c| c d e f g h i j k l m n a b
d| d e f g h i j k l m n a b c
e| e f g h i j k l m n a b c d
f| f g h i j k l m n a b c d e
g| g h i j k l m n a b c d e f
h| h i j k l m n a b c d e f g
i| i j k l m n a b c d e f g h
j| j k l m n a b c d e f g h i
k| k l m n a b c d e f g h i j
l| l m n a b c d e f g h i j k
m| m n a b c d e f g h i j k l
n| n a b c d e f g h i j k l m
```

Si los nombres reales de los elemetnos del grupo no son muy complicados (o largos), la tabla puede resultar más informativa usando estos nombres.

```
K.<b> = AbelianGroup([10])
K.cayley_table(names='elements')
```

```
  *    1   b b^2 b^3 b^4 b^5 b^6 b^7 b^8 b^9
   +----------------------------------------
  1|    1   b b^2 b^3 b^4 b^5 b^6 b^7 b^8 b^9
  b|    b b^2 b^3 b^4 b^5 b^6 b^7 b^8 b^9   1
b^2| b^2 b^3 b^4 b^5 b^6 b^7 b^8 b^9   1   b
b^3| b^3 b^4 b^5 b^6 b^7 b^8 b^9   1   b b^2
b^4| b^4 b^5 b^6 b^7 b^8 b^9   1   b b^2 b^3
b^5| b^5 b^6 b^7 b^8 b^9   1   b b^2 b^3 b^4
b^6| b^6 b^7 b^8 b^9   1   b b^2 b^3 b^4 b^5
b^7| b^7 b^8 b^9   1   b b^2 b^3 b^4 b^5 b^6
b^8| b^8 b^9   1   b b^2 b^3 b^4 b^5 b^6 b^7
b^9| b^9   1   b b^2 b^3 b^4 b^5 b^6 b^7 b^8
```

Raíces Complejas de la Unidad

Los subgrupos cíclicos finitos de $\mathbb{T}$, generados por una raíz primitiva n-ésima de la unidad están implementados como una construcción mayor en Sage, conocida como cuerpo ciclotómico. Si uno se concentra solamente en la multiplicación de potencias de un generador (ignorando la infinidad de otros elementos) entonces se tiene un grupo cíclico finito. Como esto no está implementado en Sage como grupo *per se*, es un poco más difícil hacer construcciones tales como subgrupos, pero es un excelente ejercicio intentarlo. Es un bonito ejemplo pues los números complejos constituyen una construcción concreta familiar. Acá unos pocos ejemplos de cálculos para proveerle de algunas herramientas exploratorias. Vea las observaciones a continuación de los cálculos.

```
G = CyclotomicField(14)
w = G.gen(0); w
```

```
zeta14
```

```
wc = CDF(w)
wc.abs()
```

```
1.0
```

```
wc.arg()/N(2*pi/14)
```

```
1.0
```

```
b = w^2
b.multiplicative_order()
```

```
7
```

```
bc = CDF(b); bc
```

```
0.62348980185... + 0.781831482468...*I
```

```
bc.abs()
```

```
1.0
```

```
bc.arg()/N(2*pi/14)
```

```
2.0
```

```
sg = [b^i for i in range(7)]; sg
```

```
[1, zeta14^2, zeta14^4,
zeta14^5 - zeta14^4 + zeta14^3 - zeta14^2 + zeta14 - 1,
-zeta14, -zeta14^3, -zeta14^5]
```

```
c = sg[3]; d = sg[5]
c*d
```

```
zeta14^2
```

```
c = sg[3]; d = sg[6]
c*d in sg
```

```
True
```

```
c*d == sg[2]
```

```
True
```

```
sg[5]*sg[6] == sg[4]
```

```
True
```

```
G.multiplication_table(elements=sg)
```

```
*  a b c d e f g
 +--------------
a| a b c d e f g
b| b c d e f g a
c| c d e f g a b
d| d e f g a b c
e| e f g a b c d
f| f g a b c d e
g| g a b c d e f
```

Observaciones:

1. `zeta14` es el nombre del generador usado para el cuerpo ciclotómico, es una raíz primitiva de la unidad (una raíz 14-ésima en este caso). La hemos capturado como `w`.

2. La sintaxis `CDF(w)` convertirá al número complejo `w` a la notación más familiar con partes real e imaginaria.

3. El método `.abs()` entrega el módulo del número complejo, r como está descrito en el texto. Para estos elementos de $\mathbb{C}^*$ debiera ser siempre igual a 1.

4. El método `.arg()` entrega el argumento de un número complejo, θ como está descrito en el texto. Cada elemento del grupo cíclico en este ejemplo debe tener un argumento que es un múltiplo entero de $\frac{2\pi}{14}$. La sintaxis `N()` convierte el valor simbólico de `pi` a una aproximación numérica.

5. `sg` es una lista de elementos que forma un subgrupo cíclico de orden 7, que consiste de las primeras potencias de `b = w^2`. Así, por ejemplo, la última comparación multiplica la quinta potencia de `b` con la sexta potencia de `b`, lo que sería la undécima potencia de `b`. Pero como `b` tiene orden 7, esto se reduce a la cuarta potencia.

6. Si se sabe que un subconjunto de un grupo infinito forma un subgrupo, entonces se puede producir su tabla de Cayley especificando la lista de los elementos que se desean usar. Acá pedimos una tabla de multipicación, pues esa es la operación relevante en este caso.

4.8 Ejercicios en Sage

Este conjunto de ejercicios es sobre el grupo de unidades mód n, $U(n)$, que a veces es cíclico, otras veces no lo es. Existen algunos comandos en Sage que responden muy rápidamente algunas de estas preguntas, pero en lugar de usarlos ahora, use solamente las técnicas básicas descritas. La idea acá es trabajar directamente con los elementos, y listas de elementos, para discernir la estructura de subgrupos de estos grupos.

Las hojas de trabajo de Sage le permiten formar cuadros de textos con una extensa capacidad de formato, incluyendo la posibilidad de usar sintaxis de LaTeX para expresar matemáticas. De manera que si una pregunta requiere de una explicación o un comentario, cree una nueva celda y comuníquese claramente con su audiencia. Continúe esta práctica en las próximas listas de ejercicios.

1. Ejecute el comando `R = Integers(40)` para crear el conjunto `[0,1,2,...,39]` Éste es un grupo con la operación de suma mód 40, que ignoraremos. En cambio estamos interesados en el subconjunto de los elementos que tienen inverso respecto a la *multiplicación* mód 40. Determine el tamaño de este subgrupo ejecutando el comando `R.unit_group_order()`, y obtenga una lista de estos elementos con `R.list_of_elements_of_multiplicative_group()`.

2. Puede crear elementos de este grupo coercionando enteros comunes a `R`, por ejemplo con el comando `a = R(7)`. Esto le dirá a Sage que usted quiere ver a 7 como un elemento de R, sujeto a las operaciones correspondientes. Determine los elementos del subgrupo cíclico de R generado por 7 en una lista como sigue:

```
R = Integers(40)
a = R(7)
[a^i for i in srange(16)]
```

¿Cuál es el orden de 7 en $U(40)$?

3. El grupo $U(49)$ es cíclico. Usando solamente los comandos de Sage descritos previamente, encuentre un generador de este grupo. Ahora usando *solamente* teoremas sobre la estructura de grupos cíclicos, describa cada uno de los subgrupos de $U(49)$ especificando su orden y dando un generador explícito. No repita ninguno de los subgrupos — en otras palabras, presente cada subgrupo *exactamente* una vez. Puede usar Sage para verificar su trabajo con los subgrupos, pero su respuesta respecto a los subgrupos debe depender exclusivamente de teoremas y debe ser un párrafo bien escrito con una tabla, etc.

4. El grupo $U(35)$ no es cíclico. Nuevamente, usando solamente comandos Sage descritos previamente, use cálculos para entregar evidencia irrefutable de esto. ¿Cuántos de los 16 subgrupos diferentes de $U(35)$ puede listar?

5. Nuevamente, usando solamente los comandos Sage descritos previamente, explore la estructura de $U(n)$ para varios valores de n e intente formular una conjetura interesante sobre algunas de las propiedades básicas de este grupo. (Sí, esta es una pregunta *muy* abierta, pero éste es en definitiva el mayor beneficio de explorar matemáticas usando Sage.)

5

Grupos de Permutaciones

Los grupos de permutaciones tienen un rol central en el estudio de simetrías geométricas y en la teoría de Galois, el estudio de la búsqueda de soluciones de ecuaciones polinomiales. Además son una fuente de muchos ejemplos de grupos no abelianos.

Recordemos por un momento las simetrías del triángulo equilátero $\triangle ABC$ del Capítulo 3. Las simetrías de hecho consisten en permutaciones de los tres vértices, donde una ***permutación*** del conjunto $S = \{A, B, C\}$ es una biyección $\pi : S \to S$. Los tres vértices tienen la siguientes seis permutaciones.

$$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$
$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

Hemos usado el arreglo

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

para denotar la permutación que envía A en B, B en C, y C en A. Es decir,

$$A \mapsto B$$
$$B \mapsto C$$
$$C \mapsto A.$$

Las simetrías de un triángulo forman un grupo. En este capítulo estudiaremos grupos de ese tipo.

5.1 Definiciones y Notación

En general, las permutaciones de un conjunto X forman el grupo S_X. Si X es un conjunto finito, podemos suponer que $X = \{1, 2, \ldots, n\}$. En este caso escribiremos S_n en lugar de S_X. El siguiente teorema dice que S_n es un grupo. A este grupo lo llamaremos ***grupo simétrico*** en n símbolos.

Teorema 5.1. *El grupo simétrico en n símbolos, S_n, es un grupo con $n!$ elementos, con la operación binaria de composición de funciones.*

Demostración. La identidad de S_n es simplemente la función identidad que envía 1 en 1, 2 en 2, ..., n en n. Si $f : S_n \to S_n$ es una permutación, entonces f^{-1} existe, pues f es biyectiva; luego, toda permutación tiene una inversa. La composición de funciones es asociativa, lo que hace que la operación del grupo sea asociativa. Dejamos como ejercicio la demostración de que $|S_n| = n!$. □

Un subgrupo de S_n se llama ***grupo de permutaciones***.

Ejemplo 5.2. Considere el subgrupo G de S_5 que consiste de la permutación id y las permutaciones

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$
$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

La siguiente tabla nos indica como multiplicar elementos en el grupo de permutaciones G.

$\circ$	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	id	μ	τ
τ	τ	μ	id	σ
μ	μ	τ	σ	id

Nota 5.3. Si bien es natural multiplicar los elementos en un grupo de izquierda a derecha, las funciones se componen de derecha a izquierda. Sean σ y τ permutaciones en un conjunto X. Para componer σ y τ como funciones, calculamos $(\sigma \circ \tau)(x) = \sigma(\tau(x))$. Es decir, aplicamos primero τ, luego σ. Hay diversas formas de resolver esta inconsistencia. *Nosotros adoptaremos la convención de multiplicar permutaciones de derecha a izquierda. Para calcular $\sigma\tau$, haga τ primero y luego σ.* Es decir, por $\sigma\tau(x)$ queremos decir $\sigma(\tau(x))$. (Otra manera de resolver este problema sería escribir las funciones a la derecha; es decir, en lugar de escribir $\sigma(x)$, podríamos escribir $(x)\sigma$. También podríamos multiplicar las permutaciones de izquierda a derecha para coincidir con la forma usual de multiplicar elementos en un grupo. Cada una de estas soluciones ha sido usada.)

Ejemplo 5.4. La multiplicación de permutaciones no es conmutativa en general. Sean

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Entonces

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix},$$

pero

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Notación cíclica

La notación que hemos usado hasta ahora para representar las permutaciones es engorrosa, para decir lo menos. Para trabajar efectivamente con grupos de

permutaciones, necesitaremos un método más expedito de escribir y manipular permutaciones.

Una permutación $\sigma \in S_X$ es un ***ciclo de largo*** k si existen elementos $a_1, a_2, \ldots, a_k \in X$ tales que

$$\begin{aligned} \sigma(a_1) &= a_2 \\ \sigma(a_2) &= a_3 \\ &\vdots \\ \sigma(a_k) &= a_1 \end{aligned}$$

y $\sigma(x) = x$ para todos los demás elementos $x \in X$. Escribiremos $(a_1, a_2, \ldots, a_k)$ para denotar al ciclo σ. Los ciclos son los bloques básicos para construir todas las permutaciones.

Ejemplo 5.5. La permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (162354)$$

es un ciclo de largo 6, mientras

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix} = (243)$$

es un ciclo de largo 3.

No toda permutación es un ciclo. Considere la permutación

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1243)(56).$$

Esta permutación de hecho contiene un ciclo de largo 2 y un ciclo de largo 4.

Ejemplo 5.6. Es muy simple calcular el producto de ciclos. Supongamos que

$$\sigma = (1352) \quad \text{y} \quad \tau = (256).$$

Si pensamos en σ como

$$1 \mapsto 3, \qquad 3 \mapsto 5, \qquad 5 \mapsto 2, \qquad 2 \mapsto 1,$$

y τ como

$$2 \mapsto 5, \qquad 5 \mapsto 6, \qquad 6 \mapsto 2,$$

entonces para $\sigma\tau$ recordando que primero debemos aplicar τ y luego σ, debe ser el caso que

$$1 \mapsto 3, \qquad 3 \mapsto 5, \qquad 5 \mapsto 6, \qquad 6 \mapsto 2 \mapsto 1,$$

o $\sigma\tau = (1356)$. Si $\mu = (1634)$, entonces $\sigma\mu = (1652)(34)$.

Dos ciclos en S_X, $\sigma = (a_1, a_2, \ldots, a_k)$ y $\tau = (b_1, b_2, \ldots, b_l)$, son ***disjuntos*** si $a_i \neq b_j$ para todo i y para todo j.

Ejemplo 5.7. Los ciclos (135) y (27) son disjuntos; mientras los ciclos (135) y (347) no lo son. Calculando sus productos, descubrimos que

$$\begin{aligned} (135)(27) &= (135)(27) \\ (135)(347) &= (13475). \end{aligned}$$

El producto de dos ciclos que no son disjuntos a veces se puede reducir a algo menos complicado; el producto de dos ciclos disjuntos no puede ser simplificado.

Proposición 5.8. *Sean σ y τ dos ciclos disjuntos en S_X. Entonces $\sigma\tau = \tau\sigma$.*

DEMOSTRACIÓN. Sea $\sigma = (a_1, a_2, \ldots, a_k)$ and $\tau = (b_1, b_2, \ldots, b_l)$. Debemos mostrar que $\sigma\tau(x) = \tau\sigma(x)$ para todo $x \in X$. Si x no está en $\{a_1, a_2, \ldots, a_k\}$ ni en $\{b_1, b_2, \ldots, b_l\}$, entonces tanto σ como τ fijan x. Es decir, $\sigma(x) = x$ y $\tau(x) = x$. Luego,

$$\sigma\tau(x) = \sigma(\tau(x)) = \sigma(x) = x = \tau(x) = \tau(\sigma(x)) = \tau\sigma(x).$$

No debemos olvidar que estamos multiplicando las permutaciones de derecha a izquierda,. Ahora supongamos que $x \in \{a_1, a_2, \ldots, a_k\}$. Entonces $\sigma(a_i) = a_{(i \bmod k)+1}$; es decir,

$$\begin{aligned} a_1 &\mapsto a_2 \\ a_2 &\mapsto a_3 \\ &\vdots \\ a_{k-1} &\mapsto a_k \\ a_k &\mapsto a_1. \end{aligned}$$

Pero, $\tau(a_i) = a_i$ pues σ y τ son disjuntos. Por lo tanto,

$$\begin{aligned} \sigma\tau(a_i) &= \sigma(\tau(a_i)) \\ &= \sigma(a_i) \\ &= a_{(i \bmod k)+1} \\ &= \tau(a_{(i \bmod k)+1}) \\ &= \tau(\sigma(a_i)) \\ &= \tau\sigma(a_i). \end{aligned}$$

Similarmente, si $x \in \{b_1, b_2, \ldots, b_l\}$, entonces σ y τ también conmutan. □

Teorema 5.9. *Toda permutación en S_n puede ser escrita como producto de ciclos disjuntos.*

DEMOSTRACIÓN. Podemos suponer que $X = \{1, 2, \ldots, n\}$. Si $\sigma \in S_n$ y definimos X_1 como $\{\sigma(1), \sigma^2(1), \ldots\}$, entonces el conjunto X_1 es finito pues X es finito. Ahora sea i el primer entero en X que no está en X_1 y definamos X_2 como $\{\sigma(i), \sigma^2(i), \ldots\}$. Nuevamente, X_2 es un conjunto finito. Continuando de esta manera, podemos definir conjuntos finitos disjuntos $X_3, X_4, \ldots$. Como X es un conjunto finito, estamos seguros que este proceso terminará y que habrá un número finito de estos conjuntos, digamos r. Si σ_i es el ciclo definido por

$$\sigma_i(x) = \begin{cases} \sigma(x) & x \in X_i \\ x & x \notin X_i, \end{cases}$$

entonces $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$. Como los conjuntos $X_1, X_2, \ldots, X_r$ son disjuntos, los ciclos $\sigma_1, \sigma_2, \ldots, \sigma_r$ también lo son. □

Ejemplo 5.10. Sean

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix}.$$

Usando notación cíclica, podemos escribir

$$\begin{aligned}\sigma &= (1624)\\ \tau &= (13)(456)\\ \sigma\tau &= (136)(245)\\ \tau\sigma &= (143)(256).\end{aligned}$$

Nota 5.11. Desde ahora nos resultará conveniente usar la notación cíclica para representar las permutaciones. Cuando usemos la notación cíclica, frecuentemente representaremos la permutación identidad por (1) o por ().

Transposiciones

La permutación (no trivial) más simple es un ciclo de largo 2. Tales ciclos se llaman ***transposiciones***. Como

$$(a_1, a_2, \ldots, a_n) = (a_1a_n)(a_1a_{n-1})\cdots(a_1a_3)(a_1a_2),$$

cualquier ciclo puede ser escrito como el producto de transposiciones, llevándonos a la siguiente proposición.

Proposición 5.12. *Cualquier permutación de un conjunto finito que contenga al menos dos elementos puede ser escrita como producto de transposiciones.*

Ejemplo 5.13. Considere la permutación

$$(16)(253) = (16)(23)(25) = (16)(45)(23)(45)(25).$$

Como podemos ver, no hay una única forma de representar la permutación como producto de transposiciones. Por ejemplo, podemos escribir la identidad como (12)(12), como (13)(24)(13)(24), y en muchas otras formas. Sin embargo, resulta ser, que ninguna permutación se puede escribir tanto como un producto de un número par como de un número impar de transposiciones. Por ejemplo, podemos representar la permutación (16) por

$$(23)(16)(23)$$

o por

$$(35)(16)(13)(16)(13)(35)(56),$$

pero (16) siempre será el producto de un número impar de transposiciones.

Lema 5.14. *Si la identidad se escribe como el producto de r transposiciones,*

$$\mathrm{id} = \tau_1\tau_2\cdots\tau_r,$$

entonces r es un número par.

Demostración. Procederemos por inducción en r. Una transposición no puede ser la identidad; luego, $r > 1$. Si $r = 2$, estamos listos. Supongamos que $r > 2$. En este caso el producto de al menos dos de estas transposiciones, $\tau_{r-1}\tau_r$, debe estar en uno de los casos siguientes:

$$\begin{aligned}(ab)(ab) &= \mathrm{id}\\ (bc)(ab) &= (ac)(bc)\\ (cd)(ab) &= (ab)(cd)\\ (ac)(ab) &= (ab)(bc),\end{aligned}$$

donde a, b, c, y d son distintos.

La primera ecuación simplemente dice que una transposición es su propia inversa. Si ocurre este caso, borre $\tau_{r-1}\tau_r$ del producto para obtener

$$\mathrm{id} = \tau_1\tau_2\cdots\tau_{r-3}\tau_{r-2}.$$

Por inducción $r-2$ es par; luego, r debe ser par.

En cada uno de los otros tres casos, podemos reemplazar $\tau_{r-1}\tau_r$ con el lado derecho de la ecuación correspondiente para obtener un nuevo producto de r transposiciones para la identidad. En este nuevo producto, la última aparición de a será en la penúltima transposición. Podemos continuar este proceso con $\tau_{r-2}\tau_{r-1}$ para obtener ya sea un producto de $r-2$ transposiciones o un nuevo producto de r transposiciones donde la última apaarición de a es en τ_{r-2}. Si la identidad es el producto de $r-2$ transposiciones, entonces nuevamente estamos listos, por la hipótesis de inducción; de otro modo, repetiremosel procedimiento con $\tau_{r-3}\tau_{r-2}$.

En algún momento, tendremos dos transposiciones adyacentes iguales, que se cancelarán o a solamente estará presente en la primera transposición. Pero este último caso no puede ocurrir, pues la identidad no fijaría a en esta situación. Por lo tanto, la identidad debe ser el producto de $r-2$ transposiciones y, nuevamente por la hipótesis de inducción, estamos listos. □

Teorema 5.15. *Si una permutación σ puede ser expresada como el producto de un número par de transposiciones, entonces cualquier otro producto de transposiciones igual a σ debe también contener un número par de transposiciones. De forma similar, si σ puede ser expresada como el producto de un número impar de transposiciones, entonces cualquier otro producto de transposiciones igual a σ debe también contener un número impar de transposiciones.*

Demostración. Supongamos que

$$\sigma = \sigma_1\sigma_2\cdots\sigma_m = \tau_1\tau_2\cdots\tau_n,$$

con m par. Debemos mostrar que n también es un número par. La inversa de σ es $\sigma_m\cdots\sigma_1$. Como

$$\mathrm{id} = \sigma\sigma_m\cdots\sigma_1 = \tau_1\cdots\tau_n\sigma_m\cdots\sigma_1,$$

n debe ser par por el Lema 5.14. La demostración del caso en el que σ puede ser expresada como el producto de un número impar de transposiciones lo dejamos como ejercicio. □

A la luz del Teorema 5.15, definimos que una permutación es ***par*** si puede ser expresada como el producto de un número par de transposiciones e ***impar*** si puede ser expresada como el producto de un número impar de transposiciones.

Los Grupos Alternantes

Uno de los subgrupos más importantes de S_n es el conjunto de todas las permutaciones pares, A_n. El grupo A_n se llama ***grupo alternante en n símbolos***.

Teorema 5.16. *El conjunto A_n es un subgrupo de S_n.*

DEMOSTRACIÓN. Como el producto de dos permutaciones pares es también una permutación par, A_n es cerrado. La identidad es una permutación par y por lo tanto está en A_n. Si σ es una permutación par, entonces

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_r,$$

donde σ_i son transposiciones y r es par. Como la inversa de una transposición es ella misma,

$$\sigma^{-1} = \sigma_r\sigma_{r-1} \cdots \sigma_1$$

también está en A_n. □

Proposición 5.17. *El número de permutaciones pares en S_n, $n \geq 2$, es igual al número de permutaciones impares; luego, el orden de A_n es $n!/2$.*

DEMOSTRACIÓN. Sea A_n el conjunto de permutaciones pares en S_n y B_n el conjunto de permutaciones impares. Si ppodemos mostrar que existe una biyección entre estos conjuntos, habremos demostrado que contienen el mismo número de elementos. Fijemos una transposición σ en S_n. Como $n \geq 2$, tal σ existe. Defina

$$\lambda_\sigma : A_n \to B_n$$

como

$$\lambda_\sigma(\tau) = \sigma\tau.$$

Supongamos que $\lambda_\sigma(\tau) = \lambda_\sigma(\mu)$. Entonces $\sigma\tau = \sigma\mu$ y así

$$\tau = \sigma^{-1}\sigma\tau = \sigma^{-1}\sigma\mu = \mu.$$

Por lo tanto, λ_σ es 1-1. Dejaremos la demostración de que λ_σ es sobreyectiva como ejercicio. □

Ejemplo 5.18. El grupo A_4 es el subgrupo de S_4 que consiste de las permutaciones pares. Hay doce elementos en A_4:

(1)	(12)(34)	(13)(24)	(14)(23)
(123)	(132)	(124)	(142)
(134)	(143)	(234)	(243).

Uno de los ejercicios al final del capítulo será el de encontrar todos los subgrupos de A_4. Descubrirá que no hay ningún subgrupo de orden 6. ¿Le sorprende?

Note Histórica

Lagrange fue el primero en pensar las permutaciones como funciones de un conjunto en si mismo, pero fue Cauchy quién desarrolló los teoremas básicos y la notación para las permutaciones. Él fue el primero en usar la notación cíclica. Augustin-Louis Cauchy (1789–1857) nació en París durante en el apogeo de la Revolución Francesa. Su familia dejó París y se fue al pueblo de Arcueil para escapar del Reino del Terror. Uno de los vecinos de la familia allí, fue Pierre-Simon Laplace (1749–1827), quien lo motivó a iniciar una carrera en matemáticas. Cauchy comenzó su carrera como matemático resolviendo un problema de geometría que le planteó Lagrange. Cauchy escribió más de 800 trabajos en diversos tópicos, como ecuaciones diferenciales, grupos finitos, matemáticas aplicadas, y análisis complejo. Fue uno de los matemáticos responsables de hacer que el Cálculo Diferencial fuera riguroso. Es probable que haya más teoremas y conceptos en matemáticas asociados al nombre de Cauchy que al de cualquier otro matemático.

5.2 Grupos Dihedrales

Otro tipo especial de grupo de permutaciones es el de los grupos dihedrales. Recordemos el grupo de las simetrías del triángulo equilátero en el Capítulo 3. Tales grupos consisten de los movimientos rígidos de un polígono regular de n lados o n-ágono regular. Para $n = 3, 4, \ldots$, definimos el ***n-ésimo grupo dihedral*** como el grupo de los movimientos rígidos de n n-ágono regular. Denotaremos este grupo por D_n. Podemos numerar los vértices de un n-ágono regular con $1, 2, \ldots, n$ (Figura 5.19). Note que hay exactamente n posibilidades para reemplazar al primer vértice. Si reemplazamos al primer vértice por k, entonces el segundo vértice debe ser reemplazado por el vértice $k + 1$ o por el vértice $k - 1$; luego, hay $2n$ movimientos rígidos posibles del n-ágono. Resumimos estos resultados en el siguiente teorema.

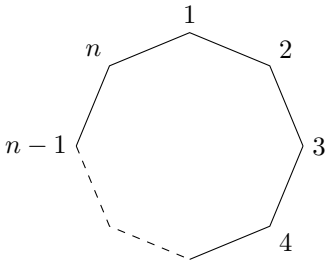


Figura 5.19: Un n-ágono regular

Teorema 5.20. *El grupo dihedral, D_n, es un subgrupo de S_n de orden $2n$.*

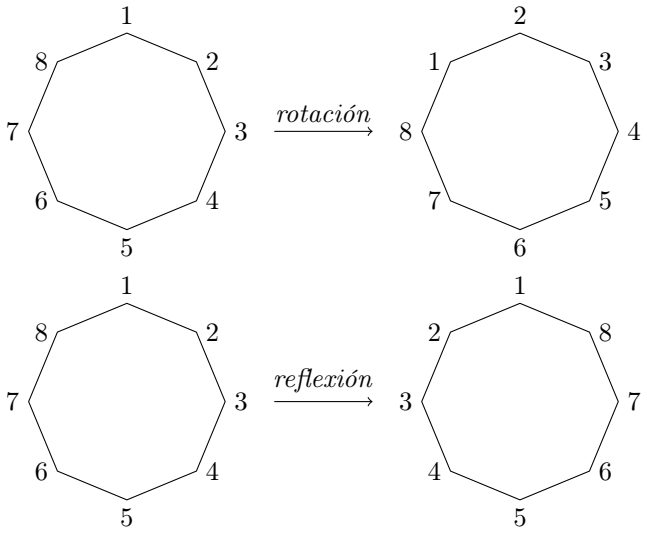


Figura 5.21: Rotaciones y reflexiones de un n-ágono regular

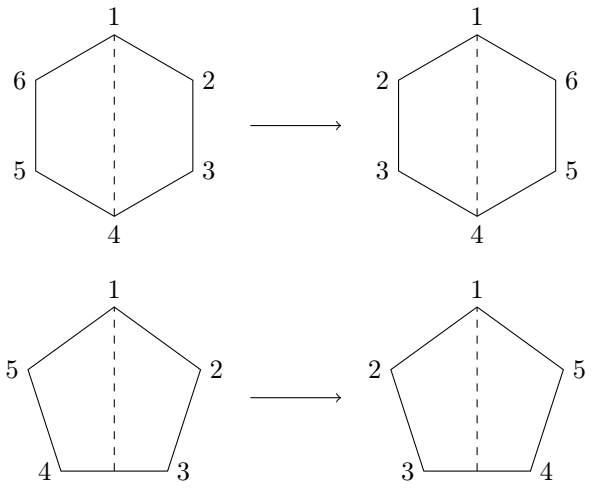


Figura 5.22: Tipos de reflexiones de un n-ágono regular

Teorema 5.23. *El grupo D_n, $n \geq 3$, consiste de todos los productos de los dos elementos r y s, que satifacen las relaciones*

$$r^n = 1$$
$$s^2 = 1$$
$$srs = r^{-1}.$$

Demostración. Los posibles movimientos de un n-ágono regular son reflexiones y rotaciones (Figura 5.21). Hay exactamente n rotaciones posibles:

$$\text{id}, \frac{360^\circ}{n}, 2 \cdot \frac{360^\circ}{n}, \ldots, (n-1) \cdot \frac{360^\circ}{n}.$$

Denotaremos la rotación en $360^\circ/n$ por r. La rotación r genera todas las rotaciones. Es decir,

$$r^k = k \cdot \frac{360^\circ}{n}.$$

Etiquete las n reflexiones $s_1, s_2, \ldots, s_n$, donde s_k es la reflexión que fija el vértice k. Hay dos casos, dependiendo de si n es par o impar. Si hay un número par de vértices, entonces una reflexión fija dos de ellos, y $s_1 = s_{n/2+1}, s_2 = s_{n/2+2}, \ldots, s_{n/2} = s_n$. Si hay un número impar de vértices, entonces una reflexión fija solamente un vértice y $s_1, s_2, \ldots, s_n$ son distintas (Figura 5.22). En cualquier caso, el orden de cada s_k es dos. Sea $s = s_1$. Entonces $s^2 = 1$ y $r^n = 1$. Como cualquier movimiento rígido t del n-ágono reemplaza al primer vértice por el vértice k, el segundo vértice será reemplazado por el $k+1$ o por el $k-1$. Si el segundo se reemplaza por $k+1$, entonces $t = r^k$. Si el segundo se reemplaza por $k-1$, entonces $t = sr^k$. Luego, r y s generan D_n. Es decir, D_n consiste de todos los productos finitos de r y s,

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}.$$

Dejaremos la demostración de que $srs = r^{-1}$ como un ejercicio. □

Ejemplo 5.24. El grupo de movimientos de un cuadrado, D_4, consiste de ocho elementos. Con los vértices numerados 1, 2, 3, 4 (Figura 5.25), las rotaciones son

$$r = (1234)$$

$$r^2 = (13)(24)$$
$$r^3 = (1432)$$
$$r^4 = (1)$$

y las reflexiones son

$$s_1 = (24)$$
$$s_2 = (13).$$

El orden de D_4 es 8. Los dos elementos restantes son

$$rs_1 = (12)(34)$$
$$r^3 s_1 = (14)(23).$$

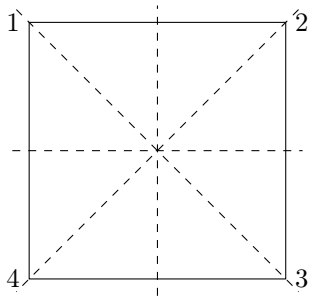


Figura 5.25: El grupo D_4

El grupo de movimientos de un Cubo

Podemos investigar los grupos de movimientos de objetos geométricos diferentes de los polígonos de n lados para obtener ejemplos interesantes de grupos de permutaciones. Consideremos el grupo de movimientos rígidos de un cubo. Una de las primeras preguntas que podemos hacer sobre este grupo es "¿cuál es su orden?" Un cubo tiene 6 caras. Si una cara en particular está apuntado hacia arriba, entonces existen cuatro rotaciones posibles del cubo que preservarán la cara apuntando hacia arriba. Luego, el orden del grupo es $6 \cdot 4 = 24$. Acabamos de demostrar la siguiente proposición.

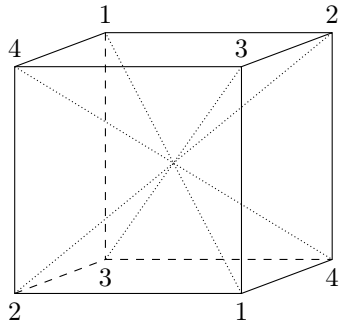


Figura 5.26: El grupo de movimientos de un cubo

Proposición 5.27. *El grupo de movimientos rígidos de un cubo contiene* 24 *elementos.*

Teorema 5.28. *El grupo de movimientos rígidos de un cubo es S_4.*

DEMOSTRACIÓN. De la Proposición 5.27, ya sabemos que el grupo de movimientos del cubo tiene 24 elementos, el mismo número de elementos que hay en S_4. Hay exactamente cuatro diagonales en el cubo. Si etiquetamos estas diagonales con 1, 2, 3, y 4, debemos mostrar que el grupo de movimientos del cubo nos dará cualquier permutación de las diagonales (Figura 5.26). Si podemos obtener todas estas permutaciones, entonces S_4 y el grupo de movimientos rígidos del cubo tendrán que ser el mismo. Para obtener una transposición, podemos rotar el cubo en 180° en torno al eje que une los puntos medios de aristas opuestas (Figura 5.29). Hay seis de tales ejes, dando todas las transposiciones en S_4. Como todo elemento en S_4 es el producto de un número finito de transposiciones, el grupo de movimientos de un cubo tiene que ser S_4. □

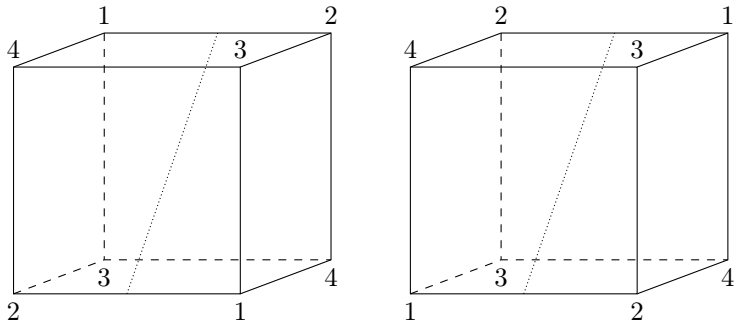


Figura 5.29: Transposiciones en el grupo de movimientos de un cubo

Sage Un grupo de permutaciones es una representación muy concreta de un grupo, y la herramientas de Sage para trabajar con grupos de permutaciones son muy buenas — convirtiendo a Sage en un lugar natural para que principiantes aprendan sobre teoría de grupos.

5.3 Ejercicios

1. Escriba las siguientes permutaciones en notación cíclica.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

2. Escriba cada una de las siguientes como producto de ciclos disjuntos.

(a) $(1345)(234)$

(b) $(12)(1253)$

(c) $(143)(23)(24)$

(d) $(1423)(34)(56)(1324)$

(e) $(1254)(13)(25)$

(f) $(1254)(13)(25)^2$

(g) $(1254)^{-1}(123)(45)(1254)$

(h) $(1254)^2(123)(45)$

(i) $(123)(45)(1254)^{-2}$
(j) $(1254)^{100}$
(k) $|(1254)|$
(l) $|(1254)^2|$
(m) $(12)^{-1}$
(n) $(12537)^{-1}$
(o) $[(12)(34)(12)(47)]^{-1}$
(p) $[(1235)(467)]^{-1}$

3. Exprese las siguientes permutaciones como producto de transposiciones e identifíquelas como pares o impares.

(a) (14356)
(b) (156)(234)
(c) (1426)(142)
(d) (17254)(1423)(154632)
(e) (142637)

4. Encuentre $(a_1, a_2, \ldots, a_n)^{-1}$.

5. Liste todos los subgrupos de S_4. Encuentre cada uno de los siguientes conjuntos.

(a) $\{\sigma \in S_4 : \sigma(1) = 3\}$
(b) $\{\sigma \in S_4 : \sigma(2) = 2\}$
(c) $\{\sigma \in S_4 : \sigma(1) = 3 \text{ and } \sigma(2) = 2\}$

¿Es alguno de estos conjuntos un subgrupo de S_4?

6. Encuentre todos los subgrupos de A_4. ¿Cuál es el orden de cada uno de ellos?

7. Encuentre todos los posibles órdenes de elementos en S_7 y en A_7.

8. Muestre que A_{10} contiene un elemento de orden 15.

9. ¿Contiene A_8 un elemento de orden 26?

10. Encuentre un elemento de orden maximal en S_n para $n = 3, \ldots, 10$.

11. ¿Cuáles son las posibles estructuras de ciclos de los elementos de A_5? ¿Y de A_6?

12. Sea $\sigma \in S_n$ un elemento de orden n. Muestre que para todos los enteros i y j, $\sigma^i = \sigma^j$ si y solo si $i \equiv j \pmod{n}$.

13. Sea $\sigma = \sigma_1 \cdots \sigma_m \in S_n$ el producto disjunto de ciclos. Demuestre que el orden de σ es el mínimo común múltiplo de los largos de los ciclos $\sigma_1, \ldots, \sigma_m$.

14. Usando notación cíclica, liste los elementos en D_5. ¿Cuáles son r y s? Escriba todo elemento como producto de r y s.

15. Si las diagonales de un cubo están etiquetadas como en la Figura 5.26, ¿a qué movimiento del cubo corresponde la permutación (12)(34)? ¿Y las otras permutaciones de las diagonales?

16. Encuentre el grupo de movimientos rígidos de un tetrahedro. Muestre que este es el mismo grupo que A_4.

17. Demuestre que S_n es no abeliano para $n \geq 3$.

18. Muestre que A_n es no abeliano para $n \geq 4$.

19. Demuestre que D_n es no abeliano para $n \geq 3$.

20. Sea $\sigma \in S_n$ un ciclo. Demuestre que σ puede ser escrito como el producto de a lo más $n-1$ transposiciones.

21. Sea $\sigma \in S_n$. Si σ no es un ciclo, demuestre que σ puede ser escrita como el producto de a lo más $n-2$ transposiciones.

22. Si σ puede ser expresada como un producto de un número par de transposiciones, muestre que cualquier otro producto de transposiciones que sea igual a σ también debe contener un número impar de estas.

23. Si σ es un ciclo de largo impar, demuestre que σ^2 también es un ciclo.

24. Muestre que un 3-ciclo es una permutación par.

25. Demuestre que en A_n con $n \geq 3$, culaquier permutación es un producto de ciclos de largo 3.

26. Demuestre que todo elemento en S_n puede ser escrito como un producto finito de las siguientes permutaciones.

(a) $(12), (13), \ldots, (1n)$

(b) $(12), (23), \ldots, (n-1, n)$

(c) $(12), (12\ldots n)$

27. Sea G un grupo y sea $\lambda_g : G \to G$ una función definida por $\lambda_g(a) = ga$. Demuestre que λ_g es una permutación de G.

28. Demuestre que existen $n!$ permutaciones de un conjunto con n elementos.

29. Recuerde que el ***centro*** de un grupo G es

$$Z(G) = \{g \in G : gx = xg \text{ para todo } x \in G\}.$$

Encuentre el centro de D_8. ¿Y el centro de D_{10}? ¿Cuál es el centro de D_n?

30. Sea $\tau = (a_1, a_2, \ldots, a_k)$ un ciclo de largo k.

(a) Demuestre que si σ es cualquier permutación, entonces

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))$$

es un ciclo de largo k.

(b) Sea μ un ciclo de largo k. Demuestre que existe una permutación σ tal que $\sigma\tau\sigma^{-1} = \mu$.

31. Para α y β en S_n, defina $\alpha \sim \beta$ si existe $\sigma \in S_n$ tal que $\sigma\alpha\sigma^{-1} = \beta$. Muestre que $\sim$ es una relación de equivalencia en S_n.

32. Sea $\sigma \in S_X$. Si $\sigma^n(x) = y$, diremos que $x \sim y$.

(a) Muestre que $\sim$ es una relación de equivalencia en X.

(b) Si $\sigma \in A_n$ y $\tau \in S_n$, muestre que $\tau^{-1}\sigma\tau \in A_n$.

(c) Defina la ***órbita*** de $x \in X$ bajo $\sigma \in S_X$ como el conjunto

$$\mathcal{O}_{x,\sigma} = \{y : x \sim y\}.$$

Calcule las órbitas de cada uno de los siguientes elementos en S_5:

$$\alpha = (1254)$$
$$\beta = (123)(45)$$
$$\gamma = (13)(25).$$

(d) Si $\mathcal{O}_{x,\sigma} \cap \mathcal{O}_{y,\sigma} \neq \emptyset$, demuestre que $\mathcal{O}_{x,\sigma} = \mathcal{O}_{y,\sigma}$. Las órbitas bajo una permutación σ son las clases de equivalencia correspondientes a la relación $\sim$.

(e) Un subgrupo H de S_X es ***transitivo*** si para cada $x, y \in X$, existe un $\sigma \in H$ tal que $\sigma(x) = y$. Demuestre que $\langle\sigma\rangle$ es transitivo si y solo si $\mathcal{O}_{x,\sigma} = X$ para algún $x \in X$.

33. Sea $\alpha \in S_n$ con $n \geq 3$. Si $\alpha\beta = \beta\alpha$ para todo $\beta \in S_n$, demuestre que α debe ser la permutación identidad; luego, el centro de S_n es el subgrupo trivial.

34. Si α es par, demuestre que α^{-1} también es par. ¿Hay un resultado análogo si α es impar?

35. Muestre que $\alpha^{-1}\beta^{-1}\alpha\beta$ es par para todo $\alpha, \beta \in S_n$.

36. Sean r y s los elementos en D_n descritos en el Teorema 5.23.

(a) Muestre que $srs = r^{-1}$.

(b) Muestre que $r^k s = sr^{-k}$ en D_n.

(c) Demuestre que el orden de $r^k \in D_n$ es $n/\operatorname{mcd}(k, n)$.

5.4 Sage

Una buena parte de de la implementación de teoría de grupos en Sage está basada en rutinas de GAP (Groups, Algorithms, and Programming) en www.gap-system.org, que está incluido en cada copia de Sage. Este es un paquete de código abierto maduro, que existe desde 1986.

Como hemos visto, los grupos pueden ser descritos de muchas maneras diferentes, tales como conjuntos de matrices, conjuntos de números complejos, o conjuntos de símbolos sujetos a ciertas relaciones. Una manera muy concreta de repersentar grupos es via permutaciones (funciones biyectivas de los enteros del 1 al n), usando la composición de funciones como la operación en el grupo. Sage tiene muchas rutinas diseñadas para trabajar con grupos de este tipo y son también una buena forma para que las personas que quieran aprender teoría de grupos ganen experiencia con las ideas básicas de la teoría de grupos. Por estas dos razones, nos concentraremos en este tipo de grupos.

Grupos de Permutaciones y sus Elementos

La forma más fácil de trabajar con elementos de grupos de permutación en Sage es escribirlos con notación cíclica. Como estos son productos de ciclos disjuntos (que conmutan), no necesitamos preocuparnos por el orden en que aparecen los ciclos. Si escribimos `(1,3)(2,4)` probablemente entenderemos que se trata de una permutación (el contenido de este capítulo!) y sabemos que podría ser un elemento de S_4, o quizás de un grupo simétrico en más de 4 símbolos. Sage no puede comenzar tan fácilmente y necesita un poco de contexto, así es que coercionamos una cadena de caracteres escritos con notación de ciclos a pertenecer a un grupo simétrico para producir elementos del grupo. A continuación algunos ejemplos y cálculos de muestra. Recuerde que Sage y el texto difieren en el orden usado para componer dos permutaciones en un producto.

```
G = SymmetricGroup(5)
sigma = G("(1,3)(2,5,4)")
sigma*sigma
```

```
(2,4,5)
```

```
rho = G("(2,4)(1,5)")
rho^3
```

```
(1,5)(2,4)
```

Si los próximos tres ejemplos parecen confusos, o "al revés", entonces sería un buen momento para revisar la discusión respecto al orden de la composición de permutaciones en Sage hecha en la subsección Grupos de simetrías.

```
sigma*rho
```

```
(1,3,5,2)
```

```
rho*sigma
```

```
(1,4,5,3)
```

```
rho^-1*sigma*rho
```

```
(1,2,4)(3,5)
```

Hay formas alternativas de crear elementos de un grupo de permutaciones, que pueden ser útiles en alguna situación particular, pero que no son de uso muy frecuente.

```
sigma1 = G("(1,3)(2,5,4)")
sigma1
```

```
(1,3)(2,5,4)
```

```
sigma2 = G([(1,3),(2,5,4)])
sigma2
```

```
(1,3)(2,5,4)
```

```
sigma3 = G([3,5,1,2,4])
sigma3
```

```
(1,3)(2,5,4)
```

```
sigma1 == sigma2
```

```
True
```

```
sigma2 == sigma3
```

```
True
```

```
sigma2.cycle_tuples()
```

```
[(1, 3), (2, 5, 4)]
```

```
[sigma3(x) for x in G.domain()]
```

```
[3, 5, 1, 2, 4]
```

La segunda versión de σ es una lista de "tuplas", que requiere muchas comas y estas deben ser incluidas a su vez en una lista. (Una tupla de largo uno debe ser escrita como `(4,)` para distinguirla del uso de paréntesis para agrupar, como en `5*(4)`.) La tercera versión usa la "fila inferior" de la notación más engorrosa de dos filas introducida al comienzo del capítulo — es una lista ordenada de las *imágenes* de la permutación cuando es considerada como una función.

Vemos que sin importar las tres formas diferentes de ingreso, todas las versiones de σ se muestran de la misma manera, y más aún son iguales entre sí. (Esta es una sutil diferencia entre — lo que un objeto *es* en Sage versus como un objeto se *muestra*.)

Podemos ser aún más cuidadosos sobre la naturaleza de nuestros elementos. Note que una vez que Sage comienza, puede promover el producto $\tau\sigma$ al grupo mayor de permutaciones. Podemos "promover" elementos a grupos mayores de permutaciones, pero sería un error tratar de forzar un elemento en un grupo simétrico demasiado pequeño.

```
H = SymmetricGroup(4)
sigma = H("(1,2,3,4)")
G = SymmetricGroup(6)
tau = G("(1,2,3,4,5,6)")
rho = tau * sigma
rho
```

```
(1,3)(2,4,5,6)
```

```
sigma.parent()
```

```
Symmetric group of order 4! as a permutation group
```

```
tau.parent()
```

```
Symmetric group of order 6! as a permutation group
```

```
rho.parent()
```

```
Symmetric group of order 6! as a permutation group
```

```
tau.parent() == rho.parent()
```

```
True
```

```
sigmaG = G(sigma)
sigmaG.parent()
```

```
Symmetric group of order 6! as a permutation group
```

Es un error intentar coercionar una permutación con demasiados símbolos a un grupo de permutaciones que use menos símbolos.

```
tauH = H(tau)
```

```
Traceback (most recent call last):
...
ValueError: Invalid permutation vector: (1,2,3,4,5,6)
```

Mejor que trabajar simplemente con elementos del grupo simétrico, podemos crear diversos grupos de permutaciones en Sage. A continuación una muestra para comenzar:

Comando Sage	Descripción
`SymmetricGroup(n)`	Grupo simétrico en n símbolos, $n!$ elementos
`DihedralGroup(n)`	Simetrías de un n-ágono, $2n$ elementos.
`CyclicPermutationGroup(n)`	Rotaciones de un n-ágono, n elementos
`AlternatingGroup(n)`	Grupo alternante en n símbolos, $n!/2$ elementos
`KleinFourGroup()`	Un grupo no cíclico de orden 4

Cuadro 5.30: Algunos grupos de permutaciones en Sage

Usted también puede localizar grupos de permutaciones en Sage usando el catálogo de `grupos`. En la próxima celda ponga el cursor después del punto final y presione la tecla de tabular (TAB). Obtendrá una lista de métodos que puede usar para crear grupos de permutaciones. Como siempre, ponga un signo de interrogación después de un método y presione la tecla de tabular para obtener documentación en línea del método. (esto funciona en una celda de Sage normal pero no parece funcionar en el "libro")

```
groups.permutation.
```

Propiedades de Permutaciones (Elementos)

A veces es más fácil tomar un elemento de una lista de elementos en un grupo de permutaciones, así ya está asociado a un "parent" y no hay necesidad de hacer ninguna coerción. En lo que sigue, `rotate` y `flip` son automáticamente elementos de `G` por la forma en que fueron obtenidos.

```
D = DihedralGroup(5)
elements = D.list(); elements
```

```
[(), (1,5)(2,4), (1,2,3,4,5), (1,4)(2,3), (1,3,5,2,4),
    (2,5)(3,4),
 (1,3)(4,5), (1,5,4,3,2), (1,4,2,5,3), (1,2)(3,5)]
```

```
rotate = elements[2]
flip = elements[3]
flip*rotate == rotate* flip
```

```
False
```

Vemos con esta última prueba que el grupo de simetrías de un pentágono es no abeliano. Pero hay una manera más fácil.

```
D = DihedralGroup(5)
D.is_abelian()
```

```
False
```

Existen muchos métodos, tanto para los grupos de permutaciones como para sus elementos. Use la celda vacía de más abajo para crear un grupo de permutaciones (el que quiera) y un elemento de un grupo de permutaciones (cualquiera). A continuación usa la tab-completion para ver todos los métodos disponibles

para un elemento, o para un grupo (nombre, punto, tecla-tab). Algunos nombres los puede reconocer, otros los aprenderemos en los capítulos siguientes, algunos son herramientas muy especializadas de investigación que podría usar para desarrollar su tesis de doctorado en teoría de grupos. Para cualquiera de estos métodos, recuerde que puede escribir el nombre, seguido de un signo de interrogación, para ver la documentación y ejemplos. *Experimente y explore* — es realmente difícil hechar a perder algo.Acá hay algunos ejemplos de varios métodos disponibles.

```
A4 = AlternatingGroup(4)
A4.order()
```

```
12
```

```
A4.is_finite()
```

```
True
```

```
A4.is_abelian()
```

```
False
```

```
A4.is_cyclic()
```

```
False
```

```
sigma = A4("(1,2,4)")
sigma^-1
```

```
(1,4,2)
```

```
sigma.order()
```

```
3
```

Un método útil al estudiar el grupo alternante es el `.sign()` implementado para elementos de un grupo de permutaciones. Retorna `1` si la permutación es par y `-1` si es impar.

```
G = SymmetricGroup(3)
sigma = G("(1,2)")
tau = G("(1,3)")
rho = sigma*tau
sigma.sign()
```

```
-1
```

```
rho.sign()
```

```
1
```

Podemos crear subgrupos entregándole al grupo una lista de "generadores." Estos elementos se usan para "generar" un subgrupo — imagine multiplicar estos elementos (y sus inversos) una y otra vez, creando nuevos elementos que también deben estar en el subgrupo y que también participan de nuevos productos, hasta que no aparezcan nuevos elementos. Esta definición termina con un enunciado terriblemente impreciso, pero debiera se suficiente por ahora.

Una mejor definición es que el subgrupo generado por los elementos es el menor subgrupo que contiene todos los generadores — lo que está bien si conocemos todos los subgrupos de antemano.

Con un único generador, los productos repetidos son simplemente las potencias del generador. El grupo generado en este caso es cíclico. Con dos (o más) generadores, especialmente en un grupo no abeliano, la situación puede ser mucho, mucho más complicada. Empecemos con un generador. Pero no olvide ponerlo en una lista de todas formas.

```
A4 = AlternatingGroup(4)
sigma = A4("(1,2,4)")
sg = A4.subgroup([sigma])
sg
```

```
Subgroup of (Alternating group of order 4!/2 as a permutation
    group)
generated by [(1,2,4)]
```

```
sg.order()
```

```
3
```

```
sg.list()
```

```
[(), (1,2,4), (1,4,2)]
```

```
sg.is_abelian()
```

```
True
```

```
sg.is_cyclic()
```

```
True
```

```
sg.is_subgroup(A4)
```

```
True
```

Podemos ahora rehacer el ejemplo del principio del capítulo. Traducimos los elementos a notación cíclica, construimos el subgrupo formado a partir de dos generadores (el subgrupo no es cíclico), y como el subgrupo es abeliano, no es necesario que veamos la tabla de Cayley de Sage como una reflexión diagonal de la tabla obtenida en el ejemplo 5.2.

```
G = SymmetricGroup(5)
sigma = G("(4,5)")
tau = G("(1,3)")
H = G.subgroup([sigma, tau])
H.list()
```

```
[(), (1,3), (4,5), (1,3)(4,5)]
```

```
text_names = ['id', 'sigma', 'tau', 'mu']
H.cayley_table(names=text_names)
```

```
    *     id sigma   tau    mu
     +------------------------
   id|    id sigma   tau    mu
sigma| sigma    id    mu   tau
  tau|   tau    mu    id sigma
   mu|    mu   tau sigma    id
```

Grupo de Movimientos de un Cubo

Podríamos imitar el ejemplo en el texto y crear elementos de S_4 como permutaciones de las diagonales. Una construcción más obvia, pero menos esclarecedora, es considerar las 8 esquinas del cubo como los elementos a permutar. Entonces algunas simetrías obvias del cubo provienen de pasar un eje por los centros de dos caras opuestas, con cuartos de vueltas y medias vueltas en torno a estos ejes. Con tres ejes y cuatro rotaciones por eje, obtenemos 12 simetrías, excepto que hemos contado la identidad tres veces.

Etiquete las cuatro esquinas superiores del 1 al 4, poniendo el 1 en la esquina delantera-izquierda, y continuando en sentido horario visto desde arriba. Use del 5 al 8 para las esquinas inferiores, de manera que 5 quede directamente bajo el 1, 6 bajo 2, etc. Usaremos cuartos de vuelta, en sentido horario, en torno a cada eje, mirando desde arriba, el frente y el lado derecho respectivamente.

```
G = SymmetricGroup(8)
above = G("(1,2,3,4)(5,6,7,8)")
front = G("(1,4,8,5)(2,3,7,6)")
right = G("(1,2,6,5)(3,7,8,4)")
cube = G.subgroup([above, front, right])
cube.order()
```

```
24
```

```
cube.list()
```

```
[(), (1,2,3,4)(5,6,7,8), (1,2,6,5)(3,7,8,4),
 (1,4,8,5)(2,3,7,6), (1,6,8)(2,7,4), (2,4,5)(3,8,6),
 (1,3,8)(2,7,5), (1,6)(2,5)(3,8)(4,7), (1,3,6)(4,7,5),
 (1,3)(2,4)(5,7)(6,8), (1,8)(2,7)(3,6)(4,5),
     (1,7)(2,3)(4,6)(5,8),
 (1,4)(2,8)(3,5)(6,7), (1,5,6,2)(3,4,8,7), (1,5,8,4)(2,6,7,3),
 (1,7)(2,6)(3,5)(4,8), (1,7)(2,8)(3,4)(5,6),
     (1,4,3,2)(5,8,7,6),
 (1,5)(2,8)(3,7)(4,6), (1,2)(3,5)(4,6)(7,8), (1,8,6)(2,4,7),
 (2,5,4)(3,6,8), (1,6,3)(4,5,7), (1,8,3)(2,5,7)]
```

Como sabemos por la discusión en el texto que el grupo de simetrías tiene 24 elementos, vemos que estos tres generadores son suficientes para crear todas las simetrías. Esto sugiere varias preguntas que se pueden encontrar en el Ejercicio 5.5.4.

5.5 Ejercicios en Sage

Estos ejercicios tienen el objetivo de familiarizarle con los grupos de permutaciones en Sage.

1. Cree el grupo simétrico completo S_{10} con el comando `G = SymmetricGroup(10)`.

2. Cree elementos de `G` con los siguientes métodos. Preste atención a las comas, comillas, corchetes, paréntesis. Los primeros dos usan cadenas de caracteres (texto) como entrada, imitando la forma en que escribimos las permutaciones (pero con comas). La siguientes dos usan listas de tuplas.

- `a = G("(5,7,2,9,3,1,8)")`
- `b = G("(1,3)(4,5)")`
- `c = G([(1,2),(3,4)])`
- `d = G([(1,3),(2,5,8),(4,6,7,9,10)])`

(a) Calcule a^3, bc, $ad^{-1}b$.

(b) Calcule los órdenes de cada uno de los elemetos individuales (`a` hasta `d`) usando un solo método de los elementos del grupo de permutaciones.

(c) Use el método `.sign()` para determinar si a, b, c, d son pares o impares.

(d) Cree dos subgrupos cíclicos de G con los comandos:

- `H = G.subgroup([a])`
- `K = G.subgroup([d])`

Liste, y estudie, los elementos de cada subgrupo. Sin usar Sage, indique el orden de cada subgrupo de K. Luego use Sage para construir un subgrupo de K de orden 10.

(e) Subgrupos más complicados se pueden formar usando dos o más generadores. Construya un subgrupo L de G con el comando `L = G.subgroup([b,c])`. Calcule el orden de L y liste todos sus elementos.

3. Construya el grupo de simetrías del tetrahedro (también es el grupo alternante en 4 símbolos, A_4) con el comando `A=AlternatingGroup(4)`. Usando herramientas tales como órdenes de elementos, y generadores de subgrupos, vea si puede encontrar *todos* los subgrupos de A_4 (cada uno exactamente una vez). Haga esto sin usar el método `.subgroups()` para justificar que su respuesta es correcta (aunque puede ser una forma conveniente de verificar su resultado). Escriba un resumen ordenado de su respuesta—no simplemente una lista larga escupida por Sage. La idea es usar Sage como una herramienta, en la medida en que sea necesario, pero básicamente su respuesta debe ser un párrafo conciso y/o una tabla. Esta es la única parte de esta tarea sin instrucciones precisas y claras, así es que dedique el tiempo suficiente a esta parte para que le quede bien. Ayuda: ningún subgrupo de A_4 requiere más de dos generadores.

4. La subsección Grupo de Movimientos de un Cubo describe las 24 simetrías de un cubo como un subgrupo del grupo simétrico S_8 generado por tres rotaciones. Conteste las siguientes preguntas sobre este grupo de simetrías.

(a) De la lista de elementos del grupo, ¿puede localizar la 10 rotaciones en torno a los ejes? (Ayuda: la identidad es fácil, las otras nueve nunca envían un símbolo en si mismo.)

(b) ¿Puede identificar las seis simetrías que son transposición de diagonales? (Ayuda: `[g for g in cube if g.order()== 2]` es un buen filtro inicial.)

(c) Verifique que cualquiera dos de las rotaciones (`above`, `front`, `right`) son suficientes para generar el grupo completo. ¿Cómo sabe que cada par genera el grupo completo?

(d) ¿Puede expresar una de las transposiciones diagonales como productos de rotaciones? Este puede ser un problema notablemente difícil, especialmente para un software. Se conoce como el "problema de las palabras."

(e) Numere las seis caras del cubo con los números del 1 al 6 (de cualquier forma que desee). Ahora considere las mismas tres simetrías usadas antes (rotaciones en cuarto de vuelta en torno a los ejes), pero ahora vistas como permutaciones de las seis caras. De esta manera, podemos construir cada simetría como un elemento de S_6. Verifique que el subgrupo generado por estas simetrías es el grupo completo de simetrías del cubo. Nuevamente, en lugar de usar tres generadores, intente usando solo dos.

5. Guarde su trabajo, y vea si puede lograr que Sage se caiga construyendo el subgrupo de S_{10} generado por los elementos `b` and `d` de orden 2 y 30 de antes. *No entregue* la lista de elementos de `N` como parte de su trabajo.

```
N = G.subgroup([b,d])
N.list()
```

¿Cuál es el orden de N?

6

Clases Laterales y Teorema de Lagrange

El Teorema de Lagrange, uno de los resultados más importantes en la teoría de grupos finitos, dice que el orden de un subgrupo debe dividir el orden del grupo completo. Este teorema entrega una poderosa herramienta para analizar los grupos finitos; da una idea de exactamente que subgrupos podemos esperar encontrar en un grupo finito. Esencial para la comprensión del Teorema de Lagrange es la noción de clase lateral.

6.1 Clases Laterales

Sea G un grupo y H un subgrupo de G. Defina una ***clase lateral izquierda*** de H con ***representante*** $g \in G$ como el conjunto

$$gH = \{gh : h \in H\}.$$

Las ***clases laterales derechas*** pueden ser definidas similiarmente como

$$Hg = \{hg : h \in H\}.$$

Si las clases laterales izquierda y derecha coinciden o si es claro del contexto a qué tipo de clases laterales nos estamos refiriendo, diremos *clase lateral* sin especificar izquierda o derecha.

Ejemplo 6.1. Sea H el subgrupo de $\mathbb{Z}_6$ que consiste de los elementos 0 y 3. Las clases laterales son

$$\begin{aligned} 0 + H = 3 + H &= \{0, 3\} \\ 1 + H = 4 + H &= \{1, 4\} \\ 2 + H = 5 + H &= \{2, 5\}. \end{aligned}$$

Las clases laterales de subgrupos de $\mathbb{Z}$ y $\mathbb{Z}_n$ siempre las escribiremos con la notación aditiva que hemos usado acá. En un grupo conmutativo, las clases laterales izquierdas y derechas son siempre idénticas.

Ejemplo 6.2. Sea H el subgrupo de S_3 definido por las permutaciones $\{(1), (123), (132)\}$. Las clases laterales izquierdas de H son

$$\begin{aligned} (1)H = (123)H = (132)H &= \{(1), (123), (132)\} \\ (12)H = (13)H = (23)H &= \{(12), (13), (23)\}. \end{aligned}$$

Las clases laterales derechas de H son exactamente las mismas que las clases laterales izquierdas:

$$H(1) = H(123) = H(132) = \{(1), (123), (132)\}$$
$$H(12) = H(13) = H(23) = \{(12), (13), (23)\}.$$

No siempre es el caso que una clase lateral derecha sea igual a una clase lateral izquierda. Sea K el subgrupo de S_3 definido por las permutaciones $\{(1), (12)\}$. Entonces las clases laterales izquierdas de K son

$$(1)K = (12)K = \{(1), (12)\}$$
$$(13)K = (123)K = \{(13), (123)\}$$
$$(23)K = (132)K = \{(23), (132)\};$$

pero, las clases laterales derechas de K son

$$K(1) = K(12) = \{(1), (12)\}$$
$$K(13) = K(132) = \{(13), (132)\}$$
$$K(23) = K(123) = \{(23), (123)\}.$$

El siguiente lema es bastante útil al tratar con clases laterales. (Dejamos su demostración como ejercicio.)

Lema 6.3. *Sea H un subgrupo de un grupo G y supongamos que $g_1, g_2 \in G$. Las siguientes condiciones son equivalentes.*

1. $g_1H = g_2H$;
2. $Hg_1^{-1} = Hg_2^{-1}$;
3. $g_1H \subset g_2H$;
4. $g_2 \in g_1H$;
5. $g_1^{-1}g_2 \in H$.

En todos los ejemplos que hemos visto, las clases laterales de un subgrupo H particionan el grupo mayor G. El siguiente teorema dice que esto siempre será el caso.

Teorema 6.4. *Sea H un subgrupo de un grupo G. Entonces las clases laterales izquierdas de H en G particionan G. Es decir, el grupo G es la unión disjunta de las clases laterales izquierdas de H en G.*

DEMOSTRACIÓN. Sean g_1H y g_2H dos clases laterales de H en G. Debemos mostrar que ya sea $g_1H \cap g_2H = \emptyset$ o $g_1H = g_2H$. Supongamos que $g_1H \cap g_2H \neq \emptyset$ y $a \in g_1H \cap g_2H$. Entonces por la definición de clase lateral izquierda, $a = g_1h_1 = g_2h_2$ para ciertos elementos h_1 y h_2 en H. Luego, $g_1 = g_2h_2h_1^{-1}$ y $g_1 \in g_2H$. Por el Lema 6.3, $g_1H = g_2H$. □

Nota 6.5. No hay nada especial en este teorema respecto a clases laterales izquierdas. Las clases laterales derechas también particionan G; la demostración de este hecho es exactamente la misma que para clases laterales izquierdas excepto que todas las multiplicaciones se deben hacer al lado opuesto de H.

Sea G un grupo y H un subgrupo de G. Se define el índice ***índice*** de H en G como el número de clases laterales izquierdas de H en G. Denotaremos este índice por $[G : H]$.

Ejemplo 6.6. Sea $G = \mathbb{Z}_6$ y sea $H = \{0, 3\}$. Entonces $[G : H] = 3$.

Ejemplo 6.7. Supongamos que $G = S_3$, $H = \{(1), (123), (132)\}$, y $K = \{(1), (12)\}$. Entonces $[G : H] = 2$ y $[G : K] = 3$.

Teorema 6.8. *Sea H un subgrupo de un grupo G. El número de clases laterales izquierdas de H en G es el mismo que el número de clases laterales derechas de H en G.*

Demostración. Sean $\mathcal{L}_H$ y $\mathcal{R}_H$ los conjuntos de clases laterales izquierdas y derechas respectivamente de H en G. Si podemos definir una función biyectiva $\phi : \mathcal{L}_H \to \mathcal{R}_H$, entonces habremos demostrado el teorema. Si $gH \in \mathcal{L}_H$, sea $\phi(gH) = Hg^{-1}$. Por el Lema 6.3, la función ϕ está bien definida; es decir, si $g_1H = g_2H$, entonces $Hg_1^{-1} = Hg_2^{-1}$. Para demostrar que ϕ es 1-1, supongamos que

$$Hg_1^{-1} = \phi(g_1H) = \phi(g_2H) = Hg_2^{-1}.$$

Nuevamente por el Lema 6.3, $g_1H = g_2H$. La función ϕ es sobre pues $\phi(g^{-1}H) = Hg$. □

6.2 Teorema de Lagrange

Proposición 6.9. *Sea H un subgrupo de G con $g \in G$ y definamos una función $\phi : H \to gH$ como $\phi(h) = gh$. La función ϕ es biyectiva; luego el número de elementos en H es el mismo que el número de elementos en gH.*

Demostración. Primero demostraremos que ϕ es 1-1. Supongamos que $\phi(h_1) = \phi(h_2)$ para ciertos elementos $h_1, h_2 \in H$. Debemos mostrar que $h_1 = h_2$, pero $\phi(h_1) = gh_1$ y $\phi(h_2) = gh_2$. Así $gh_1 = gh_2$, y por cancelación a la izquierda $h_1 = h_2$. Mostrar que ϕ es sobreyectiva es fácil. Por definición, todo elemento de gH es de la forma gh para cierto $h \in H$ y $\phi(h) = gh$. □

Teorema 6.10 (Lagrange)**.** *Sea G un grupo finito y sea H un subgrupo de G. Entonces $|G|/|H| = [G : H]$ es el número de clases laterales izquierdas diferentes de H en G. En particular, el número de elementos en H debe dividir al número de elementos en G.*

Demostración. El grupo G está particionado en $[G : H]$ clases lateralez izquierdas diferentes. Cada clase lateral izquierda tiene $|H|$ elementos; por lo tanto, $|G| = [G : H]|H|$. □

Corolario 6.11. *Supongamos que G es un grupo finito y que $g \in G$. Entonces el orden de g divide al número de elementos en G.*

Corolario 6.12. *Sea $|G| = p$ con p primo. Entonces G es cíclico y cualquier $g \in G$ tal que $g \neq e$ es un generador.*

Demostración. Sea g un elemento de G tal que $g \neq e$. Por el Corolario 6.11, el orden de g divide el orden del grupo. Como $|\langle g \rangle| > 1$, debe ser p. Luego, g genera G. □

El Corolario 6.12 sugiere que los grupos de orden primo p se ven de alguna manera como $\mathbb{Z}_p$.

Corolario 6.13. *Sean H y K sbgrupos de un grupo finito G tales que $G \supset H \supset K$. Entonces*

$$[G : K] = [G : H][H : K].$$

DEMOSTRACIÓN. Notemos que

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H][H : K]. \qquad \square$$

Nota 6.14 (El recíproco del Teorema de Lagrange es falso)**.** El grupo A_4 tiene orden 12; sin embargo, se puede demostrar que no tiene ningún subgrupo de orden 6. De acuerdo al Teorema de Lagrange, los subgrupos de un grupo de orden 12 pueden tener orden 1, 2, 3, 4, o 6. Pero no hay garantía de que existan subgrupos de todos los posibles órdenes. Para demostrar que A_4 no tiene un subgrupo de orden 6, supondremos que sí tiene un tal subgrupo H y buscaremos una contradicción. Como A_4 contiene ocho 3-ciclos, sabemos que H debe contener un 3-ciclo. Veremos que si H contiene un 3-ciclo, entonces debe contener más de 6 elementos.

Proposición 6.15. *El grupo A_4 no tiene subgrupo de orden 6.*

DEMOSTRACIÓN. Como $[A_4 : H] = 2$, hay solo dos clases laterales de H en A_4. En tanto una de las clases laterales es el mismo H, clases laterales derechas e izquierdas deben coincidir; por lo tanto, $gH = Hg$ o $gHg^{-1} = H$ para todo $g \in A_4$. Como existen ocho 3-ciclos en A_4, al menos uno de los 3-ciclos debe estar en H. Sin perder generalidad, supongamos que (123) está en H. Entonces $(123)^{-1} = (132)$ también debe estar en H. Como $ghg^{-1} \in H$ para todo $g \in A_4$ y todo $h \in H$ y

$$(124)(123)(124)^{-1} = (124)(123)(142) = (243)$$
$$(243)(123)(243)^{-1} = (243)(123)(234) = (142)$$

concluimos que H debe tener al menos los siete elementos

$$(1), (123), (132), (243), (243)^{-1} = (234), (142), (142)^{-1} = (124).$$

Por lo tanto, A_4 no tiene subgrupo de orden 6. $\square$

De hecho, podemos decir más sobre cuándo dos ciclos tienen el mismo largo.

Teorema 6.16. *Dos ciclos τ y μ en S_n tienen el mismo largo si y solo si existe $\sigma \in S_n$ tal que $\mu = \sigma\tau\sigma^{-1}$.*

DEMOSTRACIÓN. Supongamos que

$$\tau = (a_1, a_2, \ldots, a_k)$$
$$\mu = (b_1, b_2, \ldots, b_k).$$

Defina σ como la permutación

$$\begin{aligned} \sigma(a_1) &= b_1 \\ \sigma(a_2) &= b_2 \\ &\vdots \\ \sigma(a_k) &= b_k. \end{aligned}$$

Entonces $\mu = \sigma\tau\sigma^{-1}$.

Recíprocamente, supongamos que $\tau = (a_1, a_2, \ldots, a_k)$ es un k-cycle y $\sigma \in S_n$. Si $\sigma(a_i) = b$ y $\sigma(a_{(i \bmod k)+1}) = b'$, entonces $\mu(b) = b'$. Luego,

$$\mu = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k)).$$

Como σ es una biyección, μ es un ciclo del mismo largo que τ. $\square$

6.3 Teoremas de Fermat y Euler

La ***función*** ϕ de ***Euler*** es la función $\phi : \mathbb{N} \to \mathbb{N}$ definida por $\phi(n) = 1$ para $n = 1$, y, para $n > 1$, $\phi(n)$ es el número de enteros positivos m con $1 \leq m < n$ y $\text{mcd}(m, n) = 1$.

De la Proposición 3.4, sabemos que el orden de $U(n)$, el grupo de unidades en $\mathbb{Z}_n$, es $\phi(n)$. Por ejemplo, $|U(12)| = \phi(12) = 4$ como los números que son relativamente primos con 12 son 1, 5, 7, y 11. Para cualquier primo p, $\phi(p) = p - 1$. Enunciamos estos resultados en el siguiente teorema.

Teorema 6.17. *Sea $U(n)$ el grupo de unidades en $\mathbb{Z}_n$. Entonces $|U(n)| = \phi(n)$.*

El siguiente teorema de Leonhard Euler es un resultado importante en teoría de números.

Teorema 6.18 (Teorema de Euler)**.** *Sean a y n enteros tales que $n > 0$ y $\text{mcd}(a, n) = 1$. Entonces $a^{\phi(n)} \equiv 1 \pmod{n}$.*

DEMOSTRACIÓN. Por el Teorema 6.17 el orden de $U(n)$ es $\phi(n)$. Así, $a^{\phi(n)} = 1$ para todo $a \in U(n)$; y $a^{\phi(n)} - 1$ es divisible por n. Por lo tanto, $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Si consideramos el caso especial del Teorema de Euler en el que $n = p$ es primo y recordamos que $\phi(p) = p - 1$, obtenemos el siguiente resultado de Pierre de Fermat.

Teorema 6.19 (Pequeño Teorema de Fermat)**.** *Sea p un primo cualquiera y supongamos que $p \not| a$. Entonces*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Más aún, para cualquier entero b, $b^p \equiv b \pmod{p}$.

Sage Sage puede crear todos los subgrupos de un grupo, mientras el grupo no sea demasiado grande. También puede crear las clases laterales de un subgrupo.

Nota Histórica

Joseph-Louis Lagrange (1736–1813), nacido en Torino, Italia, tenía origen franco-italiano. Su talento por las matemáticas se hizo evidente desde muy temprana edad. Leonhard Euler reconoció sus habilidades cuando Lagrange, que tenía solo 19 años, le comunicó a Euler un trabajo que había realizado en el cálculo de variaciones. Ese año fue nombrado profesor de la Real Escuela de Artillería en Torino. A los 23 llegó a la Academia de Berlin. Federico el Grande había escrito a Lagrange proclamando que el "mejor rey de Europa" debía tener al "mejor matemático en Europa" en su corte. Durante 20 años Lagrange ocupó la posición dejada por su mentor, Euler. Sus trabajos incluyen contribuciones a la teoría de números, teoría de grupos, física y mecánica, el cálculo de variaciones, la teoría de ecuaciones y las ecuaciones diferenciales. Junto con Laplace y Lavoisier, Lagrange fue una de las personas responsables de crear el sistema métrico. Lagrange tuvo una gran influencia en el desarrollo de las matemáticas, dejando mucho a las próximas generaciones en cuanto a ejemplos y nuevos problemas a resolver.

6.4 Ejercicios

1. Supongamos que G es un grupo finito con un elemento g de orden 5 y un elemento h de orden 7. ¿Por qué debe ocurrir que $|G| \geq 35$?

2. Supongamos que G es un grupo finito con 60 elementos. ¿Cuáles son los órdenes de posibles subgrupos de G?

3. Demuestre o refute: Todo subgrupo de los enteros tiene índice finito.

4. Demuestre o refute: Todo subgrupo de los enteros tiene orden finito.

5. Liste las clases laterales izquierdas y derechas de los subgrupos en cada uno de los siguientes.

(a) $\langle 8 \rangle$ en $\mathbb{Z}_{24}$
(b) $\langle 3 \rangle$ en $U(8)$
(c) $3\mathbb{Z}$ en $\mathbb{Z}$
(d) A_4 en S_4
(e) A_n en S_n
(f) D_4 en S_4
(g) $\mathbb{T}$ en $\mathbb{C}^*$
(h) $H = \{(1), (123), (132)\}$ en S_4

6. Describa las clases laterales izquierdas de $SL_2(\mathbb{R})$ en $GL_2(\mathbb{R})$. ¿Cuál es el índice de $SL_2(\mathbb{R})$ en $GL_2(\mathbb{R})$?

7. Verifique el Teorema de Euler para $n = 15$ y $a = 4$.

8. Use el Pequeño Teorema de Fermat mara mostrar que si $p = 4n + 3$ es primo, entonces no hay solución de la ecuación $x^2 \equiv -1 \pmod{p}$.

9. Muestre que los enteros tienen índice infinito en el grupo aditivo de los números racionales.

10. Muestre que el grupo aditivo de los números reales tiene índice infinito en el grupo aditivo de los números complejos.

11. Sea H un subgrupo de un grupo G y supongamos que $g_1, g_2 \in G$. Demuestre que las siguientes condiciones son equivalentes.

(a) $g_1 H = g_2 H$
(b) $H g_1^{-1} = H g_2^{-1}$
(c) $g_1 H \subset g_2 H$
(d) $g_2 \in g_1 H$
(e) $g_1^{-1} g_2 \in H$

12. Si $ghg^{-1} \in H$ para todo $g \in G$ y $h \in H$, muestre que las clases laterales izquierdas son idénticas a las clases laterales derechas. Es decir, muestre que $gH = Hg$ para todo $g \in G$.

13. Que falla en la demostración del Teorema 6.8 si $\phi : \mathcal{L}_H \to \mathcal{R}_H$ está definida como $\phi(gH) = Hg$?

14. Supongamos que $g^n = e$. Muestre que el orden de g divide a n.

15. Muestre que cualquiera dos permutaciones $\alpha, \beta \in S_n$ tienen la misma estructura de ciclos si y solo si existe una permutación γ tal que $\beta = \gamma\alpha\gamma^{-1}$. Si $\beta = \gamma\alpha\gamma^{-1}$ para algún $\gamma \in S_n$, entonces α y β son ***conjugadas***.

16. Si $|G| = 2n$, demuestre que el número de elementos de orden 2 es impar. Use este resultado para demostrar que G debe contener un subgrupo de orden 2.

17. Supongamos que $[G : H] = 2$. Si a y b no están en H, muestre que $ab \in H$.

18. Si $[G : H] = 2$, demuestre que $gH = Hg$.

19. Sean H y K subgrupos de un grupo G. Demuestre que $gH \cap gK$ es una clase lateral de $H \cap K$ en G.

20. Sean H y K subgrupos de un grupo G. Defina una relación $\sim$ en G como $a \sim b$ si existe un $h \in H$ y un $k \in K$ tales que $hak = b$. Muestre que esta relación es de equivalencia. Las clases de equivalencia correspondientes se llaman ***clases laterales dobles***. Calcule las clases laterales dobles de $H = \{(1), (123), (132)\}$ en A_4.

21. Sea G un grupo cíclico de orden n. Muestre que hay exactamente $\phi(n)$ generadores para G.

22. Sea $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, donde $p_1, p_2, \ldots, p_k$ son primos distintos. Demuestre que

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

23. Muestre que

$$n = \sum_{d|n} \phi(d)$$

para todo entero positivo n.

6.5 Sage

Sage puede crear todos las clases laterales de un subgrupo, y todos los subgrupos de un grupo. Aunque estos métodos pueden ser algo lentos, hay muchas veces en que son mejores que experimentar con papel y lápiz, y pueden ser de gran ayuda para entender la estructura de los grupos finitos.

Clases Laterales

Sage creará todas las clases laterales derechas (o izquierdas) de un subgrupo. Escritas matemáticamente, las clases laterales son conjuntos, y el orden de los elementos dentro es irrelevante. En Sage, las listas son más naturales, y acá es una ventaja.

Sage crea las clases laterales de un subgrupo como lista de listas. Cada lista interna es una clase lateral particular. La primera clase lateral siempre es el subgrupo mismo, y el primer elemento de esta clase es la identidad. Cada una de las otrar clases se puede entender construída para tener su representante como primer elemento, y si usamos este elemento como representante, los elementos de la clase están en el mismo orden en que serían creados multiplicando este representante por los elementos de la primera clase (el subgrupo).

El parámetro opcional `side` puede ser `'right'` o `'left'`, y si no está explicitado, entonces por defecto se entregarán las clases laterales derechas. Las opciones se refieren a qué lado del producto está el representante. Note que ahora los resultados de Sage estarán "al revés" comparados con el texto. Acá hay un Ejemplo 6.2 reanudado, pero en un orden ligeramente diferente.

```
G = SymmetricGroup(3)
a = G("(1,2)")
H = G.subgroup([a])
rc = G.cosets(H, side='right'); rc
```

```
[[(), (1,2)], [(2,3), (1,3,2)], [(1,2,3), (1,3)]]
```

```
lc = G.cosets(H, side='left'); lc
```

```
[[(), (1,2)], [(2,3), (1,2,3)], [(1,3,2), (1,3)]]
```

Si miramos cuidadosamente, podemos ver la diferencia entre las clases laterales derechas y las izquierdas. Compare estas clases laterales con las del texto y note que derecha e izquierda están intercambiadas. No debiera ser un problema — solo téngalo presente.

```
G = SymmetricGroup(3)
b = G("(1,2,3)")
H = G.subgroup([b])
rc = G.cosets(H, side='right'); rc
```

```
[[(), (1,2,3), (1,3,2)], [(2,3), (1,3), (1,2)]]
```

```
lc = G.cosets(H, side='left'); lc
```

```
[[(), (1,2,3), (1,3,2)], [(2,3), (1,2), (1,3)]]
```

Si analizamos la lista compuesta, podemos ver que las clases laterales derechas y las izquierdas son las mismas. Veamos lo que piensa Sage:

```
rc == lc
```

```
False
```

Matemáticamente, necesitamos conjuntos, pero Sage está trabajado con listas ordenadas, y el orden importa. Sin embargo, si sabemos que nuestras listas no contienen duplicados (el método `.cosets()` nunca producirá duplicados) entonces podemos ordenar las listas y la verificación de igualdad tendrá el resultado esperado. Los elementos de un grupo de permutaciones tienen un orden definido para ellos — no es tan importante *cuál* es ese orden, solo que *algún* orden está definido. La función `sorted()` tomará cualquier lista devolviendo una versión ordenada. Así para cada lista de clases laterales, ordenaremos las clases individuales y luego ordenaremos la lista de clases ordenadas. Esta es una maniobra típica, aunque un poco complicada para las listas anidadas.

```
rc_sorted = sorted([sorted(coset) for coset in rc])
rc_sorted
```

```
[[(), (1,2,3), (1,3,2)], [(2,3), (1,2), (1,3)]]
```

```
lc_sorted = sorted([sorted(coset) for coset in lc])
lc_sorted
```

```
[[(), (1,2,3), (1,3,2)], [(2,3), (1,2), (1,3)]]
```

```
rc_sorted == lc_sorted
```

```
True
```

La lista de todas las clases laterales puede ser bastante larga (contendrá todos los elementos del grupo) y puede tomar varios segundos en ser completada, incluso para grupos pequeños. Existen formas más sofisticadas, y más rápidas, de estudiar clases laterales (como simplemente usar sus representantes), pero para entender estas técnicas es necesario tener más teoría.

Subgrupos

Sage puede calcular todos los subgrupos de un grupo. Esto puede producir una respuesta aún más larga que el método de clases laterales y puede ser mucho más lento, dependiendo de la estructura del grupo. La lista está ordenada según el tamaño de los subgrupos, con los más pequeños primero. Como una demostración, calcularemos primero una lista de todos los subgrupos de un grupo pequeño, y luego extraeremos uno de estos subgrupos de la liste para estudio posterior.

```
G = SymmetricGroup(3)
sg = G.subgroups(); sg
```

```
[Subgroup of (Symmetric group of order 3! as a permutation
    group) generated by [()],
 Subgroup of (Symmetric group of order 3! as a permutation
    group) generated by [(2,3)],
 Subgroup of (Symmetric group of order 3! as a permutation
    group) generated by [(1,2)],
 Subgroup of (Symmetric group of order 3! as a permutation
    group) generated by [(1,3)],
 Subgroup of (Symmetric group of order 3! as a permutation
    group) generated by [(1,2,3)],
 Subgroup of (Symmetric group of order 3! as a permutation
    group) generated by [(2,3), (1,2,3)]]
```

```
H = sg[4]; H
```

```
Subgroup of (Symmetric group of order 3! as a permutation
    group) generated by [(1,2,3)]
```

```
H.order()
```

```
3
```

```
H.list()
```

```
[(), (1,2,3), (1,3,2)]
```

```
H.is_cyclic()
```

```
True
```

La salida del método `.subgroups()` suele ser grande, y podemos estar interesados en las propiedades de ciertos subgrupos específicos (como en el ejemplo anterior) o preguntas más amplias como la "estructura de subgrupos" del grupo. Acá extendemos el Corolario 6.15. Note que Sage simplemente no *calcula* un subgrupo de orden 6 en A_4, esto no es un sustituto válido de una *demostración* como la dada para el corolario. Pero el resultado computacional nos anima para buscar la demostración teórica con mayor confianza.

```
G = AlternatingGroup(4)
sg = G.subgroups()
[H.order() for H in sg]
```

```
[1, 2, 2, 2, 3, 3, 3, 3, 4, 12]
```

Así que no vemos un subgrupo de orden 6 en la lista de subgrupos de A_4. Note como el Teorema de Lagrange (Teorema 6.10) está en evidencia — todos los subgrupos tienen órdenes que dividen a 12, el orden de A_4.

```
G = SymmetricGroup(4)
sg = G.subgroups()
[H.order() for H in sg]
```

```
[1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 4, 4,
    4,
 6, 6, 6, 6, 8, 8, 8, 12, 24]
```

Nuevamente, aprecie el Teorema de Lagrange en acción. Pero aún más interesante, S_4 tiene un subgrupo de orden 6. Cuatro de ello, para ser precisos. Estos cuatro subgrupos de orden 6 son similares entre ellos, ¿puede describirlos de forma simple (*antes* de escarbar el la lista `sg` para obtener más información)? Si quiere saber cuántos subgrupos tiene S_4, podría simplemente contar el número de subgrupos en la lista `sg`. La función `len()` hace esto para *cualquier* lista y es usualmente una forma sencilla de contar cosas.

```
len(sg)
```

```
30
```

Subgrupos de Grupos Cíclicos

Ahora que estamos más familiarizados con los grupos de permutaciones, y conocemos el método `.subgroups()`, podemos revisitar una idea del Capítulo 4. Los subgrupos de un grupo cíclico siempre son cíclicos, pero ¿cuántos hay y qué órdenes tienen?

```
G = CyclicPermutationGroup(20)
[H.order() for H in G.subgroups()]
```

```
[1, 2, 4, 5, 10, 20]
```

```
G = CyclicPermutationGroup(19)
[H.order() for H in G.subgroups()]
```

```
[1, 19]
```

Podríamos hacer esto todo el día, pero ahora que tiene Sage a su disposición, varíe el orden de `G` cambiando el valor de `n` y estudie varios de estos resultados. Quizás podría intentar un grupo cíclico de orden 24 y comparar con el grupo simétrico S_4 (arriba) que también tiene orden 24. ¿Se le ocurre alguna conjetura?

```
n = 8
G = CyclicPermutationGroup(n)
[H.order() for H in G.subgroups()]
```

```
[1, 2, 4, 8]
```

Función Phi de Euler

Para sumar a nuestras funciones de teoría de números del Capítulo 2, notemos que Sage pone a nuestra disposición la función ϕ de Euler como `euler_phi()`.

```
euler_phi(345)
```

```
176
```

Acá viene un experimento interesante que puede ejecutar múltiples veces.

```
m = random_prime(10000)
n = random_prime(10000)
m, n, euler_phi(m*n) == euler_phi(m)*euler_phi(n)
```

```
(5881, 1277, True)
```

¿Alguna otra conjetura? ¿Puede generalizar este resultado?

6.6 Ejercicios en Sage

Los siguientes ejercicios más que sobre clases laterales y subgrupos, son sobre el uso de Sage como herramienta experimental. Están diseñados para ayudarle a ser más eficiente y más expresivo, a la hora de escribir comandos en Sage. Tendremos muchas oportunidades de trabajar con clases laterales y subgrupos en los capítulos que vienen. Estos ejercicios no son tan guiados y su dificultad va en aumento. Están diseñados para explorar, o confirmar, resultados presentados en este o anteriores capítulos.

Importante: Debiese contestar cada uno de los últimos tres problemas con una sola línea (complicada) de Sage cuyo resultado sea `True`. Una "sola línea" quiere decir que tendrá varios comandos de Sage usados juntos de formas complejas. No quiere decir varios comandos Sage separados por punto y coma, tipeados en una sola línea. Asegúrese de incluir algunos pasos intermedios usados en construir su solución, pero usando rangos de números más pequeños para no abrumar al lector con demasiado para mirar. Esto le ayudará a usted y al corrector de su trabajo para tener confianza en que la versión final es correcta.

Cuando verifique la divisibilidad de enteros, recuerde que `range()` produce enteros comunes, cuya funcionalidad es básica. El comando `srange()` produce enteros Sage, que tienen más capacidades. (Vea el último ejercicio como ejemplo.) Y recuerde que una lista es una forma compacta de examinar muchas posibilidades a la vez.

1. Use `.subgroups()` para encontrar un ejemplo de un grupo G y un entero m, tal que (a) m divide el orden de G, y (b) G no tiene subgrupo de orden m. (No use el grupo A_4 como G, pues ese está en el texto.) Escriba una sola línea de código Sage que contenga toda la lógica necesaria para producir m como respuesta. (Puede darle un nombre simple a su grupo en una línea previa y luego referirse a él por ese nombre.) A continuación un ejemplo muy simple que le puede ayudar a estructurar su respuesta.

```
a = 5
b = 10
c = 6
d = 13
a.divides(b)
```

```
True
```

```
not (b in [c,d])
```

```
True
```

```
a.divides(b) and not (b in [c,d])
```

```
True
```

2. Ejemplifique el Pequeño Teorema de Fermat (en cualquiera de sus variantes) usando el número compuesto $391 = 17 \cdot 23$ como elección de base (ya sea a o b), y para p recorriendo todos los valores primos entre 100 y 1000.
Construya paulatinamente una solución — haga una lista de potencias (empezando por unos pocos primos), luego haga una lista de potencias reducidas en la aritmética modular, luego una lista de comparaciones con el valor predicho, luego verifique todos estos valores lógicos resultantes de la comparación. Esta es una estrategia útil en muchos problemas similares. Finalmente podrá escribir una sola línea que realice la verificación completa y devuelva `True`. A continuación hay algunas sugerencias de funciones útiles.

```
a = 20
b = 6
a.mod(b)
```

```
2
```

```
prime_range(50, 100)
```

```
[53, 59, 61, 67, 71, 73, 79, 83, 89, 97]
```

```
all([True, True, True, True])
```

```
True
```

```
all([True, True, False, True])
```

```
False
```

3. Verifique que el grupo de unidades mód n tiene orden $n - 1$ cuando n es primo, nuevamente para todos los primos entre 100 and 1000. Como antes, su resultado debe ser simplemente `True`, una única vez, indicando que la proposición respecto al orden es verdadera para todos los primos examinados. Como antes, construya su solución paso a paso, y con conjuntos menores de primos en el comienzo. Exprese su respuesta como una sola línea de código Sage.

4. Verifique el Teorema de Euler para todos los valores $0 < n < 100$ y para $1 \leq a \leq n$. Esto requerirá bucles `for` anidados con un condicional. Nuevamente, a continuación un pequeño ejemplo que puede ser útil para construir su línea única de código Sage. Note el uso de `srange()` en este ejemplo.

```
[a/b for a in srange(9) for b in srange(1,a) if gcd(a,b)==1]
```

```
[2, 3, 3/2, 4, 4/3, 5, 5/2, 5/3, 5/4, 6, 6/5,
 7, 7/2, 7/3, 7/4, 7/5, 7/6, 8, 8/3, 8/5, 8/7]
```

5. El grupo simétrico en 7 símbolos, S_7, tiene $7! = 5040$ elementos. Considere las siguientes preguntas sin utilizar Sage, basado en lo que sabemos sobre los órdenes de los elementos en grupos de permutaciones (Ejercicio 5.3.13).

- ¿Cuál es el mayor orden posible?
- ¿Cuántos elementos hay de orden 10?
- ¿Cuántos elementos hay de orden 1?
- ¿Cuántos elementos hay de orden 2?
- ¿Cuál es el menor entero positivo para el que no hay elemento de ese orden?

Estas pregunta resultan más fáciles si sabe usar los coeficientes binomiales para contar en situaciones similarmenate complejas. En cualquier caso, reflexione seriamente sobre cada una de esta preguntas (y quizás alguna otra que se le ocurra) antes de lanzarse con Sage.
Ahora, calcule cuántos elementos hay de cada orden usando el método `.order()`, e incluya esto en una lista exhaustiva que contenga el número de elementos de cada orden. Puede verificar su trabajo (o el de Sage) usando el comando `sum()` para sumar esta lista y ojalá obteniendo 5040.
Comente el proceso de primero estudiar estas preguntas sin ayuda computacional, y luego nuevamente con Sage. ¿Para qué valores de n cree que Sage sería demasiado lento y su mente más rápida?

7

Introducción a la Criptografía

La Criptografía trata del envío y recepción de mensaje secretos. El objetivo de la criptografía es enviar mensajes de manera que solo el destinatario deseado pueda leerlos. Además, al recibirlo, el destinatario requiere de cierta garantía de autenticidad; es decir que no ha sido enviado por alguien que lo esté tratando de engañar. La criptografía moderna depende fuertemente del álgebra abstracta y de la teoría de números.

El mensaje a enviar lo llamaremos ***texto claro***. El mensaje encubierto se llamará ***texto cifrado***. Tanto el texto claro como el texto cifrado están escritos en un ***alfabeto***, que consiste de ***letras*** o ***caracteres***. Los caracteres pueden incluir no solamente las letras usuales como A, ..., Z y a, ..., z sino también dígitos, marcas de puntuación, y espacios. Un ***criptosistema***, o ***cifrado***, tiene dos partes: ***encriptación***, el proceso de transformar un texto claro en un texto cifrado, y ***decriptación***, la transformación inversa del texto cifrado al texto plano.

Hay diversas familias de criptosistemas, cada una se distingue por un algoritmo particular de encriptación. Los criptosistemas en una familia específica se distinguen entre ellos por un parámetro de la función de encriptación llamado ***key (clave)***. Un criptosistema clásico tiene una sola clave, que debe ser mantenida en secreto, solo conocida por el remitente y el destinatario del mensaje. Si una persona A desea enviar mensajes secretos a dos personas diferentes B y C, y no quiere que B entienda el mensaje enviado a C ni viceversa, entonces A debe usar dos claves diferentes, un criptosistema para intercambiar mensajes con B, y otro para intercambiar mensajes con C.

Los sistemas que usan dos claves separadas, una para encriptar y otra para decriptar, se conocen como ***criptosistemas de clave pública (public key cryptosystems)***. Como el conocimiento de la clave de encriptación no le permite a nadie adivinar la clave de decriptación, la primera se puede hacer pública. Un criptosistema de clave pública le permite tanto a A como a B enviar mensajes a C usando la misma clave de encriptación. Culquiera puede encriptar mensajes para enviarselos a C, pero solo C sabe como decriptar estos mensajes.

7.1 Criptografía de Llave Privada

En criptosistemas de clave ***única*** o ***criptosistema de clave privada*** la misma clave se usa tanto para encriptar como para decriptar los mensajes. Para encriptar un texto-claro, aplicamos al mensaje alguna función que se mantiene en secreto, digamos f. Esta función devuelve un mensaje encriptado. Dada la forma encriptada del mensaje, podemos recuperar el mensaje original aplicando la transformación inversa f^{-1}. La transformación f debe ser relativamente fácil

de calcular, así como también lo debe ser f^{-1}; pero, f tiene que ser muy difícil de adivinar a partir de ejemplos disponibles de mensajes encriptados.

Ejemplo 7.1. Uno de los primeros y más famosos criptosistemas fue el código de desplazamiento usado por Julio César. Primero convertimos el alfabeto en números haciendo $\mathrm{A} = 00, \mathrm{B} = 01, \ldots, \mathrm{Z} = 25$. La función codificadors será

$$f(p) = p + 3 \bmod 26;$$

es decir, $A \mapsto D, B \mapsto E, \ldots, Z \mapsto C$. La función decodificadora es entonces

$$f^{-1}(p) = p - 3 \bmod 26 = p + 23 \bmod 26.$$

Supongamos que recibimos el mensaje encriptado DOJHEUD. Para decriptar este mensaje, lo convertimos a números:

$$3, 14, 9, 7, 4, 20, 3.$$

Luego le aplicamos la transformación inversa para obtener

$$0, 11, 6, 4, 1, 17, 0,$$

es decir ALGEBRA. Note que no hay nada especial en los números 3 y 26, podríamos usar un alfabeto mayor o un desplazamiento diferente.

El ***criptoanálisis*** se preocupa de descifrar un mensaje encriptado recibido o interceptado. Existen Métodos de probabilidades y estadísticas que son de gran ayuda al descifrar mensajes interceptados; por ejemplo, el análisis de frecuencia de los caracteres que aparecen en el mensaje encriptado puede hacer posible su decriptación.

Ejemplo 7.2. Supongamos que recibimos un mensaje que sabemos fue encriptado usando un desplazamiento en las 26 letras del alfabeto. Para determinar el desplazamiento ocupado, debemos encontrar b en la ecuación $f(p) = p + b \bmod 26$. Podemos hacer esto usando análisis de frecuencia. La letra $\mathrm{E} = 04$ es la más frecuente en el idioma inglés. Supongamos que $\mathrm{S} = 18$ es la letra que ocurre con más frecuencia en el texto-cifrado. Entonces tenemos una buena razón para sospechar que $18 = 4 + b \bmod 26$, y $b = 14$. Por lo tanto, la función encriptadora más probable es

$$f(p) = p + 14 \bmod 26.$$

La correspondiente función decriptadora es

$$f^{-1}(p) = p + 12 \bmod 26.$$

En este punto es fácil determinar si la sospecha es o no correcta.

Códigos de desplazamiento simple son ejemplos de ***criptosistemas monoalfabéticos***. En estos cifrados un caracter en el texto-cifrado representa exactamente un caracter en el mensaje original. Tales criptosistemas no son muy sofisticados y son muy fáciles de romper. De ehcho, en un desplazamiento simple como el descrito en el Ejemplo 7.1, existen solo 26 claves posibles. Sería muy fácil probarlas todas en lugar de usar el análisis de frecuencia.

Investigemos un criptosistema ligeramente más sofisticado. Supongamos que la función encriptadora está dada por

$$f(p) = ap + b \bmod 26.$$

Primero debemos determinar cuándo existe una función decriptadora f^{-1}. Tal función existe cuando podemos resolver la ecuación

$$c = ap + b \bmod 26$$

en p. Por la Proposición 3.4, esto es posible precisamente cuando a tiene inverso, es decir cuando $\mcd(a, 26) = 1$. En este caso

$$f^{-1}(p) = a^{-1}p - a^{-1}b \bmod 26.$$

Un criptosistema de este tipo se denomina ***criptosistema afín***.

Ejemplo 7.3. Consideremos el criptosistema afín $f(p) = ap + b \bmod 26$. Para que este criptosistema funcione, debemos elegir $a \in \mathbb{Z}_{26}$ que sea invertible. Esto solo es posible si $\mcd(a, 26) = 1$. Reconociendo deste hecho, elegiremos $a = 5$ pues $\mcd(5, 26) = 1$. Es muy fácil ver que $a^{-1} = 21$. Por lo tanto, podemos definir nuestra función de encriptación como $f(p) = 5p + 3 \bmod 26$. Luego, ALGEBRA se encripta como $3, 6, 7, 23, 8, 10, 3$, o DGHXIKD. La función decriptadora será

$$f^{-1}(p) = 21p - 21 \cdot 3 \bmod 26 = 21p + 15 \bmod 26.$$

Un criptosistema sería más seguro si una letra del texto-cifrado pudiese representar más de una letra del texto-claro. Para dar un ejemplo de este tipo de criptosistema, llamado ***criptosistema polialfabético***, generalizaremos los códigos afines usando matrices. La idea funciona básicamente como antes; sin embargo, en lugar de encriptar una letra a la vez, encriptaremos pares de letras. Podemo almacenar un par de letras p_1 y p_2 en un vector

$$\mathbf{p} = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}.$$

Sea A una matriz invertible de 2×2 con coeficientes en $\mathbb{Z}_{26}$. Podemos definir una función encriptadora como

$$f(\mathbf{p}) = A\mathbf{p} + \mathbf{b},$$

donde $\mathbf{b}$ es un vector columna fijo y las operaciones matriciales se llevan a cabo en $\mathbb{Z}_{26}$. La función decriptadora debe ser

$$f^{-1}(\mathbf{p}) = A^{-1}\mathbf{p} - A^{-1}\mathbf{b}.$$

Ejemplo 7.4. Supongamos que deseamos encriptar la palabra HELP. Los números correspondientes son $7, 4, 11, 15$. Si

$$A = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix},$$

entonces

$$A^{-1} = \begin{pmatrix} 2 & 21 \\ 25 & 3 \end{pmatrix}.$$

Si $\mathbf{b} = (2, 2)^{\mathrm{t}}$, entonces el mensaje encriptado queda como RRGR. La letra R representa más de una letra en el texto-claro.

Análisis de frecuencia aún es realizable en un criptosistema polialfabético, pues tenemos buena información sobre la frecuencia relativa de pares de letras en el idioma inglés. El par *th* aparece con gran frecuencia; el par *qz* nunca aparece. Para evitar decriptación por parte de un tercero, debemos usar una matriz de mayor tamaño que la usada en el Ejemplo 7.4.

7.2 Criptografía de Llave Pública

Si se usan criptosistemas tradicionales, cualquiera que sea capaz de encriptar un mensaje, también tendrá información suficiente para decriptar un mensaje interceptado. En 1976, W. Diffie y M. Hellman propusieron la criptografía de clave pública, que está basada en la observación de que los procesos de encriptación y decriptación no necesitan tener la misma clave. Esto quita el requerimiento de que la clave de encriptación sea secreta. La función encriptadora f debe ser relativamente fácil de calcular, pero f^{-1} tiene que ser muy difícil de calcular sin alguna información adicional, de manera que alguien que conozca la clave de encriptación, no pueda descubrir la clave de decriptación sin pasar por cálculos prohibitivamente difíciles. Es interesante notar que hasta la fecha para ningún método propuesto se ha demostrado que es "unidireccional;" es decir, para ningún criptosistema de clave pública existente, se ha demostrado que sea computacionalmente prohibitivo descifrar el mensaje con el solo conocimiento de la clave de encriptación.

El Criptosistema RSA

El Criptosistema RSA introducido por R. Rivest, A. Shamir, y L. Adleman en 1978, se basa en la dificultad de factorizar número grandes. Si bien no es difícil encontrar dos primos aleatorios grandes y multiplicarlos, factorizar un número de 150 dígitos que sea el producto de dos primos grandes requería de 100 millones de computadores operando 10 millones de instrucciones por segundo durante 50 millones de años con los mejores algoritmos conocidos a principios de la década de 1990. Si bien los algoritmos se han mejorado, factorizar un producto de dos primos grandes sigue siendo computacionalmente prohibitivo.

El Criptosistema RSA funciona como sigue. Supongamos que escogemos al azar dos números primos p y q de 150 dígitos cada uno. Después calculamos su producto $n = pq$ y también calculamos $\phi(n) = m = (p-1)(q-1)$, donde ϕ es la función ϕ de Euler. Ahora comenzamos a elegir enteros aleatorios E hasta que encontremos uno que sea relativamente primo con m; es decir, elegimos E tal que $\text{mcd}(E, m) = 1$. Usando el algoritmo de Euclides, podemos encontrar un número D tal que $DE \equiv 1 \pmod{m}$. Los números n y E ahora se hacen públicos.

Supongamos que la persona B (Bob) desea enviar a la persona A (Alice) un mensaje a través de un canal abierto (público). Como E y n son conocidos para todo el mundo, cualquiera puede encriptar mensajes. Bob primero convierte su mensaje en una cadena numérica de acuerdo a algún procedimiento, digamos $\text{A} = 00, \text{B} = 02, \ldots, \text{Z} = 25$. Si es necesario, descompondrá su mensaje de manera que cada pedazo sea un entero positivo menor a n. Supongamos que x es uno de estos pedazos. Bob forma el número $y = x^E \mod n$ y envía y a Alice. Para que Alice recupere x, ella solo necesita calcular $x = y^D \bmod n$. Solo Alice conoce D.

Ejemplo 7.5. Antes de explorar la teoría tras el criptosistema RSA o intentar usar enteros grandes, usaremos algunos enteros pequeños simplemente para ver que el sistema realmente funciona. Supongamos que el mensaje que deseamos enviar, una vez digitalizado es 25. Sean $p = 23$ y $q = 29$. Entonces

$$n = pq = 667$$

y

$$\phi(n) = m = (p-1)(q-1) = 616.$$

Podemos elegir $E = 487$, pues $\text{mcd}(616, 487) = 1$. El mensaje codificado lo calculamos como

$$25^{487} \bmod 667 = 169.$$

Este cálculo se puede realizar de forma razonable usando el método de los cuadrados repetidos descrito en el Capítulo 4. Usando el algoritmo de Euclides, determinamos que $191E = 1 + 151m$; Por lo tanto, la clave de decriptación es $(n, D) = (667, 191)$. Podemos recuperar el mensaje original calculando

$$169^{191} \bmod 667 = 25.$$

Examinemos ahora por qué funciona el criptosistema RSA. Sabemos que $DE \equiv 1 \pmod{m}$; luego, existe k tal que

$$DE = km + 1 = k\phi(n) + 1.$$

Debemos considerar dos casos. En el primer caso supongamos que $\text{mcd}(x, n) = 1$. Entonces, por el Teorema 6.18,

$$y^D = (x^E)^D = x^{DE} = x^{km+1} = (x^{\phi(n)})^k x = (1)^k x = x \bmod n.$$

De esta manera vemos que Alice recupera el mensaje original x cuando calcula $y^D \bmod n$.

Para el otro caso, supongamos que $\text{mcd}(x, n) \neq 1$. Como $n = pq$ y $x < n$, sabemos que x es un múltiplo de p o un múltiplo de q, pero no ambos. Describiremos solo la primera posibilidad, pues la otra es completamente similar. Entonces existe un entero r, con $r < q$ y $x = rp$. Notemos que tenemos $\text{mcd}(x, q) = 1$ y que $m = \phi(n) = (p-1)(q-1) = \phi(p)\phi(q)$. Entonces, usando el Teorema 6.18, pero ahora mód q,

$$x^{km} = x^{k\phi(p)\phi(q)} = (x^{\phi(q)})^{k\phi(p)} = (1)^{k\phi(p)} = 1 \bmod q.$$

Existe un entero t tal que $x^{km} = 1 + tq$. Luego, Alice también recupera el mensaje en este caso,

$$y^D = x^{km+1} = x^{km}x = (1 + tq)x = x + tq(rp) = x + trn = x \bmod n.$$

Podemos preguntarnos ahora como uno intentaría violar el criptosistema RSA. Para encontrar D dados n y E, necesitamos factorizar n y encontrar D usando el algoritmo de Euclides. Si supiéramos que $667 = 23 \cdot 29$ en el Ejemplo 7.5, podríamos recuperar D.

Verificación del Mensaje

Hay un problema de verificación de mensajes en los criptosistemas de clave pública. Como la clave codificadora es de público conocimiento, cualquiera tiene la capacidad de enviar un mensaje codificado. Si Alice recibe un mensaje de Bob, a ella le gustaría poder verificar que realmente fue Bob quien envió el mensaje. Supongamos que la clave encriptadora de Bob es (n', E') y su clave decriptadora es (n', D'). Además, supongamos que la clave encriptadora de Alice es (n, E) y que su clave decriptadora es (n, D). Como las claves encriptadoras son de conocimiento público, ambos pueden intercambiar mensajes cuando lo deseen. Bob quiere poder asegurarle a Alice que el mensaje que le está enviando es auténtico. Antes de enviar el mensaje x a Alice, Bob decripta x con su propia clave secreta:

$$x' = x^{D'} \bmod n'.$$

Cualquiera puede transformar x' de vuelta a x encriptando, pero solo Bob tiene la habilidad de formar x'. Ahora Bob encripta x' con la clave pública de Alice formando

$$y' = {x'}^E \bmod n,$$

un mensaje que solo Alice puede decriptar. Alice decripta el mensaje y luego encripta el resultado con la clave de encriptación de Bob para leer el mensaje original, un mensaje que solo puede haber sido enviado por Bob.

Nota Histórica

La idea de encriptar mensajes secretos se remonta a la Antiguedad. Como sabemos, Julio César usaba un código de desplazamiento simple para enviar y recibir mensajes. Sin embargo, el estudio formal de la codificación y decodificación de mensajes probablemente comenzó con los árabes en el siglo XV. En los siglos XV y XVI, matemáticos como Alberti y Viete descubrieron que los criptosistemas monoalfabéticos no ofrecían ninguna seguridad real. En el siglo XIX, F. W. Kasiski estableció métodos para violar sistemas en los que una letra del texto encriptado puede representar más de una letra del texto claro, si la misma clave era usada varias veces. Este descubrimiento llevó al uso de criptosistemas con claves que se usaban solo una vez. La Criptografía obtuvo fundamentos matemáticos firmes con los trabajos de gente como W. Friedman y L. Hill a comienzos del siglo XX.

El período que siguió a la Primera Guerra Mundial vio el desarrollo de máquinas especializadas para la encriptación y decriptación de mensajes, y los matemáticos trabajaron muy activamente en criptografía durante la Segunda Guerra Mundial. Los esfuerzos por penetrar los criptosistemas de las naciones del Eje fueron organizados en Inglaterra y en los Estados Unidos por matemáticos notables como Alan Turing y A. A. Albert. Los Aliados obtuvieron una tremenda ventaja en la Segunda Guerra Mundial al romper los sistemas de encriptación producidos por la máquina Enigma de Alemania y los cifrados Púrpura de Japón.

Hacia 1970, el interés en la criptografía comercial comenzó a solidificarse. Había una necesidad creciente de proteger transacciones bancarias, datos informáticos y correo electrónico. A comienzos de los 70, IBM desarrolló e implementó LUZIFER, el precursor de estándar de encriptación de datos del National Bureau of Standards de Estados Unidos.

El concepto de un criptosistema de clave pública, debido a Diffie y Hellman, es muy reciente (1976). Su desarrollo fue continuado por Rivest, Shamir, y Adleman con el criptosistema RSA (1978). No se sabe qué tan seguros son estos criptosistemas. El criptosistema de la mochila de decisión, desarrollado por Merkle y Hellman, ya fue roto. Es aún una pregunta abierta si el sistema RSA puede o no ser roto. En 1991, los Laboratorios RSA publicaron una lista de semiprimos (números que tienen exactamente dos factores primos) con un premio en dinero para quien pudiera factorizarlos (http://www.emc.com/emc-plus/rsa-labs/historical/the-rsa-challenge-numbers.htm). Si bien el desafío terminó en 2007, muchos de estos números aún no han sido factorizados.

Ha habido bastante controversia en relación a la investigación de criptosistemas, la criptografía en sí. En 1929, cuando Henry Stimson, Secretario de Estado de Herbert Hoover, disolvió la Cámara Negra (la división de criptografía del Departamento de Estado) con la justificación ética de que "los caballeros no leen la correspondencia de otros." Durante las últimas dos décadas del siglo XX, la Agencia Nacional de Seguridad (NSA) quería mantener en secreto la información sobre criptografía, mientras la comunidad científica peleó por el derecho de publicar la ciencia básica relacionada. Actualmente, la

investigación en criptografía matemática y la teoría de números computacional es muy activa, y los matemáticos tienen la libertad de publicar sus resultados en estas áreas.

Sage El desarrollo inicial de Sage tuvo rutinas poderosas para la teoría de números, y luego comenzó a incluir estructuras algebraicas y otras áreas de las matemáticas discretas. Es por lo tanto una herramienta natural para el estudio de criptografía, incluyendo tópicos tales como RSA, criptografía de curvas elípticas, y AES (Advanced Encryption Standard o estándar avanzado de encriptación).

7.3 Ejercicios

1. Encripte `IXLOVEXMATH` usando el criptosistema del Ejemplo 7.1.

2. Decodifique `ZLOOA WKLVA EHARQ WKHA ILQDO`, que fue codificado usando el criptosistema del Ejemplo 7.1.

3. Suponiendo que un código monoalfabético fue usado para codificar el siguiente mensaje secreto, ¿cuál era el mensaje original?

```
APHUO EGEHP PEXOV FKEUH CKVUE CHKVE APHUO
EGEHU EXOVL EXDKT VGEFT EHFKE UHCKF TZEXO
VEZDT TVKUE XOVKV ENOHK ZFTEH TEHKQ LEROF
PVEHP PEXOV ERYKP GERYT GVKEG XDRTE RGAGA
```

¿Cuál es la importancia de este mensaje en la historia de la criptografía?

4. ¿Cuál es el número total de criptosistemas monoalfabéticos posibles? ¿Qué tan seguros son tales criptosistemas?

5. Demuestre que una matriz A de 2×2 con coeficientes en $\mathbb{Z}_{26}$ es invertible si y solo si $\text{mcd}(\det(A), 26) = 1$.

6. Dada la matriz

$$A = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix},$$

use la función de encriptación $f(\mathbf{p}) = A\mathbf{p} + \mathbf{b}$ para encriptar el mensaje `CRYPTOLOGY`, donde $\mathbf{b} = (2, 5)^{\text{t}}$. ¿Cuál es la función de decriptación?

7. Encripte cada uno de los siguientes mensajes RSA x de manera que x se divida en bloques de enteros de longitud 2; es decir, si $x = 142528$, entonces encripte 14, 25, y 28 por separado.

(a) $n = 3551, E = 629, x = 31$

(b) $n = 2257, E = 47, x = 23$

(c) $n = 120979, E = 13251, x = 142371$

(d) $n = 45629, E = 781, x = 231561$

8. Calcule la llave de decriptación D para cada una de la llaves de encriptación en el Ejercicio 7.

9. Decripte cada uno de los siguientes mensajes RSA y.

(a) $n = 3551, D = 1997, y = 2791$

(b) $n = 5893, D = 81, y = 34$

(c) $n = 120979, D = 27331, y = 112135$

(d) $n = 79403, D = 671, y = 129381$

10. Para cada una de las siguientes llaves de encriptación (n, E) en el criptosistema RSA, calcule D.

(a) $(n, E) = (451, 231)$

(b) $(n, E) = (3053, 1921)$

(c) $(n, E) = (37986733, 12371)$

(d) $(n, E) = (16394854313, 34578451)$

11. Los mensajes encriptados frecuentemente se dividen en bloques de n letras. Un mensaje como `THE WORLD WONDERS WHY` puede ser encriptado como `JIW OCFRJ LPOEVYQ IOC` pero enviado como `JIW OCF RJL POE VYQ IOC`. ¿Cuáles son las ventajas de usar bloques de n letras?

12. Encuentre enteros n, E, y X tales que

$$X^E \equiv X \pmod{n}.$$

¿Es este un potencial problema en el criptosistema RSA?

13. Toda persona en el curso debiera construir un criptosistema RSA usando primos que tengan entre 10 y 15 dígitos. Entregue (n, E) y un mensaje encriptado. Mantenga el secreto de D. Vean si pueden romper los cifrados de los demás.

7.4 Ejercicios Adicionales: Primalidad y Factorización

En el criptosistema RSA es importante ser capaz de encontrar números primos grandes con facilidad. Asimismo, este criptosistema deja de ser seguro si somos capaces de factorizar un número entero que sea el producto de dos números primos grandes. Las soluciones teóricas de ambos problemas son bastante simples. Para saber si un número n es primo o para factorizar n, podemos usar intentos de división. Simplemente dividimos n entre $d = 2, 3, \ldots, \sqrt{n}$. Ya sea obtendremos una factorización, o n es primo si ningún d divide a n. El problema es que tales cálculos toman muchísimo tiempo si n es muy grande.

1. Un mejor algoritmo para factorizar enteros positivos impares es el ***algoritmo de factorización de Fermat***.

(a) Sea $n = ab$ un número impar compuesto. Demuestre que n puede ser escrito como la diferencia de dos cuadrados perfectos:

$$n = x^2 - y^2 = (x - y)(x + y).$$

Por lo tanto, un entero positivo impar se puede factorizar si y solo si podemos encontrar enteros x e y tales que $n = x^2 - y^2$.

(b) Escriba un programa para implementar el siguiente algoritmo de factorización basado en la observación en la parte (a). La expresión `ceiling(sqrt(n))` se refiere al menor entero que es mayor o igual a la raíz cuadrada de n. Escriba otro programa que use intentos de división y compare la velocidad de los dos algoritmos. ¿Cuál de ellos es más rápido y por qué?

```
x := ceiling(sqrt(n))
y := 1

1 : while x^2 - y^2 > n do
        y := y + 1

if x^2 - y^2 < n then
        x := x + 1
        y := 1
        goto 1
else if x^2 - y^2 = 0 then
        a := x - y
        b := x + y
        write n = a * b
```

Listado 7.6: algoritmo en pseudo-código

2. (Verificación de Primalidad) Recuerde el Pequeño Teorema de Fermat del Capítulo 6. Sea p un primo con $\text{mcd}(a, p) = 1$. Entonces $a^{p-1} \equiv 1 \pmod{p}$. Podemos usar el Pequeño Teorema de Fermat como un examen para primos. Por ejemplo, 15 no puede ser primo pues

$$2^{15-1} \equiv 2^{14} \equiv 4 \pmod{15}.$$

Pero, 17 es potencialmente un primo pues

$$2^{17-1} \equiv 2^{16} \equiv 1 \pmod{17}.$$

Decimos que un número compuesto impar n es un ***pseudoprimo*** si

$$2^{n-1} \equiv 1 \pmod{n}.$$

¿Cuáles de los siguientes números son primos y cuáles son pseudoprimos?

(a) 342 (c) 601 (e) 771
(b) 811 (d) 561 (f) 631

3. Sea n un número impar compuesto y b un entero positivo tal que $\text{mcd}(b, n) = 1$. Si $b^{n-1} \equiv 1 \pmod{n}$, entonces n es un ***pseudoprimo en base*** b. Muestre que 341 es un pseudoprimo en base 2 pero no es un pseudoprimo en base 3.

4. Escriba un programa para determinar todos los primos menores a 2000 usando intentos de división. Escriba un segundo programa que determine todos los números menores a 2000 que sean primos o pseudoprimos. Compare la velocidad de ambos programas. ¿Cuántos pseudoprimos hay menores a 2000? Existen números compuestos que son pseudoprimos para todas la bases con que son relativamente primos. Estos números se llaman ***números de Carmichael***. El primer número de Carmichael es el $561 = 3 \cdot 11 \cdot 17$. En 1992, Alford, Granville, y Pomerance demostraron que hay infinitos números de Carmichael [4]. Pero, los números de Carmichael son muy escasos. Existen solo 2163 números de Carmichael menores a 25×10^9. Para tests de primalidad más sofisticados, vea [1], [6], o [7].

7.5 Referencias y Lecturas Recomendadas

[1] Bressoud, D. M. *Factorization and Primality Testing.* Springer-Verlag, New York, 1989.

[2] Diffie, W. and Hellman, M. E. "New Directions in Cryptography," *IEEE Trans. Inform. Theory* **22** (1976), 644–54.

[3] Gardner, M. "Mathematical games: A new kind of cipher that would take millions of years to break," *Scientific American* **237** (1977), 120–24.

[4] Granville, A. "Primality Testing and Carmichael Numbers," *Notices of the American Mathematical Society* **39**(1992), 696–700.

[5] Hellman, M. E. "The Mathematics of Public Key Cryptography," *Scientific American* **241**(1979), 130–39.

[6] Koblitz, N. *A Course in Number Theory and Cryptography.* 2nd ed. Springer, New York, 1994.

[7] Pomerance, C., ed. "Cryptology and Computational Number Theory", *Proceedings of Symposia in Applied Mathematics* **42**(1990) American Mathematical Society, Providence, RI.

[8] Rivest, R. L., Shamir, A., and Adleman, L., "A Method for Obtaining Signatures and Public-key Criptosistemas," *Comm. ACM* **21**(1978), 120–26.

7.6 Sage

Debido a que Sage comenzó como software para el apoyo de la investigación en teoría de números, podemos rápida y fácilmente mostrar los mecanismos internos por los que funciona el algoritmo RSA. Reconozcamos que, en la práctica, muchos otros detalles tales como la codificación entre letras y enteros, o la protección de la clave privada, son igualmente importantes para proteger la seguridad de la comunicación. RSA por si mismo es solo un fundamento teórico.

Construyendo claves

Supondremos que Alice quiere enviar un mensaje secreto a Bob, junto con un mensaje de verificación (también conocido como firma digital). Comenzaremos con la construcción de un par de claves (privada y pública) para Alice y para Bob. Primero necesitamos dos primos grandes y su producto para cada uno de ellos. En la práctica, los valores de n tendrían cientos de dígitos, en lugar de solo 21 como hemos hecho acá.

```
p_a = next_prime(10^10)
q_a = next_prime(p_a)
p_b = next_prime((3/2)*10^10)
q_b = next_prime(p_b)
n_a = p_a * q_a
n_b = p_b * q_b
n_a, n_b
```

```
(10000000520000000627, 225000000300000000091)
```

Computacionalmente, el valor de la función ϕ de Euler del producto de dos primos pq puede ser obtenida como $(p-1)(q-1)$, pero podemos igualmente usar la función interna de Sage.

```
m_a = euler_phi(n_a)
m_b = euler_phi(n_b)
m_a, m_b
```

```
(100000000500000000576, 225000000270000000072)
```

Ahora podemos crear los exponentes de encriptación y decriptación. Elegimos el exponente de encriptación como un número (pequeño) relativamente primo con el valor de m. Con Sage podemos factorizar m rápidamente para elegir este valor. En la práctica no querremos hacer este cálculo para valores grandes de m, así es que podemos más fácilmente elegir valores "aleatorios" y verificar hasta el primer valor relativamente primo con m. El exponente de decriptación es el inverso multiplicativo, mód m, del exponente de encriptación. Si construye un exponente de encriptación inadecuado (no relativamente primo con m), fallará el cálculo de este inverso multiplicativo (y Sage se lo dirá). Hacemos esto dos veces — para Alice y para Bob.

```
factor(m_a)
```

```
2^6 * 3 * 11 * 17 * 131 * 521 * 73259 * 557041
```

```
E_a = 5*23
D_a = inverse_mod(E_a, m_a)
D_a
```

```
20869565321739130555
```

```
factor(m_b)
```

```
2^3 * 3^4 * 107 * 1298027 * 2500000001
```

```
E_b = 7*29
D_b = inverse_mod(E_b, m_b)
D_b
```

```
24384236482463054195
```

En esta etapa, cada individuo publicaría sus valores de n y E, guardando D en forma privada y segura. En la práctica D debiese estar protegido en el disco duro del usuario por una clave que solo conozca el dueño. Para aún mayor seguridad, una persona podría tener solo dos copias de su clave privada, una en un pituto de memoria USB que siempre lleve consigo, y una copia de respaldo en su caja de seguridad en Sage. Cada vez que la persona use D deberá indicar su clave. El valor de m puede ser desechado. Para el registro, acá están todas las claves:

```
print("Alice's␣public␣key,␣n:", n_a, "E:", E_a)
```

```
Alice's␣public␣key,␣n:␣10000000052000000627␣E:␣115
```

```
print("Alice's␣private␣key,␣D:", D_a)
```

```
Alice's␣private␣key,␣D:␣20869565321739130555
```

```
print("Bob's␣public␣key,␣n:", n_b, "E:", E_b)
```

```
Bob's␣public␣key,␣n:␣22500000030000000091␣E:␣203
```

```
print("Bob's private key, D:", D_b)
```

```
Bob's private key, D: 24384236482463054195
```

Firmando y Encriptando un Mensaje

Alice construirá un mensaje que consiste de una palabra de cuatro letras en inglés. A partir de estas cuatro letras construiremos un número que represente el mensaje en la forma que necesitamos para usar en el algoritmo RSA. La función `ord()` convertirá una letra en su valor ASCII, un número entre 0 y 127. Si usamos estos números como "dígitos" mód 128, podemos estar seguros que la palabra de cuatro letras de Alice se codificará como un entero menor a $128^4 = 268,435,456$. El valor particular no tiene importancia, mientras sea menor que el valor de nuestro n pues toda la aritmética que sigue es mód n. Elegimos una palabra popular de cuatro letras, la convertimos en "dígitos" ASCII con una lista, y construimos el entero a partir de los dígitos en la base correcta. Note como podemos tratar la palabra como una lista y que el primer dígito en la lista está en el lugar de las "unidades".

```
word = 'Sage'
digits = [ord(letter) for letter in word]
digits
```

```
[83, 97, 103, 101]
```

```
message = ZZ(digits, 128)
message
```

```
213512403
```

Primero, Alice firmará su mensaje para proveer una verificación. Para eso usa su clave privada, pues esto es algo que solo ella debiese poder hacer.

```
signed = power_mod(message, D_a, n_a)
signed
```

```
47838774644892618423
```

Luego Alice encripta el mensaje de manera que solo Bob lo pueda leer. Para esto usa la clave pública de Bob. Note que no es siquiera necesario que conozca a Bob — por ejemplo, ella podría haber obtenido la clave pública de Bob en su página web o quizás Bob la publicó en el *New York Times*.

```
encrypted = power_mod(signed, E_b, n_b)
encrypted
```

```
111866209291209840488
```

La comunicación de Alice está lista para ser transmitida por cualquier red, no importando lo insegura que pueda ser y no importando cuánta gente pueda estar vigilándola.

Decriptación y Verificación del Mensaje

Ahora supongamos que el valor de `encrypted` a llegado a Bob. Bob podría no conocer a Alice ni necesariamente creer que ha recibido un mensaje genuinamente enviado por ella. Un adversario podría estar tratando de confundir a

Bob enviándole mensajes supuestamente provenientes de Alice. Primero, Bob debe deshacer la encriptación hecha por Alice. Esto es algo que solo Bob, como el receptor intencionado, debiese ser capaz de realizar. Y lo hace usando su clave privada, que solo él conoce, y que ha mantenido segura.

```
decrypted = power_mod(encrypted, D_b, n_b)
decrypted
```

```
47838774644892618423
```

En este momento, el mensaje no tiene gran significado para Bob. Cualquiera podría haberle enviado un mensaje encriptado. Pero, este era un mensaje firmado por Alice. Deshagamos ahora la firma. Notemos que esto requiere la clave pública de Alice. Bob no necesita conocer a Alice — por ejemplo podría obtener la clave pública de Alice de su página web o quizás Alice la publicó en el *New York Times*.

```
received = power_mod(decrypted, E_a, n_a)
received
```

```
213512403
```

Bob necesita transformar esta representación entera de vuelta a una palabra con letras. La función `chr()` convierte valores ASCII en letras, y usamos una lista para hacer esto en forma repetida.

```
digits = received.digits(base=128)
letters = [chr(ascii) for ascii in digits]
letters
```

```
['S', 'a', 'g', 'e']
```

Si queremos un resultado más legible, podemos combinar estas letras en una cadena.

```
''.join(letters)
```

```
'Sage'
```

Bob está contento de haber recibido un mensaje tan interesante de Alice. ¿Qué habría sucedido si un impostor hubiese enviado un mensaje pretendiendo ser de Alice, o si un adversario hubiese interceptado y adulterado el mensaje original de Alice? (Lo segundo es lo que se conoce como un ataque de "hombre en el medio".)

En cualquiera de estos casos, el tercero no sería capaz de duplicar la primera acción de Alice — firmar su mensaje. Si un adversario firma de alguna manera el mensaje, o lo altera en cualquier forma, el resultado cuando Bob deshaga la firma producirá pura basura. (Inténtelo!) Como Bob recibió una palabra legítima, con la mayúscula apropiada, puede confiar en que el mensaje que obtuvo es el mismo que fue firmado por Alice. En la práctica, si Alice envía varios cientos de palabras en su mensaje, la probabilidad de obtener un texto coherente a partir de un mensaje adulterado, es astronómicamente pequeña.

¿Qué hemos mostrado?

1. Alice puede enviar mensajes que solo Bob puede leer.
2. Bob puede recibir mensajes secretos de cualquiera.
3. Alice puede firmar mensajes, de manera que Bob sabe que provienen genuinamente de Alice.

Por supuesto, sin hacer nuevas claves, se pueden intercambiar los roles de Alice y Bob. Y si Carol hace un par de claves, ella se puede comunicar tanto con Alice como con Bob de la misma forma.

Si usted desea usar encriptación RSA de clave pública seriamente, investigue el software GNU Privacy Guard, aka GPG, que está libremente disponible en www.gnupg.org/. Notemos que solo tiene sentido usar programas de encriptación que le permitan conocer el código fuente.

7.7 Ejercicios en Sage

1. Construya un par de claves para Alice usando los primeros dos primos mayores a 10^{12}. Para su elección de E, use un primo y use el menor posible. Obtenga los valores de n, E, y D para Alice. Luego use comandos de Sage para verificar que las claves de encriptación y decriptación de Alice son inversos multiplicativos.

2. Construya un par de claves para Bob usando los primeros dos primos mayores a $2 \cdot 10^{12}$. Para su elección de E, use un primo y use el menor posible. Obtenga los valores de n, E, y D para Alice.
Codifique la palabra `Math` usando valores ASCII de la forma descrita en esta sección (mantenga las mayúsculas como se muestran). Cree un mensaje firmado de esta palabra para una comunicación de Alice a Bob. Obtenga los tres enteros: el mensaje, el mensaje firmado, y el mensaje firmado, encriptado.

3. Muestre como Bob transformaría el mensaje recibido de Alice de vuelta a la palabra `Math`. Obtenga tanto los valores intermedios como el resultado final.

4. Cree un nuevo mensaje firmado de Alice para Bob. Simule una adulteración del mensaje sumando 1 al entero recibido por Bob, antes que el lo decripte. ¿Qué resultado obtiene Bob para las letras del mensaje cuando decripta y de-firma el mensaje adulterado?

5. (Ejercicio para la Sala de Clases) Organice el curso en grupos pequeños. Haga que cada grupo construya un par de claves con algún tamaño mínimo (dígitos en n). Cada grupo debiese guardar su clave privada en secreto, pero dejar disponible para todo el curso su clave pública. Podría ser escrita en la pizarra o pegada en un lugar público como `pastebin.com`. Luego cada grupo puede enviar un mensaje a otro grupo, donde los grupos podrían estar organizados lógicamente en un círculo para este propósito. Por supueso, los mensajes se deben transmitir públicamente también. Espere una tasa de éxito entre el 50% y el 100%.
Si no hace esto en clase, consiga un compañero de estudios e intercambie mensajes de la misma forma.

8

Teoría Algebraica de Códigos

La teoría de códigos es una aplicación del álgebra que se ha vuelto cada vez más importante durante las últimas décadas. Cuando transmitimos datos, estamos preocupados de transmitir datos a través de un canal que podría estar afectado por "ruido." Queremos ser capaces de codificar y decodificar la información de forma de poder detectar, y posiblemente corregir, los errores causados por el ruido. Esta situación surge en muchas áreas de comunicación, incluyendo la radio, telefonía, televisión, comunicaciones entre computadores, y tecnologías de almacenamiento digital. Probabilidades, combinatoria, teoría de grupos, álgebra lineal y anillos de polinomios sobre cuerpos finitos todos tienen un rol importante en la teoría de códigos.

8.1 Códigos para Detectar y para Corregir Errores

Consideremos un modelo simple de sistema de comunicaciones para el envío y recepción de mensajes codificados (ver la Figura 8.1).

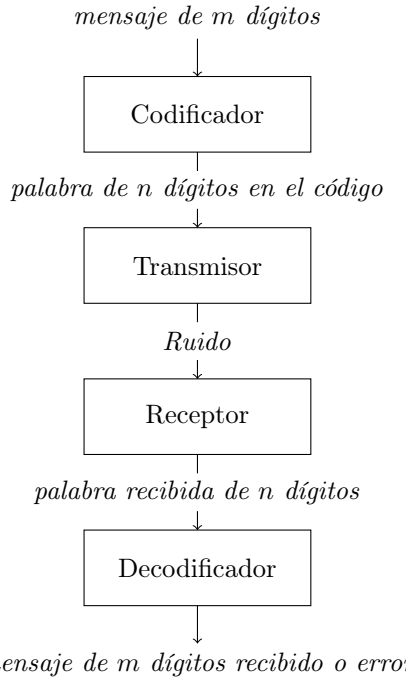


Figura 8.1: Codificar y Decodificar Mensajes

Mensajes sin codificar pueden estar compuestos de letras o caracteres, pero típicamente consisten de m-tuplas binarias. Estos mensajes se codifican en palabras de un código, que son n-tuplas binarias, a través de un mecanismo llamado ***codificador***. El mensaje es transmitido y luego decodificado. Consideraremos la aparición de errores durante la transmisión. Un ***error*** occure si hay un cambio en uno o más bits de la palabra del código. Un ***protocolo decodificador*** es un método que ya sea convierte n-tupla arbitraria recibida en un mensaje decodificado coherente o da un mensaje de error para esa n-tupla. Si el mensaje recibido es una palabra del código (una de las n-tuplas permitidas), entonces el mensaje decodificado debe ser el mensaje que fue codificado en la palabra del código. Para tuplas recibidas que no están en el código, el protocolo dará una indicación de error, o, si somos más astutos, tratará de corregir el error y reconstruir el mensaje original. Nuestro objetivos es transmitir mensajes libres de errores de la forma más barata y rápida posible.

Ejemplo 8.2. Un posible mecanismo de codificación sería enviar el mensaje múltiples veces y comparar las copias recibidas entre ellas. Supongamos que el mensaje a codificar es una n-tupla binaria $(x_1, x_2, \ldots, x_n)$. El mensaje se codifica en una $3n$-tupla binaria simplemente repitiendo el mensaje tres veces:

$$(x_1, x_2, \ldots, x_n) \mapsto (x_1, x_2, \ldots, x_n, x_1, x_2, \ldots, x_n, x_1, x_2, \ldots, x_n).$$

Para decodificar el mensaje, escogemos como el i-ésimo dígito el que aparezca en la i-ésima posición de al menos dos de las tres transmisiones. Por ejemplo, si el mensaje original es (0110), entonces el mensaje transmitido será (0110 0110 0110). Si hay un error de transmisión en el quinto dígito, entonces la palabra recibida será (0110 1110 0110), la que será correctamente decodificada como (0110).[1] Este método de repetición-triple automáticamente detecta y corrige todos los errores individuales, pero es lento e ineficiente: para enviar un mensaje que consista de n bits, se requieren $2n$ bits adicionales, y solo podemos detectar y corregir errores individuales. Veremos que es posible encontrar mecanismos de codificación que codifiquen un mensaje de n bits en uno de m bits con m mucho menor a $3n$.

Ejemplo 8.3. ***La paridad***, un mecanismo de codificación usual, es mucho más eficiente que la simple repetición. El código ASCII (American Standard Code for Information Interchange) usa 8-tuplas binarias, dando lugar a $2^8 = 256$ 8-tuplas posibles. Pero, solo se necesitan 7 bits pues solo hay $2^7 = 128$ caracteres ASCII. ¿Qué se puede o debe hacer con el bit restante? Usando los ocho dígitos, podemos detectar un error individual de transmisión. Por ejemplo, los códigos ASCII para A, B, y C son

$$\begin{aligned} \text{A} &= 65_{10} = 01000001_2, \\ \text{B} &= 66_{10} = 01000010_2, \\ \text{C} &= 67_{10} = 01000011_2. \end{aligned}$$

Note que el bit de más a la izquierda siempre es 0; es decir, los 128 caracteres ASCII tienen códigos

$$\begin{aligned} 00000000_2 &= 0_{10}, \\ &\vdots \\ 01111111_2 &= 127_{10}. \end{aligned}$$

[1] Adoptaremos la convención de numerar los dígitos de izquierda a derecha en las n-tuplas binarias.

El bit puede ser usado para controlar errores en los otros siete bits. Se pone como 0 o 1 de manera que el número total de bits 1 en la representación del caracter sea par. Usando paridad, los códigos para A, B, y C se convierten en

$$\begin{aligned} \text{A} &= 01000001_2, \\ \text{B} &= 01000010_2, \\ \text{C} &= 11000011_2. \end{aligned}$$

Supongamos que se envía una A y ocurre un error de transmisión en el sexto bit de manera que se recibe (0100 0101). Sabemos que se produjo un error pues se recibió un número impar de unos, y podemos pedir que la palabra sea retransmitida. Cuando se usa para detectar errores, el bit de más a la izquierda se llama ***bit de control de paridad***.

Por lejos el mecanismo más común de detección de errores en los computadores está basado en la adición de un bit de paridad. Típicamente, un computador guarda la información en m-tuplas llamadas ***palabras***. Largos comunes para las palabras son 8, 16, y 32 bits. Un bit en la palabra se reserva como bit de control de paridad, y no se usa para almacenar información. Este bit se pone como 0 o 1, dependiendo del número de unos de la palabra.

Agregar un control de paridad permite la detección de todos los errores únicos pues cualquier cambio a un solo bit, ya sea aumenta o disminuye en uno el número de unos, y en cualquier caso cambia la paridad de par a impar, de manera que la nueva palabra no es una palabra del código.

El sistema de paridad es fácil de implementar, pero tiene dos desventajas. En primer lugar, errores múltiples no son detectables. Supongamos que se envía una A y se alteran el primer y séptimo dígitos en la transmisión. La palabra recibida resulta ser una palabra del código, pero será decodificada como una C en lugar de una A. En segundo lugar, no tenemos la habilidad de corregir errores. Si la 8-tupla (1001 1000) es recibida, sabemos que ha ocurrido un error, pero no tenemos idea cuál es el bit que se ha cambiado. Investigaremos ahora un mecanismo de codificación que no solo nos permita detectar errores de transmisión, sino que nos permita corregirlos.

Palabra	Palabra Recibida							
Transmitida	000	001	010	011	100	101	110	111
000	0	1	1	2	1	2	2	3
111	3	2	2	1	2	1	1	0

Cuadro 8.4: Un código de repetición

Ejemplo 8.5. Supongamos que nuestro mensaje original es 0 o 1, y que 0 se codifica en (000) y 1 se codifica en (111). Si ocurre solo un error durante la transmisión, entonces podemos detectar y corregir este error. Por ejemplo, si se recibe un 101, entonces el segundo bit debe haber sido cambiado de 1 a 0. La palabra transmitida debe haber sido (111). Este método detecterá y corregirá todos los errores únicos.

En la Tabla 8.4, presentamos todas las posibles palabras que pueden ser recibidas para las palabras transmitidas (000) y (111). La Tabla 8.4 también muestra el número de bits en los que cada 3-tupla difiere de la palabra original.

Decodificación de Probabilidad Máxima

El mecanismo de codificación presentado en el Ejemplo 8.5 no es una solución completa del problema pues no toma en cuenta la posibilidad de múltiples er-

rores. Por ejemplo, ya sea un (000) o un (111) se podría enviar y se podría recibir un (001). No tenemos forma de decidir a partir de la palabra recibida si se cometió un solo error en el tercer bit o dos errores, uno en el primer bit y uno en el segundo. Sin importar el mecanismo de codificación usado, un mensaje incorrecto puede ser recibido. Podríamos transmitir un (000), tener errores en los tres bits, y recibir la palabra (111) del código. Es importante explicitar las suposiciones hechas sobre la probabilidad y distribución de los errores de transmisión de manera que, en una aplicación particular, se sabrá si un cierto mecanismo de detección de errores es apropiado. Supondremos que los errores de transmisión son infrecuentes, y, que cuando ocurren, ocurren de forma independiente en cada bit; es decir, si p es la probabilidad de un error en un bit y q es la probabilidad de error en otro bit, entonces la probabilidad de errores en ambos bits al mismo tiempo, es pq. También supondremos que una n-tupla recibida se decodificará en la palabra del código que esté más cerca; es decir, suponemos que el receptor usa ***decodificación de probabilidad máxima***.[2]

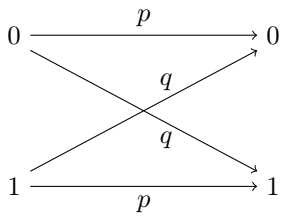


Figura 8.6: Canal binario simétrico

Un ***canal binario simétrico*** es un modelo que consiste de un transmisor capaz de enviar una señal binaria, ya sea un 0 o un 1, junto a un receptor. Sea p la probabilidad de que la señal se recibe correctamente. Entonces $q = 1-p$ es la probabilidad de recepción incorrecta. Si se envía un 1, entonces la probabilidad de recibir un 1 es p y la probabilidad de recibir un 0 es q (Figura 8.6). La probabilidad de que no ocurra ningún error durante la transmisión de una palabra binaria del código de largo n es p^n. Por ejemplo, si $p = 0.999$ y se envía un mensaje consistente de 10,000 bits, entonces la probabilidad de una transmisión perfecta es

$$(0.999)^{10,000} \approx 0.00005.$$

Teorema 8.7. *Si una n-tupla binaria $(x_1, \ldots, x_n)$ es transmitida por un canal binario simétrico con probabilidad p de que no ha ocurrido error en cada coordenada, entonces la probabilidad de que no haya errores en exactamente k coordenadas es*

$$\binom{n}{k} q^k p^{n-k}.$$

Demostración. Fijemos k coordenadas diferentes. Calculemos primero la probabilidad de que un error ha ocurrido en este conjunto fijo de coordenadas. La probabilidad de que haya ocurrido un error en una en particular de estas k coordenadas es q; la probabilidad de que ningún error haya ocurrido en una de las restantes $n-k$ coordenadas es p. La probabilidad de cada una de estos n eventos independientes es $q^k p^{n-k}$. El número posible de patrones de error con exactamente k errores es igual a

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

[2]Esta sección requiere conocimientos de probabilidad, pero puede saltarse sin pérdida de continuidad.

el número de combinaciones de k cosas elegidas entre un total de n. Cada uno de estos patrones de error tiene probabilidad $q^k p^{n-k}$ de ocurrir; luego, la probabilidad de todos estos patrones de error es

$$\binom{n}{k} q^k p^{n-k}. \qquad \square$$

Ejemplo 8.8. Supongamos que $p = 0.995$ y que se envía un mensaje de 500-bits. La probabilidad de que el mensaje haya sido enviado sin errores es

$$p^n = (0.995)^{500} \approx 0.082.$$

La probabilidad de que ocurra exactamente un error es

$$\binom{n}{1} qp^{n-1} = 500(0.005)(0.995)^{499} \approx 0.204.$$

La probabilidad de exactamente dos errores es

$$\binom{n}{2} q^2 p^{n-2} = \frac{500 \cdot 499}{2}(0.005)^2(0.995)^{498} \approx 0.257.$$

La probabilidad de más de dos errores es aproximadamente

$$1 - 0.082 - 0.204 - 0.257 = 0.457.$$

Códigos de Bloque

Si vamos a desarrollar códigos eficientes para detectar y corregir errores, necesitaremos herramientas matemáticas más sofisticadas. La teoría de grupos permitirá métodos más rápidos y eficientes para codificar y decodificar mensajes. Un código es un ***código de bloque*** (n, m) si la información que se codificará se puede dividir en bloques de m dígitos binarios, cada uno de los cuales puede ser codificado en n dígitos binarios. Más específicamente, un código de bloque (n, m) consiste de una ***función codificadora***

$$E : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$$

y una ***función decodificadora***

$$D : \mathbb{Z}_2^n \to \mathbb{Z}_2^m.$$

Una ***palabra del código*** es cualquier elemento en la imagen de E. También requerimos que E sea 1-1 de manera que dos bloques de información no sean codificados en la misma palabra del código.

Ejemplo 8.9. El código de paridad desarrollado para detectar errores individuales en caracteres ASCII es un código de bloque $(8, 7)$. La función codificadora es

$$E(x_7, x_6, \ldots, x_1) = (x_8, x_7, \ldots, x_1),$$

donde $x_8 = x_7 + x_6 + \cdots + x_1$ con la suma en $\mathbb{Z}_2$.

Sean $\mathbf{x} = (x_1, \ldots, x_n)$ y $\mathbf{y} = (y_1, \ldots, y_n)$ n-tuplas binarias. La ***distancia de Hamming*** o ***distancia***, $d(\mathbf{x}, \mathbf{y})$, entre $\mathbf{x}$ e $\mathbf{y}$ es el número de bits en que $\mathbf{x}$ e $\mathbf{y}$ difieren. La distancia entre dos palabras del código es el mínimo número de errores de transmisión necesarios para transformar una de las palabras en la otra. La ***distancia mínima*** para un código, $d_{\min}$, es el mínimo de todas las distancias $d(\mathbf{x}, \mathbf{y})$, donde $\mathbf{x}$ e $\mathbf{y}$ son palabras distintas del código. El ***peso***, $w(\mathbf{x})$, de una palabra de un código binario $\mathbf{x}$ es el número de unos en $\mathbf{x}$. Claramente, $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$, donde $\mathbf{0} = (00 \cdots 0)$.

Ejemplo 8.10. Sean $\mathbf{x} = (10101)$, $\mathbf{y} = (11010)$, y $\mathbf{z} = (00011)$ todas las palabras en un código C. Entonces tenemos las siguientes distancias de Hamming:

$$d(\mathbf{x}, \mathbf{y}) = 4, \qquad d(\mathbf{x}, \mathbf{z}) = 3, \qquad d(\mathbf{y}, \mathbf{z}) = 3.$$

La distancia mínima para este código es 3 y los pesos son:

$$w(\mathbf{x}) = 3, \qquad w(\mathbf{y}) = 3, \qquad w(\mathbf{z}) = 2.$$

La siguiente proposición lista algunas propiedades básicas sobre el peso de una palabra del código y la distancia entre dos palabras del código. La demostración se deja como ejercicio.

Proposición 8.11. *Sean* $\mathbf{x}$, $\mathbf{y}$, *y* $\mathbf{z}$ *n-tuplas binarias. Entonces*

1. $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$;
2. $d(\mathbf{x}, \mathbf{y}) \geq 0$;
3. $d(\mathbf{x}, \mathbf{y}) = 0$ *si y solo si* $\mathbf{x} = \mathbf{y}$;
4. $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$;
5. $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$.

Los pesos en un código particular son usualmente mucho más fáciles de calcular que las distancias de Hamming entre todas las palabras del código. Si un código se construye cuidadosamente, podemos sacar provecho de este hecho.

Supongamos que $\mathbf{x} = (1101)$ e $\mathbf{y} = (1100)$ son palabras en algún código. Si transmitimos (1101) y un error ocurre en el bit de más a la derecha, entonces se recibirá (1100). Como (1100) es una palabra del código, el decodificador decodificará (1100) como el mensaje transmitido. Este código claramente no es muy apropiado para la detección de errores. El problema es que $d(\mathbf{x}, \mathbf{y}) = 1$. Si $\mathbf{x} = (1100)$ e $\mathbf{y} = (1010)$ son palabras del código, entonces $d(\mathbf{x}, \mathbf{y}) = 2$. Si $\mathbf{x}$ se transmite y ocurre un solo error, entonces $\mathbf{y}$ nunca puede ser recibido. La Tabla 8.12 entrega las distancias entre todas las palabras del código de 4-bits en que los primeros tres bits son de información y el cuarto es un bit de control de paridad. Podemos ver que la distancia mínima acá es 2; luego, el código es apto como código de detección de un error.

	0000	0011	0101	0110	1001	1010	1100	1111
0000	0	2	2	2	2	2	2	4
0011	2	0	2	2	2	2	4	2
0101	2	2	0	2	2	4	2	2
0110	2	2	2	0	4	2	2	2
1001	2	2	2	4	0	2	2	2
1010	2	2	4	2	2	0	2	2
1100	2	4	2	2	2	2	0	2
1111	4	2	2	2	2	2	2	0

Cuadro 8.12: Distancias entre palabras de código de 4-bit

Para determinar exactamente cuáles son las capacidades de detección y corrección de errores de un código, debemos analizar la distancia mínima para el código. Sean $\mathbf{x}$ e $\mathbf{y}$ palabras del código. Si $d(\mathbf{x}, \mathbf{y}) = 1$ y ocurre un error donde difieren $\mathbf{x}$ e $\mathbf{y}$, entonces $\mathbf{x}$ se transforma en $\mathbf{y}$. La palabra recibida es $\mathbf{y}$

y no se produce ningún mensaje de error. Ahora supongamos que $d(\mathbf{x}, \mathbf{y}) = 2$. Entonces un único error no puede transformar $\mathbf{x}$ en $\mathbf{y}$. Por lo tanto, si $d_{\min} = 2$, tenemos la habilidad de detectar errores únicos. Pero, supongamos que $d(\mathbf{x}, \mathbf{y}) = 2$, $\mathbf{y}$ es enviado, y se recibe una palabra $\mathbf{z}$ que no está en el código tal que

$$d(\mathbf{x}, \mathbf{z}) = d(\mathbf{y}, \mathbf{z}) = 1.$$

Entonces el decodificador no puede decidir entre $\mathbf{x}$ e $\mathbf{y}$. Si bien estamos concientes de que se cometió un error, no sabemos cuál fue ese error.

Supongamos que $d_{\min} \geq 3$. Entonces el algoritmo de decodificación de máxima probabilidad corrige todos los errores únicos. Comenzando con una palabra $\mathbf{x}$ del código, un error de un único bit en la transmisión da $\mathbf{y}$ con $d(\mathbf{x}, \mathbf{y}) = 1$, pero $d(\mathbf{z}, \mathbf{y}) \geq 2$ para cualquier otra palabra $\mathbf{z} \neq \mathbf{x}$ del código. Si no necesitamos corregir errores, entonces podemos detectar más de un error cuando un código tiene distancia mínima mayor o igual a 3.

Teorema 8.13. *Sea C un código con $d_{\min} = 2n + 1$. Entonces C puede corregir cualquiera n o menos errores. Alternativamente, $2n$ o menos errores cualquiera pueden ser detectados con C.*

Demostración. Supongamos que se envía una palabra $\mathbf{x}$ del código y que se recibe la palabra $\mathbf{y}$ con a lo más n errores. Entonces $d(\mathbf{x}, \mathbf{y}) \leq n$. Si $\mathbf{z}$ es cualquier palabra del código distinta de $\mathbf{x}$, entonces

$$2n + 1 \leq d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \leq n + d(\mathbf{y}, \mathbf{z}).$$

Luego, $d(\mathbf{y}, \mathbf{z}) \geq n + 1$ e $\mathbf{y}$ será decodificada correctamente como $\mathbf{x}$. Ahora supongamos que se transmite $\mathbf{x}$ recibiéndose $\mathbf{y}$ y que al menos uno pero no más de $2n$ errores han ocurrido. Entonces $1 \leq d(\mathbf{x}, \mathbf{y}) \leq 2n$. Como la distancia mínima entre palabras del código es $2n + 1$, $\mathbf{y}$ no puede ser una palabra del código. Así, el código puede detectar entre hasta $2n$ errores. □

Ejemplo 8.14. En la Tabla 8.15, las palabras $\mathbf{c}_1 = (00000)$, $\mathbf{c}_2 = (00111)$, $\mathbf{c}_3 = (11100)$, y $\mathbf{c}_4 = (11011)$ determinan un código corrector de un error.

	00000	00111	11100	11011
00000	0	3	3	4
00111	3	0	4	3
11100	3	4	0	3
11011	4	3	3	0

Cuadro 8.15: Distancias de Hamming para un código corrector de errores

Nota Histórica

La teoría moderna de códigos comenzó en 1948 con la publicación de C. Shannon, titulada "A Mathematical Theory of Information" [7]. En su artículo, Shannon ofreció un ejemplo de un código algebraico, y el Teorema de Shannon estableció precisamente qué tan bueno puede llegar a ser un código. Richard Hamming comenzó a trabajar con códigos lineales en Bell Labs a finales de los 1940s y principios de los 1950s después de sufrir la frustración de que los programas que corría no eran capaces de recuperarse de simples errores generados por ruido. La teoría de códigos ha crecido tremendamente en las décadas siguientes a estos trabajos. *The Theory of Error-Correcting Codes*, de MacWilliams y Sloane [5], publicado en 1977, ya contenía más de 1500 citas.

Códigos lineales (códigos de bloque $(32, 6)$ de Reed-Muller) fueron usados en las sondas espaciales Mariner de la NASA. Sondas espaciales posteriores como los Voyager han usado los llamados códigos de convolución. Actualmente, hay investigación activa respecto a códigos Goppa, que dependen fuertemente de geometría algebraica.

8.2 Códigos Lineales

Para ganar más información sobre un código particular y desarrollar técnicas más eficientes de codificación, decodificación y detección de errores, necesitaremos agregar mayor estructura a nuestros códigos. Una forma de lograr esto es pedir que el código además sea un grupo. Un ***código de grupo*** o ***código lineal***es un código que además es un subgrupo de $\mathbb{Z}_2^n$.

Para verificar que un código es un código de grupo, solo necesitamos verificar una cosa. Si sumamos dos elementos en el código, el resultado debe ser una n-tupla que nuevamente esté en el código. No es necesario verificar que el elemento inverso de la n-tupla esté en el código, pues cada palabra del código es su propio inverso, tampoco es necesario verificar que $\mathbf{0}$ sea una palabra del código. Por ejemplo,

$$(11000101) + (11000101) = (00000000).$$

Ejemplo 8.16. Supongamos que tenemos un código que consiste de las siguientes 7-tuplas:

(0000000)	(0001111)	(0010101)	(0011010)
(0100110)	(0101001)	(0110011)	(0111100)
(1000011)	(1001100)	(1010110)	(1011001)
(1100101)	(1101010)	(1110000)	(1111111).

Es una tarea sencilla, aunque tediosa la de verificar que este código es un subgrupo de $\mathbb{Z}_2^7$ y que por lo tanto, es un código de grupo. Este código detecta un error y corrige un error, pero calcular todas las distancias entre pares de palabras del código para determinar que $d_{\min} = 3$ es un proceso largo y tedioso. Es mucho más sencillo ver que el peso mínimo de todas las palabras no nulas es 3. Como veremos pronto, esto no es una coincidencia. Pero la relación entre pesos y distancias en un código particular es fuertemente dependiente del hecho que el código sea un grupo.

Lema 8.17. *Sean* $\mathbf{x}$ *e* $\mathbf{y}$ *n-tuplas binarias. Entonces* $w(\mathbf{x} + \mathbf{y}) = d(\mathbf{x}, \mathbf{y})$.

Demostración. Supongamos que $\mathbf{x}$ e $\mathbf{y}$ son n-tuplas binarias. Entonces la distancia entre $\mathbf{x}$ e $\mathbf{y}$ es exactamente el número de lugares en los que difieren $\mathbf{x}$ e $\mathbf{y}$. Pero $\mathbf{x}$ e $\mathbf{y}$ difieren en una coordenada particular si y solo si la suma es 1 en esa coordenada, pues

$$\begin{aligned} 1 + 1 &= 0 \\ 0 + 0 &= 0 \\ 1 + 0 &= 1 \\ 0 + 1 &= 1. \end{aligned}$$

Así, el peso de la suma es igual a la distancia entre las dos palabras. □

Teorema 8.18. *Sea* $d_{\min}$ *la distancia mínima para un código de grupo* C. *Entonces* $d_{\min}$ *es el mínimo de todos los pesos de las palabras no nulas en* C. *Es decir,*

$$d_{\min} = \min\{w(\mathbf{x}) : \mathbf{x} \neq \mathbf{0}\}.$$

DEMOSTRACIÓN. Observe que

$$\begin{aligned} d_{\min} &= \min\{d(\mathbf{x},\mathbf{y}) : \mathbf{x} \neq \mathbf{y}\} \\ &= \min\{d(\mathbf{x},\mathbf{y}) : \mathbf{x}+\mathbf{y} \neq \mathbf{0}\} \\ &= \min\{w(\mathbf{x}+\mathbf{y}) : \mathbf{x}+\mathbf{y} \neq \mathbf{0}\} \\ &= \min\{w(\mathbf{z}) : \mathbf{z} \neq \mathbf{0}\}. \end{aligned}$$

□

Códigos Lineales

Del Ejemplo 8.16, es ahora fácil verificar que el mínimo peso distinto de cero es 3; luego, el código realmente detecta y corrige todos los errores individuales. Hemos reducido el problema de encontrar "buenos" códigos al de generar códigos de grupo. Una forma fácil de generar códigos de grupo, es emplear un poco de teoría de matrices.

Se define el ***producto interno*** de dos n-tuplas binarias como

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 + \cdots + x_ny_n,$$

donde $\mathbf{x} = (x_1, x_2, \ldots, x_n)^{\mathrm{t}}$ e $\mathbf{y} = (y_1, y_2, \ldots, y_n)^{\mathrm{t}}$ son vectores columna.[3] Por ejemplo, si $\mathbf{x} = (011001)^{\mathrm{t}}$ e $\mathbf{y} = (110101)^{\mathrm{t}}$, entonces $\mathbf{x} \cdot \mathbf{y} = 0$. También podemos pensar el producto interno como el producto de un vector fila con un vector columna; es decir,

$$\begin{aligned} \mathbf{x} \cdot \mathbf{y} &= \mathbf{x}^{\mathrm{t}}\mathbf{y} \\ &= \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \\ &= x_1y_1 + x_2y_2 + \cdots + x_ny_n. \end{aligned}$$

Ejemplo 8.19. Supongamos que las palabras a ser codificadas consisten de todas las 3-tuples binarias y que nuestro mecanismo de codificación es el de control de paridad. Para codificar una 3-tupla arbitraria, agregamos un cuarto bit para obtener un número par de unos. Note que una n-tupla arbitraria $\mathbf{x} = (x_1, x_2, \ldots, x_n)^{\mathrm{t}}$ tiene un número par de unos exactamente cuando $x_1 + x_2 + \cdots + x_n = 0$; luego, una 4-tupla $\mathbf{x} = (x_1, x_2, x_3, x_4)^{\mathrm{t}}$ tiene un número par de unos si y solo si $x_1 + x_2 + x_3 + x_4 = 0$, o

$$\mathbf{x} \cdot \mathbf{1} = \mathbf{x}^{\mathrm{t}}\mathbf{1} = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 0.$$

Este ejemplo nos da esperanza de que haya una conexión entre las matrices y la teoría de códigos.

Sea $\mathbb{M}_{m\times n}(\mathbb{Z}_2)$ el conjunto de todas las matrices de $m \times n$ con coeficientes en $\mathbb{Z}_2$. Hacemos operaciones entre las matrices como siempre excepto que todas nuestras operaciones de suma y producto ocurren en $\mathbb{Z}_2$. Defina el ***espacio nulo*** de una matriz $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$ como el conjunto de todas las n-tuplas binarias $\mathbf{x}$ tales que $H\mathbf{x} = \mathbf{0}$. Denotamos el espacio nulo de una matriz H por $\mathrm{Null}(H)$.

[3] Como estaremos trabajando con matrices, escribiremos las n-tuplas binarias como vectores columna por el resto del capítulo.

Ejemplo 8.20. Supongamos que

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Para que una 5-tupla $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5)^{\mathrm{t}}$ esté en el espacio nulo de H, $H\mathbf{x} = \mathbf{0}$. Equivalentemente, se debe satisfacer el siguiente sistema de ecuaciones:

$$\begin{aligned} x_2 + x_4 &= 0 \\ x_1 + x_2 + x_3 + x_4 &= 0 \\ x_3 + x_4 + x_5 &= 0. \end{aligned}$$

El conjunto de las 5-tuplas binarias que satisfacen estas ecuaciones es

$$(00000) \qquad (11110) \qquad (10101) \qquad (01011).$$

Es fácil determiar que este código es un código de grupo.

Teorema 8.21. *Sea H en $\mathbb{M}_{m\times n}(\mathbb{Z}_2)$. Entonces el espacio nulo de H es un código de grupo.*

Demostración. Como cada elemento de $\mathbb{Z}_2^n$ es su propio inverso, lo único que necesita ser verificado es la clausura. Sean $\mathbf{x}, \mathbf{y} \in \mathrm{Null}(H)$ para alguna matriz H en $\mathbb{M}_{m\times n}(\mathbb{Z}_2)$. Entonces $H\mathbf{x} = \mathbf{0}$ y $H\mathbf{y} = \mathbf{0}$. Así

$$H(\mathbf{x} + \mathbf{y}) = H\mathbf{x} + H\mathbf{y} = \mathbf{0} + \mathbf{0} = \mathbf{0}.$$

Luego, $\mathbf{x} + \mathbf{y}$ está en el espacio nulo de H y por lo tanto es una palabra del código. □

Un código es un ***código lineal*** si está determinado por el espacio nulo de alguna matriz $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$.

Ejemplo 8.22. Sea C el código dado por la matriz

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Supongamos que se recibe la 6-tupla $\mathbf{x} = (010011)^{\mathrm{t}}$. Es simplemente cuestión de multiplicar matrices para determinar si $\mathbf{x}$ está o no en el código. Como

$$H\mathbf{x} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},$$

la palabra recibida no está en el código. Debemos intentar corregirla o pedir que sea transmitida nuevamente.

8.3 Matrices Verificadora y Generadora

Debemos encontrar una forma sistemática de generar códigos lineales así como métodos rápidos de decodificación. Examinando las propiedades de la matriz H y eligiendo H cuidadosamente, es posible desarrollar métodos muy eficientes

para codificar y decodificar mensajes. Con este objetivo, introduciremos la matriz generadora estándar y la matriz verificadora canónica.

Supongamos que H es una matriz de $m \times n$ con coeficiente en $\mathbb{Z}_2$ y $n > m$. las últimas m columnas de la matriz forman la matriz identidad de $m \times m$, I_m, entonces la matriz es una ***matriz verificadora canónica***. Más específicamente, $H = (A \mid I_m)$, donde A es la matriz de $m \times (n-m)$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,n-m} \\ a_{21} & a_{22} & \cdots & a_{2,n-m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{m,n-m} \end{pmatrix}$$

y I_m es la matriz identidad de $m \times m$

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Con cada matriz verificadora canónica podemos asociar una ***matriz generadora estándar*** de $n \times (n-m)$

$$G = \begin{pmatrix} I_{n-m} \\ \hline A \end{pmatrix}.$$

Nuestro objetivo será mostrar que existe un $\mathbf{x}$ que satisfaga $G\mathbf{x} = \mathbf{y}$ si y solo si $H\mathbf{y} = \mathbf{0}$. dado un bloque $\mathbf{x}$ a ser codificado, la matriz G nos permitirá codificarlo rápidamente a una palabra $\mathbf{y}$ del código lineal.

Ejemplo 8.23. Supongamos que tenemos las siguientes ocho palabras por codificar:

$$(000), (001), (010), \ldots, (111).$$

Para

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

la matrices generadora estándar y verificadora canónica son

$$G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

y

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

respectivamente.

Observe que las filas en H representan las verificaciones de paridad en ciertas posiciones de las 6-tuplas. Los unos en la matriz identidad sirven como verificadores de paridad para los unos en la misma fila. Si $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5, x_6)$,

entonces

$$\mathbf{0} = H\mathbf{x} = \begin{pmatrix} x_2 + x_3 + x_4 \\ x_1 + x_2 + x_5 \\ x_1 + x_3 + x_6 \end{pmatrix},$$

lo que produce un sistema de ecuaciones:

$$\begin{aligned} x_2 + x_3 + x_4 &= 0 \\ x_1 + x_2 + x_5 &= 0 \\ x_1 + x_3 + x_6 &= 0. \end{aligned}$$

Acá x_4 sirve como bit de control para x_2 y x_3; x_5 es un bit de control para x_1 y x_2; y x_6 es un bit de control para x_1 y x_3. La matriz identidad impide que x_4, x_5, y x_6 tengan que controlarse entre ellos. Luego, x_1, x_2, y x_3 pueden ser arbitrarios pero x_4, x_5, y x_6 deben ser escogidos de manera de asegurar las paridades respectivas. Se calcula fácilmente que el espacio nulo de H es

$$\begin{array}{cccc} (000000) & (001101) & (010110) & (011011) \\ (100011) & (101110) & (110101) & (111000). \end{array}$$

Una forma aún más fácil de calcular el espacio nulo es con la matriz generadora G (Tabla 8.24).

Palabra de Mensaje $\mathbf{x}$	Palabra del código $G\mathbf{x}$
000	000000
001	001101
010	010110
011	011011
100	100011
101	101110
110	110101
111	111000

Cuadro 8.24: Un código generado por una matriz

Teorema 8.25. *Si $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$ es una matriz verificadora canónica, entonces* $\mathrm{Null}(H)$ *consiste de todas las $\mathbf{x} \in \mathbb{Z}_2^n$ cuyos primeros $n-m$ bits son arbitrarios pero cuyos últimos m bits están determinados por $H\mathbf{x} = \mathbf{0}$. Cada uno de los últimos m bits sirve como control de paridad para algunos de los primeros $n-m$ bits. Luego, H da lugar a un código de bloque $(n, n-m)$.*

Dejamos la demostración de este teorema como ejercicio. A la luz del teorema, los primeros $n-m$ bits de $\mathbf{x}$ se denominan ***bits de información*** y los últimos m bits se denominan ***bits de verificación***. En el Ejemplo 8.23, los primeros tres bits son de información y los últimos tres son bits de verificación.

Teorema 8.26. *Supongamos que G es una matriz generadora estándar de $n \times k$. Entonces $C = \{\mathbf{y} : G\mathbf{x} = \mathbf{y}$ para $\mathbf{x} \in \mathbb{Z}_2^k\}$ es un código de bloque (n, k). Más específicamente, C es un código de grupo.*

Demostración. Sean $G\mathbf{x}_1 = \mathbf{y}_1$ y $G\mathbf{x}_2 = \mathbf{y}_2$ dos palabras del código. Entonces $\mathbf{y}_1 + \mathbf{y}_2$ está en C pues

$$G(\mathbf{x}_1 + \mathbf{x}_2) = G\mathbf{x}_1 + G\mathbf{x}_2 = \mathbf{y}_1 + \mathbf{y}_2.$$

Debemos mostrar además que dos bloques de mensaje diferentes no pueden ser codificados a la misma palabra del código. Es decir, debemos mostrar que si $G\mathbf{x} = G\mathbf{y}$, entonces $\mathbf{x} = \mathbf{y}$. Supongamos que $G\mathbf{x} = G\mathbf{y}$. Entonces

$$G\mathbf{x} - G\mathbf{y} = G(\mathbf{x} - \mathbf{y}) = \mathbf{0}.$$

Pero las primeras k coordenadas en $G(\mathbf{x}-\mathbf{y})$ son exactamente $x_1 - y_1, \ldots, x_k - y_k$, pues están determinadas por la matriz identidad, I_k, que es parte de G. Luego, $G(\mathbf{x} - \mathbf{y}) = \mathbf{0}$ si y solo si $\mathbf{x} = \mathbf{y}$. □

Antes de demostrar la relación entre la matriz verificadora canónica y la matriz generadora estándar, demostraremos un lema.

Lema 8.27. *Sea $H = (A \mid I_m)$ una matriz verificadora canónica de $m \times n$ y $G = \begin{pmatrix} I_{n-m} \\ A \end{pmatrix}$ la correspondiente matriz generadora estándar de $n \times (n-m)$. Entonces $HG = \mathbf{0}$.*

Demostración. Sea $C = HG$. El coeficiente ijth de C es

$$\begin{aligned} c_{ij} &= \sum_{k=1}^{n} h_{ik} g_{kj} \\ &= \sum_{k=1}^{n-m} h_{ik} g_{kj} + \sum_{k=n-m+1}^{n} h_{ik} g_{kj} \\ &= \sum_{k=1}^{n-m} a_{ik} \delta_{kj} + \sum_{k=n-m+1}^{n} \delta_{i-(m-n),k} a_{kj} \\ &= a_{ij} + a_{ij} \\ &= 0, \end{aligned}$$

donde

$$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

es la delta de Kronecker. □

Teorema 8.28. *Sea $H = (A \mid I_m)$ una matriz verificadora canónica de $m \times n$ y sea $G = \begin{pmatrix} I_{n-m} \\ A \end{pmatrix}$ la correspondiente matriz generadora estándar de $n \times (n-m)$. Sea C el código generado por G. Entonces $\mathbf{y}$ está en C si y solo si $H\mathbf{y} = \mathbf{0}$. En particular, C es un código lineal con matriz verificadora canónica H.*

Demostración. Primero supongamos que $\mathbf{y} \in C$. Entonces $G\mathbf{x} = \mathbf{y}$ para algún $\mathbf{x} \in \mathbb{Z}_2^m$. Por el Lema 8.27, $H\mathbf{y} = HG\mathbf{x} = \mathbf{0}$.

Recíprocamente, supongamos que $\mathbf{y} = (y_1, \ldots, y_n)^{\mathrm{t}}$ está en el espacio nulo de H. Debemos encontrar $\mathbf{x}$ en $\mathbb{Z}_2^{n-m}$ tal que $G\mathbf{x}^{\mathrm{t}} = \mathbf{y}$. Como $H\mathbf{y} = \mathbf{0}$, se debe satisfacer el siguiente conjunto de ecuaciones:

$$\begin{aligned} a_{11}y_1 + a_{12}y_2 + \cdots + a_{1,n-m}y_{n-m} + y_{n-m+1} &= 0 \\ a_{21}y_1 + a_{22}y_2 + \cdots + a_{2,n-m}y_{n-m} + y_{n-m+1} &= 0 \\ &\vdots \\ a_{m1}y_1 + a_{m2}y_2 + \cdots + a_{m,n-m}y_{n-m} + y_{n-m+1} &= 0. \end{aligned}$$

Equivalentemente, $y_{n-m+1}, \ldots, y_n$ están determinados por $y_1, \ldots, y_{n-m}$:

$$y_{n-m+1} = a_{11}y_1 + a_{12}y_2 + \cdots + a_{1,n-m}y_{n-m}$$

$$\begin{aligned} y_{n-m+1} &= a_{21}y_1 + a_{22}y_2 + \cdots + a_{2,n-m}y_{n-m} \\ &\vdots \\ y_{n-m+1} &= a_{m1}y_1 + a_{m2}y_2 + \cdots + a_{m,n-m}y_{n-m}. \end{aligned}$$

Por ende podemos tomar $x_i = y_i$ para $i = 1, \ldots, n-m$. □

Sería bueno poder calcular la distancia mínima de un código lineal directamente a partir de su matriz H para poder determinar las capacidades de detección y corrección de errores del código. Supongamos que

$$\begin{aligned} \mathbf{e}_1 &= (100\cdots00)^{\mathrm{t}} \\ \mathbf{e}_2 &= (010\cdots00)^{\mathrm{t}} \\ &\vdots \\ \mathbf{e}_n &= (000\cdots01)^{\mathrm{t}} \end{aligned}$$

son la n-tuplas en $\mathbb{Z}_2^n$ de peso 1. Para una matriz binaria H de $m \times n$, $H\mathbf{e}_i$ es exactamente la columna i-ésima de la matriz H.

Ejemplo 8.29. Observe que

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Enunciamos el resultado en la siguiente proposición y dejamos su demostración como ejercicio.

Proposición 8.30. *Sea $\mathbf{e}_i$ la n-tupla binaria con un 1 en la i-ésima coordenada y 0 en todas las demás y supongamos que $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$. Entonces $H\mathbf{e}_i$ es la i-ésima columna de la matriz H.*

Teorema 8.31. *Sea H una matriz binaria de $m \times n$. Entonces el espacio nulo de H es un código que puede detectar un error si y solo si ninguna columna de H consiste solamente de ceros.*

Demostración. Supongamos que $\mathrm{Null}(H)$ es un código que detecta un error. Entonces la distancia mínima del código debe ser al menos 2. Como el espacio nulo es un código de grupo, es necesario que el código no tenga ninguna palabra de peso menor a 2 aparte de la palabra cero. Es decir, $\mathbf{e}_i$ no debe ser una palabra del código para $i = 1, \ldots, n$. Como $H\mathbf{e}_i$ es la i-ésima columna de H, la i-ésima columna no tiene puros ceros.

Recíprocamente, supongamos que ninguna columna de H es la columna cero. Por la Proposición 8.30, $H\mathbf{e}_i \neq \mathbf{0}$; luego, la distancia mínima del código es al menos 2, y el código tiene la capacidad de detectar un error.. □

Ejemplo 8.32. Si consideramos las matrices

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

y

$$H_2 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

entonces el espacio nulos de H_1 es un código que detecta un error y el espacio nulo de H_2 no lo es.

Podemos mejorar el Teorema 8.31. Este teorema nos entrega condiciones sobre la matriz H que nos dicen cuándo el peso mínimo del código formado por el espacio nulo de H es 2. También podemos determinar cuándo la distancia mínima de un código lineal es 3 examinando la matriz correspondiente.

Ejemplo 8.33. Si hacemos

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

y queremos determinar si H es la matriz verificadora canónica para un código corrector de un error, es necesario asegurarse que $\text{Null}(H)$ no contenga ninguna 4-tupla de peso 2. Es decir, (1100), (1010), (1001), (0110), (0101), y (0011) no deben estar en $\text{Null}(H)$. El próximo teorema establece que podemos saber si el código determinado por H es corrector de errores examinando las columnas de H. Note en este ejemplo que no solo H no tiene columnas nulas, sino que tampoco tiene columnas repetidas.

Teorema 8.34. *Sea H una matriz binaria. El espacio nulo de H es un código corrector de un error si H no contiene columnas de puros ceros ni dos columnas iguales.*

Demostración. La n-tupla $\mathbf{e}_i + \mathbf{e}_j$ tiene unos en la posiciones i-ésima y j-ésima y ceros en las demás, y $w(\mathbf{e}_i + \mathbf{e}_j) = 2$ para $i \neq j$. Como

$$\mathbf{0} = H(\mathbf{e}_i + \mathbf{e}_j) = H\mathbf{e}_i + H\mathbf{e}_j$$

Solo puede ocurrir si la i-ésima y la j-ésima columnas son idénticas. Como no contiene palabras de peso menor o igual a 2, el espacio nulo de H es un código corrector de un error. □

Supongamos ahora que tenemos una matriz verificadora canónica H con tres filas. Nos podemos preguntar cuántas columnas le podemos agregar a la matriz y seguir teniendo un espacio nulo que sea un código que detecte y corrija un error. Como cada columna tiene tres entradas, hay $2^3 = 8$ columnas diferentes posibles. No podemos agregar las columnas

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Podemos entonces agregar hasta cuatro columnas manteniendo una distancia mínima de 3.

En general, si H es una matriz verificadora canónica de $m \times n$, entonces hay $n - m$ posiciones de información en cada palabra del código. Cada columna tiene m bits, así es que hay 2^m posibles columnas diferentes. Es necesario que las columnas $\mathbf{0}, \mathbf{e}_1, \ldots, \mathbf{e}_m$ sean excluidas, dejando $2^m - (1 + m)$ columnas restantes para información si queremos mantener la habilidad de no solo detectar sino también corregir un error.

8.4 Decodificación Eficiente

Estamos ahora en el punto donde somos capaces de generar códigos lineales que detecten y corrijan errores con relativa facilidad, pero aún es un proceso lento el de decodificar una n-tupla recibida y determinar cuál es la palabra del código más cercana, pues la n-tupla recibida debe ser comparada con todas las posibles palabras del código para determinar la decodificación apropiada. Este puede ser un impedimento serio si el código es muy grande.

Ejemplo 8.35. Dada la matriz binaria

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

y las 5-tuplas $\mathbf{x} = (11011)^{\mathrm{t}}$ and $\mathbf{y} = (01011)^{\mathrm{t}}$, podemos calcular

$$H\mathbf{x} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \qquad \text{and} \qquad H\mathbf{y} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Luego, $\mathbf{x}$ es una palabra del código e $\mathbf{y}$ no lo es, pues $\mathbf{x}$ está en el espacio nulo e $\mathbf{y}$ no lo está. Notemos que $H\mathbf{y}$ es idéntica a la primera columna de H. De hecho, es ahí donde ocurrió el error. Si cambiamos el primer bit en $\mathbf{y}$ de 0 a 1, obtenemos $\mathbf{x}$.

Si H es una matriz de $m \times n$ y $\mathbf{x} \in \mathbb{Z}_2^n$, entonces decimos que el ***síndrome*** de $\mathbf{x}$ es $H\mathbf{x}$. La siguiente proposición permite la detección y corrección rápida de errores.

Proposición 8.36. *Sea H una matriz de $m \times n$ que determina un código lineal y sea $\mathbf{x}$ la n-tupla recibida. Escribamos $\mathbf{x}$ como $\mathbf{x} = \mathbf{c} + \mathbf{e}$, donde $\mathbf{c}$ es la palabra transmitida y $\mathbf{e}$ es el error de transmisión. Entonces el síndrome $H\mathbf{x}$ de la palabra recibida $\mathbf{x}$ es igual al síndrome del error $\mathbf{e}$.*

Demostración. La demostración sigue del hecho que

$$H\mathbf{x} = H(\mathbf{c} + \mathbf{e}) = H\mathbf{c} + H\mathbf{e} = \mathbf{0} + H\mathbf{e} = H\mathbf{e}. \qquad \square$$

Esta proposición nos dice que el síndrome de una palabra recibida depende solamente del error y no de la palabra trasmitida. La demostración del siguiente teorema sigue inmediatamente de la Proposición 8.36 y del hecho que $H\mathbf{e}$ es la i-ésima columna de la matriz H.

Teorema 8.37. *Sea $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$ y supongamos que el código lineal correspondiente a H es corrector de un error. Sea $\mathbf{r}$ una n-tupla recibida que fue trasmitida con a lo más un error. Si el síndrome de $\mathbf{r}$ es $\mathbf{0}$, entonces no ha ocurrido ningún error; de lo contrario, si el síndrome de $\mathbf{r}$ es igual a alguna columna de H, digamos la i-ésima columna, entonces el error ocurrió en el i-ésimo bit.*

Ejemplo 8.38. Consideremos la matriz

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

y supongamos que las 6-tuples $\mathbf{x} = (111110)^t$, $\mathbf{y} = (111111)^t$, y $\mathbf{z} = (010111)^t$ fueron recibidas. Entonces

$$H\mathbf{x} = \begin{pmatrix}1\\1\\1\end{pmatrix}, H\mathbf{y} = \begin{pmatrix}1\\1\\0\end{pmatrix}, H\mathbf{z} = \begin{pmatrix}1\\0\\0\end{pmatrix}.$$

Luego, $\mathbf{x}$ tiene un error en el tercer bit y $\mathbf{z}$ tiene un error en el cuarto bit. Las palabras trasmitidas para $\mathbf{x}$ y $\mathbf{z}$ deben haber sido (110110) y (010011), respectivamente. El síndrome de $\mathbf{y}$ no aparece en ninguna de las columnas de H, de manera que más de un error debe haber ocurrido para producir $\mathbf{y}$.

Decodificación por Clases Laterales

Podemos usar teoría de grupos para obtener otro método de decodificación. Un código lineal C es un subgrupo de $\mathbb{Z}_2^n$. Decodificación ***por Clases Laterales*** o ***decodificación estándar*** usa las clases laterales de C en $\mathbb{Z}_2^n$ para implementar la decodificación de probabilidad máxima. Supongamos que C un código lineal (n, m). Una clase lateral de C en $\mathbb{Z}_2^n$ se escribe en la forma $\mathbf{x}+C$, donde $\mathbf{x} \in \mathbb{Z}_2^n$. Por el Teorema de Lagrange (Teorema 6.10), hay 2^{n-m} clases laterales de C en $\mathbb{Z}_2^n$.

Ejemplo 8.39. Sea C el código lineal $(5, 3)$ dado por la matriz verificadora

$$H = \begin{pmatrix}0&1&1&0&0\\1&0&0&1&0\\1&1&0&0&1\end{pmatrix}.$$

El código consiste de las palabras

$$(00000) \quad (01101) \quad (10011) \quad (11110).$$

Hay $2^{5-2} = 2^3$ clases laterales de C en $\mathbb{Z}_2^5$, cada una de orden $2^2 = 4$. Estas clases laterales aparecen en la Tabla 8.40.

Representante de la clase	Clase lateral
C	(00000) (01101) (10011) (11110)
$(10000) + C$	(10000) (11101) (00011) (01110)
$(01000) + C$	(01000) (00101) (11011) (10110)
$(00100) + C$	(00100) (01001) (10111) (11010)
$(00010) + C$	(00010) (01111) (10001) (11100)
$(00001) + C$	(00001) (01100) (10010) (11111)
$(10100) + C$	(00111) (01010) (10100) (11001)
$(00110) + C$	(00110) (01011) (10101) (11000)

Cuadro 8.40: Clases laterales de C

Nuestra tarea es descubrir cómo conocer las clases laterales nos puede ayudar a decodificar un mensaje. Supongamos que $\mathbf{x}$ era la palabra trasmitida y que $\mathbf{r}$ es la n-tupla recibida. Si $\mathbf{e}$ es el error de trasmisión, entonces $\mathbf{r} = \mathbf{e} + \mathbf{x}$ o, equivalentemente, $\mathbf{x} = \mathbf{e} + \mathbf{r}$. Pero, esto es exactamente equivalente a decir que $\mathbf{r}$ es un elemento de la clase $\mathbf{e}+C$. En la decodificación de máxima probabilidad esperamos que $\mathbf{e}$ sea lo más pequeño que se pueda; es decir, $\mathbf{e}$ tendrá el

menor peso. Una n-tupla de peso mínimo en una clase se denomina ***líder de clase***. Una vez que hemos determinado un líder para cada clase, el proceso de decodificación se transforma en el de calcular $\mathbf{r} + \mathbf{e}$ para obtener $\mathbf{x}$.

Ejemplo 8.41. En la Tabla 8.40, note que hemos elegido un representante de peso mínimo para cada clase. Estos representantes son líderes de clase. Ahora supongamos que recibimos la palabra $\mathbf{r} = (01111)$. Para decodificar $\mathbf{r}$, lo encontramos en la clase $(00010) + C$; luego, la palabra del código originalmente trasmitida debe haber sido $(01101) = (01111) + (00010)$.

Un problema potencial con este método de decodificación es que tengamos que examinar cada clase en busca de la palabra recibida. La siguiente proposición entrega un método para la implementación de la decodificación por clases laterales. Establece que podemos asociar un síndrome con cada clase; luego, podemos hacer una tabla que asigna un líder de clase a cada síndrome. Tal lista se denomina ***tabla de decodificación***.

Síndromes	Líder de clase
(000)	(00000)
(001)	(00001)
(010)	(00010)
(011)	(10000)
(100)	(00100)
(101)	(01000)
(110)	(00110)
(111)	(10100)

Cuadro 8.42: Síndromes para cada clase

Proposición 8.43. *Sea C un código lineal (n, k) dado por la matriz H y supongamos que $\mathbf{x}$ e $\mathbf{y}$ están en $\mathbb{Z}_2^n$. Entonces $\mathbf{x}$ e $\mathbf{y}$ están en la misma clase lateral de C si y solo si $H\mathbf{x} = H\mathbf{y}$. Es decir, dos n-tuplas están en la misma clase lateral si y solo si tienen el mismo síndrome.*

Demostración. Dos n-tuplas $\mathbf{x}$ e $\mathbf{y}$ están en la misma clase lateral de C precisamente cuando $\mathbf{x} - \mathbf{y} \in C$; pero, esto es equivalente a que $H(\mathbf{x} - \mathbf{y}) = 0$ o $H\mathbf{x} = H\mathbf{y}$. □

Ejemplo 8.44. La Tabla 8.42 es una tabla de decodificación para el código C dado en el Ejemplo 8.39. Si se recibe $\mathbf{x} = (01111)$, entonces su síndrome se calcula como

$$H\mathbf{x} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

Examinando la tabla de decodificación, determinamos que el líder de clase es (00010). Es fácil ahora decodificar la palabra recibida.

Dado un código de bloque (n, k), surge la pregunta sobre si la decodificación por clases laterales es un sistema manejable o no. Una tabla de decodificación requiere una lista de líderes de clases laterales y síndromes uno para cada una de las 2^{n-k} clases laterales de C. Supongamos que tenemos un código de bloque $(32, 24)$. Tenemos una enorme cantidad de palabras en el código, 2^{24}, pero hay solamente $2^{32-24} = 2^8 = 256$ clases laterales.

Sage Sage tiene bastantes comandos para teoría de códigos, incluyendo la capacidad de construir diferentes familias de códigos.

8.5 Ejercicios

1. ¿Por qué no es aceptable el siguiente sistema de codificación?

Información	0	1	2	3	4	5	6	7	8
Palabra del Código	000	001	010	011	101	110	111	000	001

2. Sin realizar ninguna suma, explique por qué el siguiente conjunto de 4-tuplas en $\mathbb{Z}_2^4$ no puede ser un código de grupo.

$$(0110) \quad (1001) \quad (1010) \quad (1100)$$

3. Calcule las distancias de Hamming entre las siguientes pares de n-tuplas.

(a) $(011010), (011100)$

(b) $(11110101), (01010100)$

(c) $(00110), (01111)$

(d) $(1001), (0111)$

4. Calcule los pesos de las siguientes n-tuplas.

(a) (011010)

(b) (11110101)

(c) (01111)

(d) (1011)

5. Si un código lineal C tiene peso mínimo 7, ¿cuáles son las capacidades de detección y corrección de errores de C?

6. Para cada uno de los siguientes códigos, ¿cuál es la distancias mínima del código? ¿Cuál es la mejor situación que podemos esperar en relación a detección y corrección de errores?

(a) (011010) (011100) (110111) (110000)

(b) (011100) (011011) (111011) (100011) (000000) (010101) (110100) (110011)

(c) (000000) (011100) (110101) (110001)

(d) (0110110) (0111100) (1110000) (1111111) (1001001) (1000011) (0001111) (0000000)

7. Calcule el espacio nulo de cada una de las siguientes matrices. ¿Qué tipo de códigos de bloque (n, k) son los espacios nulos? ¿Puede encontrar una matriz (no necesariamente una matriz generadora estándar) que genere cada código? ¿Son únicas sus matrices generadoras?

(a)
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(c)
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(d)
$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

8. Construya un código de bloque $(5, 2)$. Discuta las capacidades de detección y corrección de errores de su código.

9. Sea C el código obtenido como espacio nulo de la matriz

$$H = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Decodifique el mensaje

$$01111 \quad 10101 \quad 01110 \quad 00011$$

si es posible.

10. Supongamos que se transmite un mensaje binario de 1000 bits, que la probabilidad de error en un bit es p y que los errores que puedan ocurrir en bits diferentes son independientes entre ellos. Si $p = 0.01$, ¿Cuál es la probabilidad de que ocurra más de un error? ¿Cuál es la probabilidad de que ocurran exactamente dos errores? Repita el problema para $p = 0.0001$.

11. ¿Qué matrices son matrices verificadoras canónicas? Para aquella matrices que sean matrices verificadoras canónicas, ¿cuáles son las correspondientes matrices generadoras estándar? ¿Cuáles son las capacidades de detección y corrección de errores de cada una de estas matrices?

(a)
$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(c)
$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

(d)
$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

12. Liste todos los posible síndromes para los códigos generados por cada una de las matrices del Ejercicio 8.5.11.

13. Sea

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Calcule el síndrome causado por cada uno de los siguientes errores de transmisión.

(a) Un error en el primer bit.

(b) Un error en el tercer bit.

(c) Un error en el último bit.

(d) Errores en el tercer y cuarto bits.

14. Sea C el código de grupo en $\mathbb{Z}_2^3$ definido por las palabras (000) and (111). Calcule las clases laterales de H en $\mathbb{Z}_2^3$. ¿Por qué no es necesario especificar si se trata de clases laterales derechas o izquierdas? Entregue el error singular de transmisión, si lo hay, que corresponda con cada clase lateral.

15. Para cada una de las siguientes matrices, encuentre las clases laterales para el código C correspondiente. Entregue una tabla de decodificación para cada código si es posible.

(a)
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(c)
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(d)
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

16. Sean $\mathbf{x}$, $\mathbf{y}$, y $\mathbf{z}$ n-tuplas binarias. Demuestre cada uno de los siguientes enunciados.

(a) $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$

(b) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x} + \mathbf{z}, \mathbf{y} + \mathbf{z})$

(c) $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$

17. Una ***métrica*** en un conjunto X es una función $d : X \times X \to \mathbb{R}$ que satisface las siguientes condiciones.

(a) $d(\mathbf{x}, \mathbf{y}) \geq 0$ para todo $\mathbf{x}, \mathbf{y} \in X$;

(b) $d(\mathbf{x}, \mathbf{y}) = 0$ si y solo si $\mathbf{x} = \mathbf{y}$;

(c) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$;

(d) $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$.

En otros palabras, una métrica es simplemente una generalización de la noción de distancia. Demuestre que la distancia de Hamming es una métrica en $\mathbb{Z}_2^n$. Decodificar un mensaje en realidad corresponde a decidir cuál es la palabra del código más cercana en términos de la distancia de Hamming.

18. Sea C un código lineal binario. Muestre que entre las i-ésimas coordenadas de la palabras en C hay puros ceros o exactamente la mitad son ceros.

19. Sea C un código lineal binario. Muestre que ya sea todas las palabras tienen peso par o exactamente la mitad de ellas tienen peso par.

20. Muestre que las palabras de peso par en un código lineal binario C también forman un código lineal.

21. Si hemos de usar un código lineal corrector de errores para transmitir los 128 caracteres ASCII, ¿qué tamaño de matriz debe usarse? ¿Qué tamaño de matriz debe usarse para transmitir el conjunto ASCII extendido de 256 caracteres? ¿Y si solo requerimos detección de errores en ambos casos?

22. Encuentre la matriz verificadora canónica que da el código de verificación de paridad con tres posiciones de información. ¿Cuál es la matriz para siete posiciones de información? ¿Cuáles son las matrices generadoras estándar correspondientes?

23. ¿Cuántas posiciones de verificación se necesitan para un código de corrección de un error con 20 posiciones de información? ¿Con 32 posiciones de información?

24. Sea $\mathbf{e}_i$ la n-tupla binaria con un 1 en la i-ésima coordenada y 0 en las demás y supongamos que $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$. Muestre que $H\mathbf{e}_i$ es la i-ésima columna de la matriz H.

25. Sea C un código lineal (n, k). Definamos el ***código dual*** o ***código ortogonal*** de C como

$$C^{\perp} = \{\mathbf{x} \in \mathbb{Z}_2^n : \mathbf{x} \cdot \mathbf{y} = 0 \text{ para todo } \mathbf{y} \in C\}.$$

(a) Encuentre el código dual del código lineal C donde C está dado por la matriz

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

(b) Muestre que $C^{\perp}$ es un código lineal $(n, n-k)$.

(c) Encuentre las matrices verificadora canónica y generadora estándar de C y $C^{\perp}$. ¿Qué sucede en general? Demuestre su conjetura.

26. Sea H una matriz de $m \times n$ sobre $\mathbb{Z}_2$, donde la i-ésima columna es el número i escrito en binario con m bits. El espacio nulo de una tal matriz se llama ***código de Hamming***.

(a) Muestre que la matriz

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

genera un código de Hamming. ¿Cuáles son las propiedades de corrección de errores de un código de Hamming?

(b) La columna correspondiente al síndrome también marca el bit donde ocurrió el error; es decir, la i-ésima columna de la matriz es i escrito como número binario, y el síndrome inmediatamente nos dice cuál es el bit erróneo. Si la palabra recibida es (101011), Calcule el síndrome. ¿En qué bit ocurrió el error en este caso, y cuál era la palabra originalmente transmitida?

(c) Entregue un matriz binaria H para el código de Hamming con seis posiciones de informacióny cuatro de verificación. ¿Cuáles son la posiciones de verificación y cuáles son las de información? Codifique los mensajes (101101) y (001001). Decodifique las palabras recibidas (0010000101) y (0000101100). ¿Cuáles son los posibles síndromes para este código?

(d) ¿Cuál es el número de bits de verificación y el número de bits de información en un código de Hamming de bloque (m, n)? Encuentre tanto una cota superior como una cota inferior para el número de bits de información en términos del número de bits de verificación. Códigos de Hamming que tengan el máximo posible número de bits de información con k bits de verificación se llaman ***perfectos***. Cada posible síndrome a excepción de $\mathbf{0}$ ocurre como una columna. Si el número de bits de información es menor al máximo, entonces el código se llama ***recortado***. En este caso, dé un ejemplo donde algunos síndromes puedan representar errores múltiples.

8.6 Ejercicios de Programación

1. Escriba un programa para implementar un código lineal $(16, 12)$. Su programa debe ser capaz de codificar y decodificar mensajes usando decodificación por clases laterales. Una vez que haya escrito su programa, escriba un programa para simular un canal binario simétrico con ruido de trasmisión. Compare los resultados de su simulación con la probabilidad de error predicha.

8.7 Referencias y Lecturas Recomendadas

[1] Blake, I. F. "Codes and Designs," *Mathematics Magazine* **52**(1979), 81–95.

[2] Hill, R. *A First Course in Coding Theory.* Oxford University Press, Oxford, 1990.

[3] Levinson, N. "Coding Theory: A Counterexample to G. H. Hardy's Conception of Applied Mathematics," *American Mathematical Monthly* **77**(1970), 249–58.

[4] Lidl, R. and Pilz, G. *Applied Abstract Algebra.* 2nd ed. Springer, New York, 1998.

[5] MacWilliams, F. J. and Sloane, N. J. A. *The Theory of Error-Correcting Codes.* North-Holland Mathematical Library, 16, Elsevier, Amsterdam, 1983.

[6] Roman, S. *Coding and Information Theory.* Springer-Verlag, New York, 1992.

[7] Shannon, C. E. "A Mathematical Theory of Communication," *Bell System Technical Journal* **27**(1948), 379–423, 623–56.

[8] Thompson, T. M. *From Error-Correcting Codes through Sphere Packing to Simple Groups.* Carus Monograph Series, No. 21. Mathematical Association of America, Washington, DC, 1983.

[9] van Lint, J. H. *Introduction to Coding Theory.* Springer, New York, 1999.

8.8 Sage

Sage contiene una colección importante de códigos lineales y una variedad de métodos que pueden ser usados para investigarlos.

Construyendo Códigos Lineales

El objeto `codes` puede ser usado para obtener una lista concisa de los códigos implementados disponibles. Escriba `codes.` y presione `Tab`. La mayor parte de las interfaces a Sage le entregarán una lista. Puede usar el signo de interrogación al final del nombre de un método para aprender más sobre los distintos parámetros.

```
codes.
```

Usaremos el código binario de Hamming $(7, 4)$ clásico como ilustración. "Binario" quiere decir que tenemos vectores con solo ceros y unos, 7 es el largo y significa que los vectores tienen 7 coordenadas, y 4 es la dimensión, lo que significa que este código contiene $2^4 = 16$ vectores. La documentación supone que sabemos unas pocas cosas de más adelante en el texto. Usamos `GF(2)` para especificar que el código es binario — esto tendrá más sentido después de haber

estudiado cuerpos finitos. Un segundo parámetro es `r` y podemos ver de las fórmulas en la documentación que poniendo `r=3` nos dará largo 7.

```
H = codes.HammingCode(GF(2), 3); H
```

```
[7, 4] Hamming Code over GF(2)
```

Propiedades de los Códigos Lineales

Podemos ahora examinar el código que acabamos de construir. Primero su dimensión.

```
H.dimension()
```

```
4
```

El código es suficientemente pequeño como para listar todas sus palabras.

```
H.list()
```

```
[(0, 0, 0, 0, 0, 0, 0), (1, 0, 0, 0, 0, 1, 1), (0, 1, 0, 0,
    1, 0, 1),
 (1, 1, 0, 0, 1, 1, 0), (0, 0, 1, 0, 1, 1, 0), (1, 0, 1, 0,
     1, 0, 1),
 (0, 1, 1, 0, 0, 1, 1), (1, 1, 1, 0, 0, 0, 0), (0, 0, 0, 1,
     1, 1, 1),
 (1, 0, 0, 1, 1, 0, 0), (0, 1, 0, 1, 0, 1, 0), (1, 1, 0, 1,
     0, 0, 1),
 (0, 0, 1, 1, 0, 0, 1), (1, 0, 1, 1, 0, 1, 0), (0, 1, 1, 1,
     1, 0, 0),
 (1, 1, 1, 1, 1, 1, 1)]
```

La distancia mínima es posiblemente una de sus propiedades más importantes. Los códigos de Hamming siempre tienen distancia mínima $d = 3$, de manera que siempre son correctores de un error.

```
H.minimum_distance()
```

```
3
```

Sabemos que la matriz verificadora y la matriz generadora son útiles para la construcción, descripción y análisis de los códigos lineales. Los nombres de los métodos en Sage son un poco crípticos. Sage tienen rutinas para analizar matrices con elementos de diferentes cuerpos, de manera que haremos buena parte del análisis de estas matrices dentro de Sage.

```
C = H.parity_check_matrix(); C
```

```
[1 0 1 0 1 0 1]
[0 1 1 0 0 1 1]
[0 0 0 1 1 1 1]
```

La matriz generadora del texto tienen *columnas* que son palabras del código, y combinaciones lineales de las columnas (el espacio de columnas de la matriz) son palabras del código. En Sage la matriz generadora tiene *filas* que son palabras del código y el espacio de filas de la matriz es el código. Tenemos acá otro punto en que debemos traducir mentalmente entre una elección hecha en el texto y un elección hecha por los desarrolladores de Sage.

```
G = H.generator_matrix(); G
```

```
[1 0 0 0 0 1 1]
[0 1 0 0 1 0 1]
[0 0 1 0 1 1 0]
[0 0 0 1 1 1 1]
```

A continuación una verificación parcial de que estas dos matrices son correctas, ejercitando el Lema 8.27. Note que necesitamos transponer la matriz generadora por las razones expuestas antes.

```
C*G.transpose() == zero_matrix(3, 4)
```

```
True
```

Notemos que la matriz verificadora puede no ser canónica y que la matriz generadora puede no ser estándar. Sage puede producir una matriz generadora que tenga un conjunto de columnas que formen la matriz identidad, pero no se garantiza que estas columnas sean las primeras. (Columnas, no filas.) Tal matriz se dice ***sistemática***, y el método Sage es `.systematic_generator_matrix()`.

```
H.systematic_generator_matrix()
```

```
[1 0 0 0 0 1 1]
[0 1 0 0 1 0 1]
[0 0 1 0 1 1 0]
[0 0 0 1 1 1 1]
```

Decodificando un Código Lineal

Podemos decodificar mensajes recibidos originados por un código lineal. Supongamos que recibimos el vector binario de largo 7`r`.

```
r = vector(GF(2), [1, 1, 1, 1, 0, 0, 1]); r
```

```
(1, 1, 1, 1, 0, 0, 1)
```

Podemos reconocer que uno o más errores han ocurrido, pues `r` no pertenece al código, dado que el siguiente cálculo no resulta en el vector cero.

```
C*r
```

```
(1, 1, 0)
```

Un código lineal tiene un método `.decode`. Usted puede elegir entre distintos algoritmos, pero los códigos de Hamming tienen su algoritmo particular. El algoritmo por defecto es el del uso de síndromes.

```
H.decode_to_code(r)
```

```
(1, 1, 0, 1, 0, 0, 1)
```

Si estamos dispuesto a suponer que solo ha ocurrido un eror (lo que podemos, si la probabilidad de error en una entrada particular del vector es muy baja), entonces vemos que ocurrió un error en la tercera posición.

Recuerde que podría ser que ocurra más de un error. Por ejemplo, supongamos que el mensaje es el mismo de antes y ocurren errores en la tercera, quinta y sexta posiciones.

```
message = vector(GF(2), [1, 1, 0, 1, 0, 0, 1])
errors = vector(GF(2), [0, 0, 1, 0, 1, 1, 0])
received = message + errors
received
```

```
(1, 1, 1, 1, 1, 1, 1)
```

Entonces parece querecibimos una palabra del código, por lo que suponemos que no hubo errores en absoluto, y decodificamos incorrectamente.

```
H.decode_to_code(received) == message
```

```
False
```

```
H.decode_to_code(received) == received
```

```
True
```

8.9 Ejercicios en Sage

1. Construya el código (binario) Golay con el constructor `codes.GolayCode()`. Lea la documentación para asegurarse de construir la versión binaria (y no la ternaria), y no construya la versión extendida (que es el default).

(a) Use métodos Sage para calcular el largo, la dimensión y la distancia mínima del código.

(b) ¿Cuántos errores puede detectar este código? ¿Cuántos puede corregir?

(c) Encuentre una palabra distinta de cero en el código e introduzca tres errores sumando un vector con tres 1's (de su elección) para crear un mensaje recibido. Muestre que el mensaje se decodifica correctamente.

(d) Recicle sus elecciones de la parte anterior, pero ahora agregue un error adicional. ¿Se decodifica correctamente el mensaje recibido?

2. Una técnica que permita mejorar las características de un código es agregar un bit de paridad general, tal como el bit de paridad del código ASCII descrito en el Ejemplo 8.3. Tales códigos se conocen como versiones ***extendidas*** del código original.

(a) Construya el código de Golay binario y obtenga la matriz evrificadora. Use comandos Sage para extender esta matriz creando una nueva matriz de paridad que considere un bit de paridad global adicional. los métodos `.augment()` y `.stack()` para matrices le pueden resultar útiles, así como los constructores `zero_vector()` y `ones_matrix()` (recordando que especificamos las entradas binarias como pertenecientes al cuerpo `GF(2)`.)

Cree el código extendido entregando la matriz de paridad aumentada al constructor `codes.from_parity_check_matrix()` y calcule la longitud, dimension y distancia mínima del código extendido.

(b) ¿En qué sentido son mejores las características de este nuevo código? ¿A qué costo?

(c) Ahora cree el código de Golay binario extendido con `codes.GolayCode()` y la opción apropiada para obtener la versión extendida. Con algo de suerte, las listas ordenadas de sus palabras y las del código implementado en Sage, serán las mismas. Si no, el método `.is_permutation_equivalent()` debiera retornar `True` indicando que su código y el de Sage son simplemente reordenamientos, el uno del otro.

3. El dual de un código de bloque (n, k) está formado por el conjunto de los vectores bianrios ortogonales a todos los vectores del código original. El Ejercicio 8.5.25 describe esta construcción y pregunta por algunas de sus propiedades. Se puede obtener el dual de un código en Sage con el método `.dual_code()`. Construya los códigos de Hamming binarios, y sus duales, con el parámetro `r` variando desde `2` hasta `5`. Construya una tabla con seis columnas (posiblemente usando la función `html.table()`) que liste r, el largo del código, la dimensión del código original, la de su dual, la distancia mínima del código y la de su dual.
Conjeture fórmulas para la dimensión y distancia mínima del dual de un código de Hamming en términos del parámetro r.

4. Un código con distancia mínima d se llama ***perfecto*** si todo vector posible está a distancia menor o igual a $(d-1)/2$ de alguna palabra del código. Si expandimos nuestra idea de geometría para incluir la noción de distancia de Hamming como la métrica, entonces podemos hablar de una esfera de radio r en torno a un vector o palabra. Para un código de longitud n, una esfera de este tipo contiene

$$1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}$$

vectores en su interior. Para un código perfecto, las esferas de radio $(d-1)/2$ centradas en las palabras del código particionan exactamente el espacio de todos los vectores posibles. (Esto es lo que establece una relación entre la teoría de códigos y los problemas de empaquetamiento de esferas.)
Una consecuencia de que un código de dimensión k sea perfecto es que

$$2^k \left(\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{\frac{d-1}{2}} \right) = 2^n$$

Recíprocamente, si un código tiene distancia mínima d y cumple la condición anterior, entonces el código es perfecto.
Escriba una función en Sage, llamada `is_perfect()` que tome un código lineal como entrada y retorne `True` o `False` según si el código es o no perfecto. Demuestre su función verificando que el código de Golay binario es perfecto, y use un bucle para verificar que los códigos de Hamming binarios son perfectos para longitudes menores a 32.

9

Isomorfismos

Muchos grupos pueden parecer diferentes a primera vista, pero pueden reconocerse como iguales después de un cambio de nombre de sus elementos. Por ejemplo, $\mathbb{Z}_4$ y el subgrupo del grupo de la circunferencia $\mathbb{T}$ generado por i pueden ser reconocidos como el mismo grupo demostrando que existe una correspondencia entre sus elementos y entre las operaciones de grupo de ambos. En tal caso diremos que los grupos son isomorfos.

9.1 Definición y Ejemplos

Dos grupos $(G, \cdot)$ y $(H, \circ)$ son ***isomorfos*** si existe una función biyectiva $\phi : G \to H$ que preserve la operación de grupo; es decir,

$$\phi(a \cdot b) = \phi(a) \circ \phi(b)$$

para todo a y b en G. Si G es isomorfo con H, escribimos $G \cong H$. La función ϕ se llama un ***isomorfismo***.

Ejemplo 9.1. Para demostrar que $\mathbb{Z}_4 \cong \langle i \rangle$, defina una función $\phi : \mathbb{Z}_4 \to \langle i \rangle$ como $\phi(n) = i^n$. Debemos mostrar que ϕ es biyectiva y que preserva la operación de grupo. La función ϕ es biyectiva pues

$$\begin{aligned} \phi(0) &= 1 \\ \phi(1) &= i \\ \phi(2) &= -1 \\ \phi(3) &= -i. \end{aligned}$$

Como

$$\phi(m+n) = i^{m+n} = i^m i^n = \phi(m)\phi(n),$$

se preserva la operación de grupo.

Ejemplo 9.2. Podemos definir un isomorfismo ϕ del grupo aditivo de los números reales $(\mathbb{R}, +)$ al grupo multiplicativo de los números reales positivos $(\mathbb{R}^+, \cdot)$ mediante la función exponencial; es decir,

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y).$$

Por supuesto, debemos aún demostrar que ϕ es una biyección; esto puede ser hecho usando cálculo diferencial.

Ejemplo 9.3. Los enteros son isomorfos al subgrupo de $\mathbb{Q}^*$ que consiste de los elementos de la forma 2^n. Defina una función $\phi : \mathbb{Z} \to \mathbb{Q}^*$ como $\phi(n) = 2^n$. Entonces

$$\phi(m+n) = 2^{m+n} = 2^m 2^n = \phi(m)\phi(n).$$

Por definición la función ϕ es sobreyectiva en el subconjunto $\{2^n : n \in \mathbb{Z}\}$ de $\mathbb{Q}^*$. Para mostrar que la función es inyectiva, supongamos que $\phi(m) = \phi(n)$. Entonces $2^m = 2^n$ y $2^{m-n} = 1$. Concluimos que $m = n$.

Ejemplo 9.4. Los grupos $\mathbb{Z}_8$ y $\mathbb{Z}_{12}$ no pueden ser isomorfos pues tienen diferentes órdenes; Sin embargo $U(8) \cong U(12)$. Sabemos que

$$U(8) = \{1, 3, 5, 7\}$$
$$U(12) = \{1, 5, 7, 11\}.$$

Un isomorfismo $\phi : U(8) \to U(12)$ está dado por

$$1 \mapsto 1$$
$$3 \mapsto 5$$
$$5 \mapsto 7$$
$$7 \mapsto 11.$$

La función ϕ no es el único isomorfismo posible entre estos dos grupos. Podríamos definir otro isomorfismo ψ como $\psi(1) = 1$, $\psi(3) = 11$, $\psi(5) = 5$, $\psi(7) = 7$. De hecho, estos dos grupos son isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_2$ (Vea el Ejemplo 3.28 en el Capítulo 3).

Ejemplo 9.5. Si bien S_3 y $\mathbb{Z}_6$ poseen el mismo número de elementos, podríamos sospechar que no son isomorfos, pues $\mathbb{Z}_6$ es abeliano y S_3 es no abeliano. Para demostrar que esto es así, supongamos que $\phi : \mathbb{Z}_6 \to S_3$ es un isomorfismo. Sean $a, b \in S_3$ dos elementos tales que $ab \neq ba$. Como ϕ es un isomorfismo, existen elementos m y n en $\mathbb{Z}_6$ tales que

$$\phi(m) = a \quad \text{and} \quad \phi(n) = b.$$

Pero,

$$ab = \phi(m)\phi(n) = \phi(m+n) = \phi(n+m) = \phi(n)\phi(m) = ba,$$

lo que contradice el hecho de que a y b no conmutan.

Teorema 9.6. *Sea $\phi : G \to H$ un isomorfismo de grupos. Entonces se cumplen las siguientes proposiciones.*

1. *$\phi^{-1} : H \to G$ es un isomorfismo.*
2. *$|G| = |H|$.*
3. *Si G es abeliano, entonces H es abeliano.*
4. *Si G es cíclico, entonces H es cíclico.*
5. *Si G tiene un subgrupo de orden n, entonces H tiene un subgrupo de orden n.*

Demostración. Las afirmaciones (1) y (2) son consecuencia de que ϕ sea una biyección. Demostraremos (3) y dejaremos el resto del teorema para ser demostrado en los ejercicios.

(3) Supongamos que h_1 y h_2 son elementos de H. Como ϕ es sobreyectiva, existen elementos $g_1, g_2 \in G$ tales que $\phi(g_1) = h_1$ y $\phi(g_2) = h_2$. Por lo tanto,

$$h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) = \phi(g_2 g_1) = \phi(g_2)\phi(g_1) = h_2 h_1. \qquad \square$$

Estamos ahora en condiciones de caracterizar todos los grupos cíclicos.

Teorema 9.7. *Todo grupo cíclico de orden infinito es isomorfo a* $\mathbb{Z}$.

Demostración. Sea G un grupo cíclico de orden infinito y supongamos que a es un generador de G. Definamos la función $\phi : \mathbb{Z} \to G$ como $\phi : n \mapsto a^n$. Entonces

$$\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n).$$

Para mostrar que ϕ es inyectiva, supongamos que m y n son dos elementos en $\mathbb{Z}$, con $m \neq n$. Podemos suponer que $m > n$. Debemos mostrar que $a^m \neq a^n$. Supongamos lo contrario; es decir, $a^m = a^n$. En ese caso $a^{m-n} = e$, con $m - n > 0$, lo que contradice el hecho de que a tiene orden infinito. Nuestra función es sobreyectiva pues todo elemento en G puede ser escrito como a^n para algún entero n y $\phi(n) = a^n$. □

Teorema 9.8. *Si G es un grupo cíclico de orden n, entonces G es isomorfo a $\mathbb{Z}_n$.*

Demostración. Sea G un grupo cíclico de orden n generado por a y defina una función $\phi : \mathbb{Z}_n \to G$ como $\phi : k \mapsto a^k$, donde $0 \leq k < n$. La demostración de que ϕ es un isomorfismo es uno de los ejercicios al final del capítulo. □

Corolario 9.9. *Si G es un grupo de orden p, donde p es un número primo, entonces G es isomorfo a $\mathbb{Z}_p$.*

Demostración. La demostración es un resultado directo del Corolario 6.12. □

El principal objetivo en la teoría de grupos es el de clasificar todos los grupos; sin embargo, tiene sentido considerar que dos grupos isomorfos son en realidad el mismo grupo. Enunciamos este resultado en el siguiente teorema, cuya demostración dejamos coom ejercicio.

Teorema 9.10. *El isomorfismo de grupos define una relación de equivalencia en la clase de todos los grupos.*

Luego, podemos modificar nuestro objetivo de clasificar todos los grupos al de clasificar todos los grupos ***salvo isomorfismo***; es decir, consideraremos que dos grupos son el mismo si son isomorfos.

Teorema de Cayley

Cayley demostró que si G es un grupo, entonces es isomorfo a un grupo de permutaciones de algún conjunto; luego, todo grupo es un grupo de permutaciones. El Teorema de Cayley es lo que llamamos un teorema de representaciones. El objetivo de la teoría de representaciones es encontrar un isomorfismo de algún grupo G que queramos estudiar a un grupo sobre el que tengamos bastante información, tal como un grupo de permutaciones o de matrices.

Ejemplo 9.11. Considere el grupo $\mathbb{Z}_3$. La tabla de Cayley para $\mathbb{Z}_3$ es como sigue.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

La tabla de sumas para $\mathbb{Z}_3$ sugiere que es igual al grupo de permutaciones

$G = \{(0), (012), (021)\}$. El isomorfismo acá es

$$0 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} = (0)$$
$$1 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} = (012)$$
$$2 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} = (021).$$

Teorema 9.12 (Cayley)**.** *Todo grupo es isomorfo a un grupo de permutaciones.*

DEMOSTRACIÓN. Sea G un grupo. Debemos encontrar un grupo de permutaciones $\overline{G}$ que sea isomorfo a G. Para cualquier $g \in G$, definamos una función $\lambda_g : G \to G$ como $\lambda_g(a) = ga$. Afirmamos que λ_g es una permutación de G. Para demostrar que λ_g es 1-1, supongamos que $\lambda_g(a) = \lambda_g(b)$. Entonces

$$ga = \lambda_g(a) = \lambda_g(b) = gb.$$

Luego, $a = b$. Para demostrar que λ_g es sobre, debemos demostrar que para cada $a \in G$, existe b tal que $\lambda_g(b) = a$. Sea $b = g^{-1}a$.

Estamos preparados para definir nuestro grupo $\overline{G}$. Sea

$$\overline{G} = \{\lambda_g : g \in G\}.$$

Debemos mostrar que $\overline{G}$ es un grupo con la operación de composición de funciones y encontrar un isomorfismo entre G y $\overline{G}$. Tenemos la clausura bajo composición de funciones pues

$$(\lambda_g \circ \lambda_h)(a) = \lambda_g(ha) = gha = \lambda_{gh}(a).$$

Además,

$$\lambda_e(a) = ea = a$$

y

$$(\lambda_{g^{-1}} \circ \lambda_g)(a) = \lambda_{g^{-1}}(ga) = g^{-1}ga = a = \lambda_e(a).$$

Podemos definir un isomorfismo de G en $\overline{G}$ como $\phi : g \mapsto \lambda_g$. La operación de grupo se preserva pues

$$\phi(gh) = \lambda_{gh} = \lambda_g\lambda_h = \phi(g)\phi(h).$$

Es 1-1, pues si $\phi(g)(a) = \phi(h)(a)$, entonces

$$ga = \lambda_g a = \lambda_h a = ha.$$

Luego, $g = h$. Que ϕ sea sobre sigue del hecho de que $\phi(g) = \lambda_g$ para cualquier $\lambda_g \in \overline{G}$. □

El isomorfismo $g \mapsto \lambda_g$ se conoce como la ***representación regular izquierda*** de G.

Nota histórica

Arthur Cayley nació en Inglaterra en 1821, pero pasó la primera parte de su vida en Rusia, donde su padre era comerciante. Cayley se educó en Cambridge, donde ganó el primer Premio Smith en matemáticas. Ejerció como abogado la mayor parte de su vida adulta, y escribió varios trabajos antes de entrar a la profesión legal a los 25 años de edad. Durante su práctica como abogado siguió sus investigaciones matemáticas, escribiendo más de 300 publicaciones en esta etapa de su vida. Estas incluyeron parte de sus obras más importantes. En 1863 dejó la abogacía para convertirse en profesor en Cambridge. Cayley escribió más de 900 trabajos en áreas como teoría de grupos, geometría y álgebra lineal. Sus conocimentos legales eran muy apreciados en Cambridge; participó en la redacción de muchos de los estatutos de la universidad. Cayley fue también uno de los responsables de la admisión de mujeres a Cambridge.

9.2 Productos Directos

Dados dos grupos G y H, se puede construir un nuevo grupo a partir del producto Cartesiano de G y H, $G \times H$. Recíprocamente, dado un grupo grande, a veces es posible descomponer el grupo; es decir, un grupo a veces es isomorfo al producto directo de dos grupos menores. En lugar de estudiar el grupo grande G, es usualmente más fácil estudiar los grupos componentes de G.

Producto Directo Externo

Si $(G, \cdot)$ y $(H, \circ)$ son grupos, entonces podemos transformar el producto cartesiano de G y H en un nuevo grupo. Como conjunto, el grupo no es más que el conjunto de pares ordenados $(g, h) \in G \times H$ con $g \in G$ y $h \in H$. Podemos definir una operación binaria en $G \times H$ como

$$(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2);$$

es decir, simplemente multiplicamos los elementos en la primera coordenada usando el producto en G y los elementos en la segunda coordenada usando el producto de H. Hemos especificado las operaciones particulares $\cdot$ y $\circ$ en cada grupo para mayor claridad; usualmente escribiremos simplemente $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Proposición 9.13. *Sean G y H grupos. El conjunto $G \times H$ es un grupo con la operación $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ donde $g_1, g_2 \in G$ y $h_1, h_2 \in H$.*

Demostración. Claramente la operación binaria definida arriba es cerrada. Si e_G y e_H son las identidades de los grupos G y H respectivamente, entonces (e_G, e_H) es la identidad de $G \times H$. El inverso de $(g, h) \in G \times H$ es (g^{-1}, h^{-1}). El hecho de que la operación sea asociativa es consecuencia directa de la asociatividad de G y H. □

Ejemplo 9.14. Sea $\mathbb{R}$ el grupo de los números reales con la operación de adición. El producto cartesiano de $\mathbb{R}$ con si mismo, $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, también es un grupo, en el que la operación es simplemente la suma por coordenadas; es decir, $(a, b) + (c, d) = (a + c, b + d)$. La identidad $(0, 0)$ y el inverso de (a, b) es $(-a, -b)$.

Ejemplo 9.15. Considere

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}.$$

Si bien $\mathbb{Z}_2 \times \mathbb{Z}_2$ y $\mathbb{Z}_4$ ambos contienen cuatro elementos, no son isomorfos. Cada elemento (a, b) en $\mathbb{Z}_2 \times \mathbb{Z}_2$ tiene orden 2 o 1, pues $(a, b) + (a, b) = (0, 0)$; pero, $\mathbb{Z}_4$ es cíclico.

El grupo $G \times H$ se llama ***producto directo externo*** de G y H. Note que no hay nada especial en el hecho de haber usado solo dos grupos para formar un grupo nuevo. El producto directo

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n$$

de los grupos $G_1, G_2, \ldots, G_n$ se define de exactamente la misma forma. Si $G = G_1 = G_2 = \cdots = G_n$, escribiremos G^n en lugar de $G_1 \times G_2 \times \cdots \times G_n$.

Ejemplo 9.16. El grupo $\mathbb{Z}_2^n$, considerado como conjunto, es simplemente el conjunto de todas las n-tuplas binarias. La operación del grupo es el "o exclusivo" de dos n-tuplas binarias. Por ejemplo,

$$(01011101) + (01001011) = (00010110).$$

Este grupo es importante en la teoría de códigos, en criptografía y en muchas áreas de computación.

Teorema 9.17. *Sea $(g, h) \in G \times H$. Si g y h tienen órdenes finitos r y s respectivamente, entonces el orden de (g, h) en $G \times H$ es el mínimo común múltiplo de r y s.*

Demostración. Supongamos que m es el mínimo común múltiplo de r y s y sea $n = |(g, h)|$. Entonces

$$(g, h)^m = (g^m, h^m) = (e_G, e_H)$$
$$(g^n, h^n) = (g, h)^n = (e_G, e_H).$$

Luego, n divide a m, y $n \leq m$. Sin embargo, por la segunda ecuación, tanto r como s dividen a n; por lo tanto, n es un múltiplo común de r y s. Como m es el *mínimo común múltiplo* de r y s, $m \leq n$. Por lo tanto, m debe ser igual a n. □

Corolario 9.18. *Sea $(g_1, \ldots, g_n) \in \prod G_i$. Si g_i tiene orden finito r_i en G_i, entonces el orden de $(g_1, \ldots, g_n)$ en $\prod G_i$ es el mínimo común múltiplo de $r_1, \ldots, r_n$.*

Ejemplo 9.19. Sea $(8, 56) \in \mathbb{Z}_{12} \times \mathbb{Z}_{60}$. Como $\text{mcd}(8, 12) = 4$, el orden de 8 es $12/4 = 3$ en $\mathbb{Z}_{12}$. Similarmente, el orden de 56 en $\mathbb{Z}_{60}$ es 15. El mínimo común múltiplo de 3 y 15 es 15; luego, $(8, 56)$ tiene orden 15 en $\mathbb{Z}_{12} \times \mathbb{Z}_{60}$.

Ejemplo 9.20. El grupo $\mathbb{Z}_2 \times \mathbb{Z}_3$ consiste de los pares

$$(0, 0), \quad (0, 1), \quad (0, 2), \quad (1, 0), \quad (1, 1), \quad (1, 2).$$

En este caso, a diferencia del caso de $\mathbb{Z}_2 \times \mathbb{Z}_2$ y $\mathbb{Z}_4$, es verdad que $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. Solo debemos mostrar que $\mathbb{Z}_2 \times \mathbb{Z}_3$ es cíclico. Es fácil ver que $(1, 1)$ es un generador para $\mathbb{Z}_2 \times \mathbb{Z}_3$.

El siguiente teorema nos dice exactamente cuándo el producto directo de dos grupos cíclicos es cíclico.

Teorema 9.21. *El grupo $\mathbb{Z}_m \times \mathbb{Z}_n$ es isomorfo a $\mathbb{Z}_{mn}$ si y solo si* $\text{mcd}(m, n) = 1$.

DEMOSTRACIÓN. Primero mostraremos que si $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$, entonces $\text{mcd}(m,n) = 1$. Demostraremos el contrapositivo; es decir, mostraremos que si $\text{mcd}(m,n) = d > 1$, entonces $\mathbb{Z}_m \times \mathbb{Z}_n$ no puede ser cíclico. Note que mn/d es divisible tanto por m como por n; luego, cualquier elemento $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$,

$$\underbrace{(a,b) + (a,b) + \cdots + (a,b)}_{mn/d \text{ times}} = (0,0).$$

Por lo tanto, ningún (a,b) puede generar todo $\mathbb{Z}_m \times \mathbb{Z}_n$.

El recíproco es consecuencia directa del Teorema 9.17 pues $\text{mcm}(m,n) = mn$ si y solo si $\text{mcd}(m,n) = 1$. □

Corolario 9.22. *Sean $n_1, \ldots, n_k$ enteros positivos. Entonces*

$$\prod_{i=1}^{k} \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 \cdots n_k}$$

si y solo si $\text{mcd}(n_i, n_j) = 1$ *para todo* $i \neq j$.

Corolario 9.23. *Si*

$$m = p_1^{e_1} \cdots p_k^{e_k},$$

donde los p_i son primos distintos, entonces

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

DEMOSTRACIÓN. Como el máximo común divisor de $p_i^{e_i}$ y $p_j^{e_j}$ es 1 para $i \neq j$, la demostración se sigue del Corolario 9.22. □

En el Capítulo 13, demostraremos que todos los grupos abelianos finitos son isomorfos a productos directos de la forma

$$\mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$$

donde $p_1, \ldots, p_k$ son primos (no necesariamente distintos).

Producto Directo Interno

El producto directo externo de dos grupos construye un grupo grande a partir de los dos grupos menores. Quisiéramos ser capaces de revertir el proceso y descomponer convenientemente un grupo grande en sus componentes como producto directo; es decir, quisiéramos poder decir cuándo un grupo es isomorfo al producto directo de dos de sus subgrupos.

Sea G un grupo con subgrupos H y K que satisfagan las siguientes condiciones.

- $G = HK = \{hk : h \in H, k \in K\}$;
- $H \cap K = \{e\}$;
- $hk = kh$ para todo $k \in K$ y $h \in H$.

Entonces G es el ***producto directo interno*** de H y K.

Ejemplo 9.24. El grupo $U(8)$ es el producto directo interno de

$$H = \{1,3\} \quad \text{y} \quad K = \{1,5\}.$$

Ejemplo 9.25. El grupo dihedral D_6 es un producto directo interno de sus dos subgrupos

$$H = \{\mathrm{id}, r^3\} \quad \text{and} \quad K = \{\mathrm{id}, r^2, r^4, s, r^2s, r^4s\}.$$

Se puede mostrar fácilmente que $K \cong S_3$; por lo tanto, $D_6 \cong \mathbb{Z}_2 \times S_3$.

Ejemplo 9.26. No todo grupo puede ser escrito como el producto directo interno de dos subgrupos propios. Si el grupo S_3 fuese un producto directo interno de subgrupos propios H y K, entonces uno de ellos, digamos H, tendría que tener orden 3. En ese caso H es el subgrupo $\{(1), (123), (132)\}$. El subgrupo K tiene que tener orden 2 pero sin importar cuál subgrupo escojamos como K, la condición de que $hk = kh$ nunca se cumplirá para $h \in H$ y $k \in K$.

Teorema 9.27. *Sea G el producto directo interno de dos subgrupos H y K. Entonces G es isomorfo a $H \times K$.*

Demostración. Como G es un producto directo interno, podemos escribir cualquier elemento $g \in G$ como $g = hk$ para ciertos $h \in H$ y $k \in K$. Definamos una función $\phi : G \to H \times K$ como $\phi(g) = (h, k)$.

El primer problema que debemos enfrentar es mostrar que ϕ es una función bien definida; es decir, debemos mostrar que h y k están únicamente determinados por g. Supongamos que $g = hk = h'k'$. Entonces $h^{-1}h' = k(k')^{-1}$ está tanto en H como en K, así es que debe ser la identidad. Por lo tanto, $h = h'$ y $k = k'$, lo que demuestra que ϕ está, en efecto, bien definida.

Para demostrar que ϕ preserva la operación de grupo, sean $g_1 = h_1k_1$ y $g_2 = h_2k_2$ y observemos que

$$\begin{aligned}
\phi(g_1g_2) &= \phi(h_1k_1h_2k_2) \\
&= \phi(h_1h_2k_1k_2) \\
&= (h_1h_2, k_1k_2) \\
&= (h_1, k_1)(h_2, k_2) \\
&= \phi(g_1)\phi(g_2).
\end{aligned}$$

Dejaremos la demostración de que ϕ es una biyección como ejercicio. □

Demostración. Definamos una función $\psi : H \times K \to G$ como $\psi((h, k) = hk$. La operación de grupo se preserva pues

$$\psi((h_1, k_1)(h_2, k_2)) = \psi((h_1h_2, k_1k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \psi((h_1, k_1))\psi((h_2, k_2))$$

Para verificar que ψ es 1-1, supongamos que $hk = h'k'$. Entonces $h^{-1}h' = k(k')^{-1}$ está tanto en H como en K, así es que debe ser la identidad. Por lo tanto, $h = h'$ y $k = k'$, lo que demuestra que ψ es 1-1.

La sobreyectividad es consecuencia inmediata de la definición del producto directo interno. □

Ejemplo 9.28. El grupo $\mathbb{Z}_6$ es un producto directo interno isomorfo a $\{0, 2, 4\} \times \{0, 3\}$.

Podemos extender la definición de producto directo interno de G a una colección de subgrupos $H_1, H_2, \ldots, H_n$ de G, condicionándolos a que

- $G = H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n : h_i \in H_i\}$;
- $H_i \cap \langle \cup_{j \neq i} H_j \rangle = \{e\}$;
- $h_ih_j = h_jh_i$ para todo $h_i \in H_i$ y $h_j \in H_j$.

Dejaremos la demostración del siguiente teorema como ejercicio.

Teorema 9.29. *Sea G el producto interno de los subgrupos H_i, donde $i = 1, 2, \ldots, n$. Entonces G es isomorfo a $\prod_i H_i$.*

Sage Sage puede determinar rápidamente si dos grupos de permutaciones son isomorfos, aunque esto debiera ser, en teoría, un cálculo muy difícil.

9.3 Ejercicios

1. Demuestre que $\mathbb{Z} \cong n\mathbb{Z}$ para $n \neq 0$.

2. Demuestre que $\mathbb{C}^*$ es isomorfo al subgrupo de $GL_2(\mathbb{R})$ que consiste de las matrices de la forma

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

3. Demuestre o refute: $U(8) \cong \mathbb{Z}_4$.

4. Demuestre que $U(8)$ es isomorfo al grupo de matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

5. Muestre que $U(5)$ es isomorfo a $U(10)$, pero $U(12)$ no lo es.

6. Muestre que las raíces n-ésimas de la unidad forman un grupo isomorfo a $\mathbb{Z}_n$.

7. Muestre que cualquier grupo cíclico de orden n es isomorfo a $\mathbb{Z}_n$.

8. Demuestre que $\mathbb{Q}$ no es isomorfo a $\mathbb{Z}$.

9. Sea $G = \mathbb{R} \setminus \{-1\}$ y defina una operación binaria en G como

$$a * b = a + b + ab.$$

Demuestre que G es un grupo con esta operación. Muestre que $(G, *)$ es isomorfo al grupo multiplicativo de los números reales distintos de cero.

10. Muestre que las matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

forman un grupo. Encuentre un isomorfismo de G con un grupo conocido de orden 6.

11. Encuentre cinco grupos no isomorfos de orden 8.

12. Demuestre que S_4 no es isomorfo a D_{12}.

13. Sea $\omega = \text{cis}(2\pi/n)$ una raíz n-ésima primitiva de la unidad. Demuestre que las matrices

$$A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \quad \text{y} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

generan un grupo multiplicativo isomorfo a D_n.

14. Muestre que el conjunto de todas las matrices de la forma

$$\begin{pmatrix} \pm 1 & k \\ 0 & 1 \end{pmatrix},$$

es un grupo isomorfo a D_n, donde las entradas de la matriz están en $\mathbb{Z}_n$.

15. Liste todos los elementos de $\mathbb{Z}_4 \times \mathbb{Z}_2$.

16. Encuentre el orden de cada uno de los siguientes elementos.

(a) $(3, 4)$ en $\mathbb{Z}_4 \times \mathbb{Z}_6$

(b) $(6, 15, 4)$ en $\mathbb{Z}_{30} \times \mathbb{Z}_{45} \times \mathbb{Z}_{24}$

(c) $(5, 10, 15)$ en $\mathbb{Z}_{25} \times \mathbb{Z}_{25} \times \mathbb{Z}_{25}$

(d) $(8, 8, 8)$ en $\mathbb{Z}_{10} \times \mathbb{Z}_{24} \times \mathbb{Z}_{80}$

17. Demuestre que D_4 no puede ser el producto directo interno de dos de sus subgrupos propios.

18. Demuestre que el subgrupo de $\mathbb{Q}^*$ que consiste de elementos de la forma $2^m 3^n$ para $m, n \in \mathbb{Z}$ es un producto directo interno isomorfo a $\mathbb{Z} \times \mathbb{Z}$.

19. Demuestre que $S_3 \times \mathbb{Z}_2$ es isomorfo a D_6. ¿Puede hacer una conjetura sobre D_{2n}? Demuestre su conjetura.

20. Demuestre o refute: Todo grupo abeliano de orden divisible por 3 contiene un subgrupo de orden 3.

21. Demuestre o refute: Todo grupo no abeliano de orden divisible por 6 contiene un subgrupo de orden 6.

22. Sea G un grupo de orden 20. Si G tiene subgrupos H y K de órdenes 4 y 5 respectivamente tales que $hk = kh$ para todo $h \in H$ y $k \in K$, demuestre que G es el producto directo interno de H y K.

23. Demuestre o refute la siguiente aseveración. Sean G, H, y K grupos. Si $G \times K \cong H \times K$, entonces $G \cong H$.

24. Demuestre o refute: Existe un grupo abeliano no cíclico de orden 51.

25. Demuestre o refute: Existe un grupo abeliano no cíclico de orden 52.

26. Sea $\phi : G \to H$ un isomorfismo de grupos. Muestre que $\phi(x) = e_H$ si y solo si $x = e_G$, donde e_G y e_H son las identidades de G y H, respectivamente.

27. Sea $G \cong H$. Muestre que si G es cíclico, entonces también lo es H.

28. Demuestre que cualquier grupo G de orden p, p primo, debe ser isomorfo a $\mathbb{Z}_p$.

29. Muestre que S_n es isomorfo a un subgrupo de A_{n+2}.

30. Demuestre que D_n es isomorfo a un subgrupo de S_n.

31. Sean $\phi : G_1 \to G_2$ y $\psi : G_2 \to G_3$ isomorfismos. Muestre que ϕ^{-1} y $\psi \circ \phi$ son ambos isomorfismos. Usando estos resultados, muestre que el isomorfismo de grupos define una relación de equivalencia en la clase de todos los grupos.

32. Demuestre que $U(5) \cong \mathbb{Z}_4$. ¿Puede generalizar este resultado para $U(p)$, donde p es primo?

33. Escriba las permutaciones asociadas con cada elemento de S_3 en la demostración del Teorema de Cayley.

34. Un ***automorfismo*** de un grupo G es un isomorfismo consigo mismo. Demuestre que la conjugación compleja es un automorfismo del grupo aditivo de los números complejos; es decir, muestre que la función $\phi(a+bi) = a-bi$ es un isomorfismo de $\mathbb{C}$ a $\mathbb{C}$.

35. Demuestre que $a+ib \mapsto a-ib$ es un automorfismo de $\mathbb{C}^*$.

36. Demuestre que $A \mapsto B^{-1}AB$ es un automorfismo de $SL_2(\mathbb{R})$ para todo B en $GL_2(\mathbb{R})$.

37. Denotaremos el conjunto de todos los automorfismo de G como $\mathrm{Aut}(G)$. Demuestre que $\mathrm{Aut}(G)$ es un subgrupo de S_G, el grupo de permutaciones de G.

38. Encuentre $\mathrm{Aut}(\mathbb{Z}_6)$.

39. Encuentre $\mathrm{Aut}(\mathbb{Z})$.

40. Encuentre dos grupos G y H no isomorfos tales que $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$.

41. Sea G un grupo y $g \in G$. Definamos una función $i_g : G \to G$ como $i_g(x) = gxg^{-1}$. Demuestre que i_g define un automorfismo de G. Un automorfismo de este tipo se llama ***automorfismo interno***. El conjunto de todos los automorfismos internos se denota por $\mathrm{Inn}(G)$.

42. Demuestre que $\mathrm{Inn}(G)$ es un subgrupo de $\mathrm{Aut}(G)$.

43. ¿Cuáles son los automorfismos internos del grupo de los cuaterniones Q_8? ¿Es $\mathrm{Inn}(G) = \mathrm{Aut}(G)$ en este caso?

44. Sea G un grupo y $g \in G$. Definamos las funciones $\lambda_g : G \to G$ y $\rho_g : G \to G$ como $\lambda_g(x) = gx$ y $\rho_g(x) = xg^{-1}$. Muestre que $i_g = \rho_g \circ \lambda_g$ es un automorfismo de G. El isomorfismo $g \mapsto \rho_g$ se llama ***representación regular derecha*** de G.

45. Sea G el producto directo interno de los subgrupos H y K. Muestre que la función $\phi : G \to H \times K$ definida por $\phi(g) = (h,k)$ para $g = hk$, donde $h \in H$ y $k \in K$, es biyectiva.

46. Sean G y H grupos isomorfos. Si G tiene un subgrupo de orden n, demuestre que H también tiene un subgrupo de orden n.

47. Si $G \cong \overline{G}$ y $H \cong \overline{H}$, muestre que $G \times H \cong \overline{G} \times \overline{H}$.

48. Demuestre que $G \times H$ es isomorfo a $H \times G$.

49. Sean $n_1, \ldots, n_k$ enteros positivos. Muestre que

$$\prod_{i=1}^{k} \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 \cdots n_k}$$

si y solo si $\mathrm{mcd}(n_i, n_j) = 1$ para $i \neq j$.

50. Demuestre que $A \times B$ es abeliano si y solo si A y B son abelianos.

51. Si G es el producto directo interno de $H_1, H_2, \ldots, H_n$, demuestre que G es isomorfo a $\prod_i H_i$.

52. Sean H_1 y H_2 subgrupos de G_1 y G_2, respectivamente. Demuestre que $H_1 \times H_2$ es un subgrupo de $G_1 \times G_2$.

53. Sean $m, n \in \mathbb{Z}$. Demuestre que $\langle m, n\rangle = \langle d\rangle$ si y solo si $d = \text{mcd}(m, n)$.

54. Sean $m, n \in \mathbb{Z}$. Demuestre que $\langle m\rangle \cap \langle n\rangle = \langle l\rangle$ si y solo si $l = \text{mcm}(m, n)$.

55. (Grupos de orden $2p$) En esta serie de ejercios clasificaremos todos los grupos de orden $2p$, donde p es un primo impar.

(a) Supongamos que G es un grupo de orden $2p$, sonde p es un primo impar. Si $a \in G$, muestre que a tiene orden 1, 2, p, o $2p$.

(b) Supongamos que G tiene un elemento de orden $2p$. Demuestre que G es isomorfo a $\mathbb{Z}_{2p}$. Luego, G es cíclico.

(c) Supongamos que G no contiene un elemento de orden $2p$. Muestre que G contiene un elemento de orden p. *Ayuda*: Suponga que G no contiene un elemento de orden p.

(d) Supongamos que G no contiene un elemento de orden $2p$. Muestre que G contiene un elemento de orden 2.

(e) Sea P un subgrupo de G de orden p e $y \in G$ de orden 2. Muestre que $yP = Py$.

(f) Supongamos que G no contiene un elemento de orden $2p$ y que $P = \langle z\rangle$ es un subgrupo de orden p generado por z. Si y es un elemento de orden 2, entonces $yz = z^k y$ para algún $2 \leq k < p$.

(g) Supongamos que G no contiene un elemento de orden $2p$. Demuestre que G no es abeliano.

(h) Supongamos que G no contiene un elemento de orden $2p$ y $P = \langle z\rangle$ es un subgrupo de orden p generado por z e y es n elemento de orden 2. Muestre que podemos listar los elementos de G como $\{z^i y^j \mid 0 \leq i < p, 0 \leq j < 2\}$.

(i) Supongamos que G no contiene un elemento de orden $2p$ y $P = \langle z\rangle$ es un subgrupo de orden p generado por z e y es un elemento de orden 2. Demuestre que el producto $(z^i y^j)(z^r y^s)$ puede ser expresado como $z^m y^n$ para ciertos enteros no negativos m, n. Luego, concluya que solo hay una posibilidad para un grupo no-abeliano de orden $2p$, debe ser por lo tanto el grupo que ya conocemos, el grupo dihedral.

9.4 Sage

Sage tiene una capacidad limitada de creación efectiva de isomorfismos. Sin embargo, tiene es muy efectivo para determinar si dos grupos de permutaciones son isomorfos. Esto nos permitirá iniciar un pequeño proyecto para localizar *todos* los grupos de orden menor a 16 en los grupos de permutaciones de Sage.

Verificación de Isomorfía

Si `G` y `H` son dos grupos de permutaciones, entonces el comando `G.is_isomorphic(H)` entregará `True` o `False` según si los grupos sean o no isomorfos. Como ser "isomorfo a" es una relación de equivalencia por el Teorema 9.10, no importa cuál grupo ocupa el lugar de `G` y cuál ocupa el lugar de `H`.

Tenemos así algunos ejemplos más con los que trabajar, veamos el comando Sage que crea el producto directo externo. Si `G` y `H` son dos grupos de permutaciones, entonces el comando `direct_product_permgroups([G,H])` entregará el producto directo externo como un nuevo grupo de permutaciones.

Note que esta es una función (no un método) y el input es una lista. En lugar de tener solo dos grupos en la lista, cualquier cantidad de grupos puede ser suministrada. Ilustramos la verificación de isomorfismos en el contexto del Teorema 9.21, que es una equivalencia, de manera que nos dice *exactamente* cuándo tenemos grupos isomorfos. Usamos grupos cíclicos de permutaciones en reemplazo de $\mathbb{Z}_n$ por el Teorema 9.8.

Primero, dos grupos isomorfos.

```
m = 12
n = 7
gcd(m, n)
```

```
1
```

```
G = CyclicPermutationGroup(m)
H = CyclicPermutationGroup(n)
dp = direct_product_permgroups([G, H])
K = CyclicPermutationGroup(m*n)
K.is_isomorphic(dp)
```

```
True
```

Ahora, dos grupos no isomorfos.

```
m = 15
n = 21
gcd(m, n)
```

```
3
```

```
G = CyclicPermutationGroup(m)
H = CyclicPermutationGroup(n)
dp = direct_product_permgroups([G, H])
K = CyclicPermutationGroup(m*n)
K.is_isomorphic(dp)
```

```
False
```

Note como el simple cálculo de un máximo común divisor predice el cálculo extremadamente complicado de determinar si dos grupos son isomorfos. Esta es una buena ilustración del poder de las matemáticas, que reemplaza un problema difícil (isomorfía de grupos) por un problema simple (factorización y divisibilidad de enteros). Construyamos un producto directo de grupos cíclicos más, pero con tres grupos, con órdenes que sean relativamente primos de a dos.

Si intenta lo siguiente con parámetros mayores puede que obtenga un error (`database_gap`).

```
m = 6
n = 5
r = 7
G = CyclicPermutationGroup(m)
H = CyclicPermutationGroup(n)
L = CyclicPermutationGroup(r)
dp = direct_product_permgroups([G, H, L])
K = CyclicPermutationGroup(m*n*r)
K.is_isomorphic(dp)
```

```
True
```

Clasificando Grupos Finitos

Una vez que concebimos grupos isomorfos como el "mismo", o "fundamentalmente iguales," o "estructuralmente idénticos," es natural preguntarnos cuántos grupos finitos "realmente diferentes" existen. El Corolario 9.9 nos entrega una respuesta parcial: para cada número primo hay exactamente un grupo finito, con $\mathbb{Z}_p$ como una manifestación concreta.

Embarquémosnos en la búsqueda de todos los grupos de orden menor a 16 en los grupos de permutación de Sage. Para órdenes primos $1, 2, 3, 5, 7, 11$ y 13 sabemos que existe solo un grupo para cada uno, y podemos obtenerlos todos:

```
[CyclicPermutationGroup(p) for p in [1, 2, 3, 5, 7, 11, 13]]
```

```
[Cyclic group of order 1 as a permutation group,
 Cyclic group of order 2 as a permutation group,
 Cyclic group of order 3 as a permutation group,
 Cyclic group of order 5 as a permutation group,
 Cyclic group of order 7 as a permutation group,
 Cyclic group of order 11 as a permutation group,
 Cyclic group of order 13 as a permutation group]
```

Así nuestro primer caso desconocido es el orden 4. Sage conoce al menos tres grupos así, y podemos usar Sage para verificar si cualquier par de ellos es isomorfo. Note que como "ser isomorfo a" es una relación de equivalencia y por lo tanto una relación transitiva, las dos verificaciones que siguen son suficientes.

```
G = CyclicPermutationGroup(4)
H = KleinFourGroup()
T1 = CyclicPermutationGroup(2)
T2 = CyclicPermutationGroup(2)
K = direct_product_permgroups([T1, T2])
G.is_isomorphic(H)
```

```
False
```

```
H.is_isomorphic(K)
```

```
True
```

Tenemos así al menos dos grupos diferentes: $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$, el último también conocido como 4-grupo de Klein. Sage no será capaz de decirnos si tenemos una lista *completa* — eso siempre requerirá resultados teóricos como el Teorema 9.10. Pronto tendremos un resultado más general que resuelva el caso de orden 4, pero por ahora, un análisis cuidadoso (a mano) de las posibilidades para la tabla de Cayley de un grupo de orden 4 debiera llevarle a las dos posibilidades de arriba como las únicas posibilidades. Intente deducir como se debiera ver la tabla de Cayley de un grupo de orden 4, dado que ya sabre sobre el elemento identidad, los inversos y la ley de cancelación.

Hemos visto al menos dos grupos de orden 6 (el siguiente en la lista de nuestros órdenes no primos). Uno es abeliano y el otro no los es, de manera que no necesitamos que Sage lo diga para saber que son estructuralmente diferentes. Pero hagámoslo de todas formas.

```
G = CyclicPermutationGroup(6)
H = SymmetricGroup(3)
G.is_isomorphic(H)
```

```
False
```

¿Es todo? Existe $\mathbb{Z}_3 \times \mathbb{Z}_2$, pero ese es simplemente $\mathbb{Z}_6$ pues 2 y 3 son relativamente primos. El grupo dihedral, D_3, es simplemente S_3, el grupo simétrico en 3 símbolos.

```
G = DihedralGroup(3)
H = SymmetricGroup(3)
G.is_isomorphic(H)
```

```
True
```

El Ejercicio 9.3.55 de esta sección clasifica todos los grupos de orden $2p$, donde p es un primo impar. Un tal grupo puede ser un grupo cíclico o un grupo dihedral. Así los dos grupos de arriba, $\mathbb{Z}_6$ y D_3, son realmente todos los grupos de orden6.

Por este resultado general, además del orden 6, también conocemos las listas completas de grupos de órdenes 10 y 14. Continuará.

Productos Directos Internos

Un producto directo interno es una proposición sobre subgrupos de un solo grupo, junto con un teorema que los relaciona con un producto directo externo. Trabajaremos con un ejemplo acá que ilustrará la naturaleza de un producto directo interno.

Dado un entero n, el conjunto de los enteros positivos menores a n, y relativamente primos con n forma un grupo con la operación de multiplicación mód n. Trabajaremos en el conjunto `Integers(n)` donde podemos sumar y multiplicar, pero nos restringiremos a usar solamente la multiplicación.

Primero construiremos el grupo en sí. Notemos cómo debemos convertir `x` en un entero (un elemento de `ZZ`) de manera que el cálculo del máximo común divisor se realice correctamente.

```
Z36 = Integers(36)
U = [x for x in Z36 if gcd(ZZ(x), 36) == 1]
U
```

```
[1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35]
```

Tenemos así un grupo de orden 12. Intentaremos encontrar un subgrupo de orden 6 y un subgrupo de orden 2 para formar el producto directo interno, y restringiremos nuestra búsqueda a los subgrupos cíclicos de orden 6. Sage tiene un método que nos entrega el orden de cada uno de estos elementos, en relación a la multiplicación, así es que examinemos eso a continuación.

```
[x.multiplicative_order() for x in U]
```

```
[1, 6, 6, 6, 3, 2, 2, 6, 3, 6, 6, 2]
```

Tenemos muchas opciones para generadores de un subgrupo cíclico de orden 6 y para un subgrupo cíclico de orden 2. Por supuesto, algunas de los posibles generadores de un subgrupo de orden 6 generarán el mismo subgrupo. ¿Puede descubrir, simplemente contando, cuántos subgrupos de orden 6 hay? Escogeremos el primer elemento de orden 6, y el último elemento de orden 2, sin razón particular. Después de hacer esto una vez, le invitamos a intentar otras opciones para entender por qué algunas nos llevan a un producto directo interno y otras no. Note que elegimos los elementos de la lista `U` de manera de estar seguros que son elementos de `Z36` y se comportarán correctamente al ser multiplicados.

```
a = U[1]
A = [a^i for i in srange(6)]
A
```

```
[1, 5, 25, 17, 13, 29]
```

```
b = U[11]
B = [b^i for i in srange(2)]
B
```

```
[1, 35]
```

Así `A` y `B` son dos subgrupos cíclicos. Note que su intersección es el elemento identidad, uno de nuestros requisitos para un producto directo interno. Tenemos así un buen comienzo.

```
[x for x in A if x in B]
```

```
[1]
```

`Z36` es un grupo abeliano, así la condición de que todos los productos conmuten, se cumplirá, pero ilustraremos los comandos Sage que verificarán esto en una situación no abeliana.

```
all([x*y == y*x for x in A for y in B])
```

```
True
```

Finalmente, necesitamos verificar que formando los productos de elementos de `A` y `B` obtenemos todo el grupo. Ordenar la lista resultante nos facilitará la verificación visual, y es necesario si queremos que Sage haga la verificación.

```
T = sorted([x*y for x in A for y in B])
T
```

```
[1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35]
```

```
T == U
```

```
True
```

Eso es. Resumimos ahora toda esta información en la proposición que "`U` es el producto interno directo de `A` y `B`." Por el Teorema 9.27, vemos que `U` es isomorfo al producto de un grupo cíclico de orden 6 y un grupo cíclico de orden 2. Así es que en un sentido muy real, `U` no es más ni menos complicado que $\mathbb{Z}_6 \times \mathbb{Z}_2$, que a su vez es isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Entendemos así completamente la "estructura" de `U`. Por ejemplo, podemos ver que `U` no es cíclico, pues cuando se escribe como producto de grupos cíclicos, los órdenes no son relativamente primos. La expresión final de `U` sugiere que se pueden encontrar tres subgrupos cíclicos de `U`, con órdenes 3, 2 y 2, de manera que `U` es un producto directo interno de tres subgrupos.

9.5 Ejercicios en Sage

1. Este ejercicio trata de poner en práctica el Teorema de Cayley. Primero, lea y estudie el teorema. Dese cuenta que este resultado por sí solo es fundamentalmente de interés teórico, pero con algo más de teoría podríamos llegar

a aspectos más sutiles de esto, (un área conocida como "teoría de representaciones").
Usted debiese crear estas representaciones fundamentalmente con lapiz y papel, usando Sage como una calculadora sofisticada y asistente. No es necesario que incluya todos estos cálculos en su hoja de trabajo. Cunstruya las representaciones pedidas e incluya verificaciones en Sage que demuestren que su representación representa correctamente al grupo.
Comience por construir una representación permutacionesl del grupo de los cuaterniones, Q. Hay ocho elemento en Q $(\pm 1, \pm I, \pm J, \pm K)$, de manera que obtendrá un subgrupo de S_8. Para cada $g \in Q$ forme la función T_g, definida como $T_g(x) = xg$. Note que esta definición está al "revés" de la dada en el texto. Esto es pues Sage compone las permutaciones de izquierda a derecha, mientra que en el texto se componen de derecha a izquierda. Para crear las permutaciones T_g, la forma de dos líneas de escribir las permutaciones podría ser un buen paso intermedio. Probablemente querrá "codificar" cada elemento de Q con un entero en $\{1, 2, \ldots, 8\}$.
Una tal representación está incluida en Sage como `QuaternionGroup()` — su respuesta debiese verse muy similar, pero quizás no idéntica. Puede usar el método `.is_isomorphic()` para verificar si su representación está bien. Pero no lo use como sustituto para la parte de cada pregunta que le pide estudiar propiedades de su representación con este objetivo.

(a) Construya la representación permutacional de $\mathbb{Z}_2 \times \mathbb{Z}_4$ descrita en el Teorema de Cayley. (Recuerde que este grupo es aditivo, mientras el teorema usa notación multiplicativa.) Incluya la representación de *cada uno* de los 8 elementos. Después construya la el grupo permutacional como subgrupo de un grupo simétrico generado por exactamente dos de los 8 elementos que ya construyó. Ayuda: ¿qué elementos de $\mathbb{Z}_2 \times \mathbb{Z}_4$ podría usar para generar todo $\mathbb{Z}_2 \times \mathbb{Z}_4$? Use comandos en Sage para investigar distintas propiedades de su grupo de permutaciones, distintos de `.list()`, para proveer evidencia de que su subgrupo es correcto.

(b) Construya una representación permutacional de $U(24)$, el grupo de unidades mód 24. Nuevamente entregue una representación para *cada* elemento. Después construya el grupo como subgrupo del grupo simétrico generándolo con tres elementos. Para determinar estos tres generadores, es probable que necesite entender $U(24)$ como producto directo interno. Use comandos en Sage para investigar distintas propiedades de su grupo de permutaciones, distintos de `.list()`, para proveer evidencia de que su subgrupo es correcto.

2. Considere las simetrías del decágono regular, D_{10} en el texto, `DihedralGroup(10)` en Sage. Supongamos que los vértices del decágono han sido etiquetados del 1 al 10 en orden. Identifique la permutación que corresponde a una rotación en 180 grados y úsela para generar un subgrupo R de orden 2. Identifique la permutación que corresponde a una rotación en 72 grados, y cualquiera de las diez permutaciones que corresponden a reflexiones del decágono respecto a una recta. Use estas últimas dos permutaciones para generar un subgrupo S de orden 10. Use Sage para verificar que el grupo dihedral completo es el producto directo interno de los subgrupos R y S comprobando las condiciones en la definición de un producto directo interno.
Tenemos un teorema que dice que si un grupo es un producto directo interno, entonces es isomorfo a algún producto directo externo. Comprenda que eso no quiere decir que pueda usar el recíproco en este problema. En otras palabras, establecer un isomorfismo de G con un producto directo externo *no demuestra* que G sea un producto directo interno.

10

Subgrupos Normales y Grupos Cociente

Si H es un subgrupo de un grupo G, entonces las clases laterales derechas no son siempre las mismas que las clases laterales izquierdas; es decir, no siempre se cumple que $gH = Hg$ para todo $g \in G$. Los subgrupos que tienen esta propiedad juegan un papel crítico en la teoría de grupos—permiten la construcción de una nueva clase de grupos, llamados grupos cociente. Los grupos cociente pueden ser estudiados directamente o usando homomorfismos, una generalización de los isomorfismos. Estudiaremos homomorfismos en el Capítulo 11.

10.1 Grupos Cociente y Subgrupos Normales

Subgrupos Normales

Un subgrupo H de un grupo G es ***normal*** en G se $gH = Hg$ para todo $g \in G$. Es decir, un subgrupo normal de un grupo G es un subgrupo para el que las clases laterales derechas e izquierdas coinciden.

Ejemplo 10.1. Sea G un grupo abeliano. Todo subgrupo H de G es un subgrupo normal. Como $gh = hg$ para todo $g \in G$ y $h \in H$, siempre se cumple que $gH = Hg$.

Ejemplo 10.2. Sea H el subgrupo de S_3 que consiste de los elementos (1) y (12). Como

$$(123)H = \{(123), (13)\} \quad \text{and} \quad H(123) = \{(123), (23)\},$$

H no puede ser un subgrupo normal de S_3. Sin embargo, el subgrupo N, que consiste de las permutaciones (1), (123), y (132), es normal pues las clases laterales de N son

$$N = \{(1), (123), (132)\}$$
$$(12)N = N(12) = \{(12), (13), (23)\}.$$

El siguiente teorema es fundamental para nuestra comprensión de los subgrupo normales.

Teorema 10.3. *Sea G un grupo y N un subgrupo de G. Entonces las siguientes proposiciones son equivalentes.*

1. *El subgrupo N es normal en G.*

2. *Para todo* $g \in G$, $gNg^{-1} \subset N$.

3. *Para todo* $g \in G$, $gNg^{-1} = N$.

DEMOSTRACIÓN. (1) $\Rightarrow$ (2). Como N es normal en G, $gN = Ng$ para todo $g \in G$. Luego, para un $g \in G$ dado y para $n \in N$, existe n' en N tal que $gn = n'g$. Por lo tanto, $gng^{-1} = n' \in N$ y $gNg^{-1} \subset N$.

(2) $\Rightarrow$ (3). Sea $g \in G$. Como $gNg^{-1} \subset N$, solo debemos demostrar que $N \subset gNg^{-1}$. Para $n \in N$, $g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in N$. Luego, $g^{-1}ng = n'$ para algún $n' \in N$. Por lo tanto, $n = gn'g^{-1}$ está en gNg^{-1}.

(3) $\Rightarrow$ (1). Supongamos que $gNg^{-1} = N$ para todo $g \in G$. Entonces para cualquier $n \in N$ existe $n' \in N$ tal que $gng^{-1} = n'$. Por lo tanto, $gn = n'g$ y $gN \subset Ng$. Similarmente, $Ng \subset gN$. □

Grupos cociente

Si N es un subgrupo normal de un grupo G, entonces las clases laterales de N en G forman un grupo G/N con la operación $(aN)(bN) = abN$. Este grupo se llama ***cociente*** de G por N. Nuestra primera tarea es demostrar que G/N es realmente un grupo.

Teorema 10.4. *Sea N un subgrupo normal de un grupo G. Las clases laterales de N en G forman un grupo G/N de orden $[G : N]$.*

DEMOSTRACIÓN. La operación de grupo en G/N es $(aN)(bN) = abN$. Debemos verificar que esta operación está bien definida; es decir, el producto en el grupo debe ser independiente de la elección de representantes para las clases laterales. Sean $aN = bN$ y $cN = dN$. Debemos mostrar que

$$(aN)(cN) = acN = bdN = (bN)(dN).$$

Entonces $a = bn_1$ y $c = dn_2$ para algún n_1 y algún n_2 en N. Luego,

$$\begin{aligned} acN &= bn_1dn_2N \\ &= bn_1dN \\ &= bn_1Nd \\ &= bNd \\ &= bdN. \end{aligned}$$

El resto del teorema es fácil: $eN = N$ es la identidad y $g^{-1}N$ es el inverso de gN. El orden de G/N es, por supuesto, el número de clases laterales de N en G. □

Es muy importante recordar que los elementos de un grupo cociente son *conjuntos de elementos* en el grupo original.

Ejemplo 10.5. Considere el subgrupo normal de S_3, $N = \{(1), (123), (132)\}$. Las clases laterales de N en S_3 son N y $(12)N$. El grupo cociente S_3/N tiene la siguiente tabla de multiplicación.

	N	$(12)N$
N	N	$(12)N$
$(12)N$	$(12)N$	N

Este grupo es isomorfo a $\mathbb{Z}_2$. Al inicio, multiplicar clases laterales puede parecer complicado y extraño; sin embargo, note que S_3/N es un grupo más pequeño. El grupo cociente entrega cierta información acerca de S_3. En realidad,

$N = A_3$, es el conjunto de permutaciones pares, y $(12)N = \{(12), (13), (23)\}$ es el conjunto de permutaciones impares. La información capturada en G/N es la paridad; es decir, multiplicar dos elementos pares o dos elementos impares resulta en una permutación par, mientra que multiplicar un elemento par con un impar resulta en una permutación impar.

Ejemplo 10.6. Considere el subgrupo normal $3\mathbb{Z}$ de $\mathbb{Z}$. Las clases laterales de $3\mathbb{Z}$ en $\mathbb{Z}$ son

$$\begin{aligned} 0 + 3\mathbb{Z} &= \{\ldots, -3, 0, 3, 6, \ldots\} \\ 1 + 3\mathbb{Z} &= \{\ldots, -2, 1, 4, 7, \ldots\} \\ 2 + 3\mathbb{Z} &= \{\ldots, -1, 2, 5, 8, \ldots\}. \end{aligned}$$

El grupo $\mathbb{Z}/3\mathbb{Z}$ está dado por la tabla de multiplicación de más abajo.

$+$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$1+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$
$2+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$

En general, el subgrupo $n\mathbb{Z}$ de $\mathbb{Z}$ es normal. Las clases laterales de $\mathbb{Z}/n\mathbb{Z}$ son

$$\begin{aligned} &n\mathbb{Z} \\ &1 + n\mathbb{Z} \\ &2 + n\mathbb{Z} \\ &\vdots \\ &(n-1) + n\mathbb{Z}. \end{aligned}$$

La suma de clases laterales $k + \mathbb{Z}$ y $l + \mathbb{Z}$ es $k + l + \mathbb{Z}$. Note que hemos escrito las clases laterales de forma aditiva, pues la operación del grupo es la adición de enteros.

Ejemplo 10.7. Considere el grupo dihedral D_n, generado por dos elementos r y s, que satisfacen las relaciones

$$\begin{aligned} r^n &= \mathrm{id} \\ s^2 &= \mathrm{id} \\ srs &= r^{-1}. \end{aligned}$$

El elemento r en realidad genera el subgrupo cíclico de las rotaciones, R_n, en D_n. Como $srs^{-1} = srs = r^{-1} \in R_n$, el grupo de rotaciones es un subgrupo normal de D_n; por lo tanto, D_n/R_n es un grupo. Como hay exactamente dos elementos en este grupo, debe ser isomorfo a $\mathbb{Z}_2$.

10.2 La Simplicidad del Grupo Alternante

De especial interés resultan ser los grupos que no tienen subgrupos normales propios no triviales. Tales grupos se llaman ***grupos simples***. Por supuesto, ya tenemos una clase completa de grupos simples, $\mathbb{Z}_p$, donde p es primo. Estos grupos son trivialmente simples pues no tienen otro subgrupo propio que no sea solamente la identidad. Otros ejemplos de grupos simpple no son tan fáciles de encontrar. Podemos, sin embargo, mostar que el grupo alternante, A_n, es simple para $n \geq 5$. La demostración de este resultado requiere de varios lemas.

Lema 10.8. *El grupo alternante A_n es generado por 3-ciclos para $n \geq 3$.*

DEMOSTRACIÓN. Para mostrar que los 3-ciclos generan A_n, solo necesitamos mostrar que cualquier par de transpociones puede ser escrito como el producto de 3-ciclos. Como $(ab) = (ba)$, todo par de transpociciones debe ser uno de los siguientes:

$$\begin{aligned}(ab)(ab) &= \mathrm{id}\\ (ab)(cd) &= (acb)(acd)\\ (ab)(ac) &= (acb).\end{aligned}$$

□

Lema 10.9. *Sea N un subgrupo normal de A_n, donde $n \geq 3$. Si N contiene un 3-ciclo, entonces $N = A_n$.*

DEMOSTRACIÓN. Demostraremos primero que A_n es generado por 3-ciclos de la forma específica (ijk), donde i y j están fijos en $\{1, 2, \ldots, n\}$ y hacemos variar k. Cada 3-ciclo es el producto de 3-ciclos de este tipo, pues

$$\begin{aligned}(iaj) &= (ija)^2\\ (iab) &= (ijb)(ija)^2\\ (jab) &= (ijb)^2(ija)\\ (abc) &= (ija)^2(ijc)(ijb)^2(ija).\end{aligned}$$

Ahora supongamos que N es un subgrupo normal no trivial de A_n para $n \geq 3$ tal que N contiene un 3-ciclo de la forma (ija). Usando la normalidad de N, vemos que

$$[(ij)(ak)](ija)^2[(ij)(ak)]^{-1} = (ijk)$$

está en N. Luego, N debe contener todos los 3-ciclos (ijk) para $1 \leq k \leq n$. Por el Lema 10.8, estos 3-ciclos generan A_n; luego, $N = A_n$. □

Lema 10.10. *Para $n \geq 5$, todo subgrupo normal no trivial N de A_n contiene un 3-ciclo.*

DEMOSTRACIÓN. Sea σ un elemento arbitrario, distinto de la identidad,en un subgrupo normal N. Existen varias posibles estructuras de ciclos para σ.

- σ es un 3-ciclo.
- σ es el producto de ciclos disjuntos, $\sigma = \tau(a_1 a_2 \cdots a_r) \in N$, con $r > 3$.
- σ es el producto de ciclos disjuntos, $\sigma = \tau(a_1 a_2 a_3)(a_4 a_5 a_6)$.
- $\sigma = \tau(a_1 a_2 a_3)$, donde τ es el producto de 2-ciclos disjuntos.
- $\sigma = \tau(a_1 a_2)(a_3 a_4)$, donde τ es el producto de un número par de 2-ciclos disjuntos.

Si σ es un 3-ciclo, entonces estamos listos. Si N contiene un producto de ciclos disjuntos, σ, y al menos uno de esos ciclos tiene largo mayor a 3, digamos $\sigma = \tau(a_1 a_2 \cdots a_r)$, entonces

$$(a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1}$$

está en N pues N es normal; luego,

$$\sigma^{-1}(a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1}$$

también está en N. Como

$$\begin{aligned}\sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} &= \sigma^{-1}(a_1a_2a_3)\sigma(a_1a_3a_2)\\ &= (a_1a_2\cdots a_r)^{-1}\tau^{-1}(a_1a_2a_3)\tau(a_1a_2\cdots a_r)(a_1a_3a_2)\\ &= (a_1a_ra_{r-1}\cdots a_2)(a_1a_2a_3)(a_1a_2\cdots a_r)(a_1a_3a_2)\\ &= (a_1a_3a_r),\end{aligned}$$

N debe contener un 3-ciclo; luego, $N = A_n$.

Ahora supongamos que N contiene un producto disjunto de la forma

$$\sigma = \tau(a_1a_2a_3)(a_4a_5a_6).$$

Entonces

$$\sigma^{-1}(a_1a_2a_4)\sigma(a_1a_2a_4)^{-1} \in N$$

pues

$$(a_1a_2a_4)\sigma(a_1a_2a_4)^{-1} \in N.$$

Así

$$\begin{aligned}\sigma^{-1}(a_1a_2a_4)\sigma(a_1a_2a_4)^{-1} &= [\tau(a_1a_2a_3)(a_4a_5a_6)]^{-1}(a_1a_2a_4)\tau(a_1a_2a_3)(a_4a_5a_6)(a_1a_2a_4)^{-1}\\ &= (a_4a_6a_5)(a_1a_3a_2)\tau^{-1}(a_1a_2a_4)\tau(a_1a_2a_3)(a_4a_5a_6)(a_1a_4a_2)\\ &= (a_4a_6a_5)(a_1a_3a_2)(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6)(a_1a_4a_2)\\ &= (a_1a_4a_2a_6a_3).\end{aligned}$$

Así N contiene un ciclo disjunto de largo mayor a 3, y podemos aplicar el caso anterior.

Supongamos que N es un producto disjunto de la forma $\sigma = \tau(a_1a_2a_3)$, donde τ es el producto disjunto de 2-ciclos. Como $\sigma \in N$, $\sigma^2 \in N$, y

$$\begin{aligned}\sigma^2 &= \tau(a_1a_2a_3)\tau(a_1a_2a_3)\\ &= (a_1a_3a_2).\end{aligned}$$

Así N contiene un 3-ciclo.

El único caso que nos queda es un producto disjunto de la forma

$$\sigma = \tau(a_1a_2)(a_3a_4),$$

donde τ es el producto de un número par de 2-ciclos disjuntos. Pero

$$\sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1}$$

está en N pues $(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1}$ está en N; de manera que

$$\begin{aligned}\sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} &= \tau^{-1}(a_1a_2)(a_3a_4)(a_1a_2a_3)\tau(a_1a_2)(a_3a_4)(a_1a_2a_3)^{-1}\\ &= (a_1a_3)(a_2a_4).\end{aligned}$$

Como $n \geq 5$, podemos encontrar $b \in \{1, 2, \ldots, n\}$ de manera que $b \neq a_1, a_2, a_3, a_4$. Sea $\mu = (a_1a_3b)$. Entonces

$$\mu^{-1}(a_1a_3)(a_2a_4)\mu(a_1a_3)(a_2a_4) \in N$$

y

$$\begin{aligned}\mu^{-1}(a_1a_3)(a_2a_4)\mu(a_1a_3)(a_2a_4) &= (a_1ba_3)(a_1a_3)(a_2a_4)(a_1a_3b)(a_1a_3)(a_2a_4)\\ &= (a_1a_3b).\end{aligned}$$

Por lo tanto, N contiene un 3-ciclo. Esto completa la demostración del lema. □

Teorema 10.11. *El grupo alternante, A_n, es simple para $n \geq 5$.*

DEMOSTRACIÓN. Sea N un subgrupo normal no trivial de A_n. Por el Lema 10.10, N contiene un 3-ciclo. Por el Lema 10.9, $N = A_n$; por lo tanto, A_n no contiene ningún subgrupo normal que sea propio y no trivial para $n \geq 5$. □

Sage Sage puede determinar fácilmente si un subgrupo es normal o no. Si lo es, puede crear el grupo cociente. Pero la construcción entrega un nuevo grupo de permutaciones, ismomorfo al grupo cociente, de manera que su utilidad es limitada.

Nota Histórica

Uno de los principales problemas de la teoría de grupos finitos ha sido el de clasificar todos los grupos finitos simples. Este problema tiene más de un siglo y recién fue resuelto en las últimas décadas del siglo XX. En cierto sentido, los grupos finitos simples son los bloques para construir todos los grupos finitos. Los primeros grupos simples no abelianos en ser descubiertos fueron los grupos alternantes. Galois fue el primero en demostrar que A_5 era simple. Más tarde, matemáticos tales como C. Jordan y L. E. Dickson encontraron varias familias infinitas de grupos de matrices que eran simples. Otras familias de grupos simples fueron descubiertas en la década de 1950. Alrededor del 1900, William Burnside conjecturó que todos los grupos simples no abelianos debían tener orden par. En 1963, W. Feit y J. Thompson demostraron la conjetura de Burnside y publicaron sus resultados en el trabajo "Solvability of Groups of Odd Order," que apareció en el *Pacific Journal of Mathematics*. Su demostración, de unas 250 páginas, dio impulso a un programa en los 1960s y los 1970s para clasificar todos los grupos finitos simples. Daniel Gorenstein fue el organizador de este notable esfuerzo. Uno de los últimos grupos simples fue el "Monster," descubierto por R. Greiss. El Monster, un grupo de matrices de 196,833×196,833, es uno de los 26 grupos simples esporádicos, o especiales. Estos grupos simples esporádicos son grupos que no calzan en ninguna familia infinita de grupos simples. Algunos de los grupos esporádicos juegan un rol importante en la física.

10.3 Ejercicios

1. Para cada uno de los siguientes grupos G, determine si es que H es un subgrupo normal de G. Si H es un subgrupo normal, escriba una tabla de Cayley para el grupo cociente G/H.

(a) $G = S_4$ and $H = A_4$

(b) $G = A_5$ and $H = \{(1), (123), (132)\}$

(c) $G = S_4$ and $H = D_4$

(d) $G = Q_8$ and $H = \{1, -1, I, -I\}$

(e) $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$

2. Encuentre todos los subgrupos de D_4. ¿Cuáles subgrupos son normales? ¿Cuáles son todos los grupos cociente de D_4 salvo isomorfismo?

3. Encuentre todos los subgrupos de the quaternion group, Q_8. ¿Cuáles subgrupos son normales? ¿Cuáles son todos los grupos cociente de Q_8 salvo isomorfismo?

4. Sea T el grupo de matrices triangulares superiores no singulares de 2×2 con coeficientes en $\mathbb{R}$; es decir, matrices de la forma

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix},$$

donde a, b, $c \in \mathbb{R}$ y $ac \neq 0$. Sea U el conjunto de matrices de la forma

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

donde $x \in \mathbb{R}$.

(a) Muestre que U es un subgrupo de T.

(b) Demuestre que U es abeliano.

(c) Demuestre que U es normal en T.

(d) Muestre que T/U es abeliano.

(e) ¿Es T normal en $GL_2(\mathbb{R})$?

5. Muestre que la intersección de dos subgrupos normales es un subgrupo normal.

6. Si G es abeliano, demuestre que G/H también es abeliano.

7. Demuestre o refute: Si H es un subgrupo normal de G tal que H y G/H son abelianos, entonces G es abeliano.

8. Si G es cíclico, demuestre que G/H también es cíclico.

9. Demuestre o refute: Si H y G/H son cíclicos, entonces G es cíclico.

10. Sea H un subgrupo de índice 2 de un grupo G. Demuestre que H es normal en G. Concluya que S_n no es simple para $n \geq 3$.

11. Si un grupo G tiene exactemente un subgrupo H de orden k, demuestre que H es normal en G.

12. Defina el ***centralizador*** de un elemento g en un grupo G como el conjunto

$$C(g) = \{x \in G : xg = gx\}.$$

Muestre que $C(g)$ es un subgrupo de G. Si g genera un subgrupo normal de G, demuestre que $C(g)$ es normal en G.

13. Recuerde que el ***centro*** de un grupo G es el conjunto

$$Z(G) = \{x \in G : xg = gx \text{ para todo } g \in G\}.$$

(a) Calcule el centro de S_3.

(b) Calcule el centro de $GL_2(\mathbb{R})$.

(c) Muestre que el centro de cualquier grupo G es un subgrupo normal de G.

(d) Si $G/Z(G)$ es cíclico, demuestre que G es abeliano.

14. Sea G un grupo y sea $G' = \langle aba^{-1}b^{-1} \rangle$; es decir, G' es el subgrupo de todos los productos finitos de elementos en G de la forma $aba^{-1}b^{-1}$. El subgrupo G' se llama ***subgrupo conmutador*** de G.

(a) Muestre que G' es un subgrupo normal de G.

(b) Sea N un subgrupo normal de G. Demuestre que G/N es abeliano si y solo si N contiene al subgrupo conmutador de G.

10.4 Sage

Sage tiene varias funciones convenientes que nos permitirán investigar rápidamente si un subgrupo es normal, y de ser así, la naturaleza del grupo cociente resultante. Pero para una comprensión inicial, también podemos trabajr directamente con las clases laterales. Ensuciémosnos las manos primero, después aprenderemos sobre la forma fácil.

Multiplicando Clases Laterales

La definición de grupo cociente requiere de un subgrupo normal, y entonces *definimos* una forma de "multiplicar" dos clases laterales del subgrupo para obtener otra clase lateral. Es importante darse cuenta que podemos interpretas la definición de subgrupos normal como la condición *exacta* que necesitamos para que nuestro nuevo producto nos resulte. Haremos dos ejemplos — primero con un subgrupo normal, luego con un subgrupo que no lo es.

Considere el grupo dihedral D_8 que es el grupo de simetrías de un octógono. Si tomamos el elemento que corresponde a un cuarto de vuelta, podemos usarlo para generar un subgrupo de orden 4. Este será un subgrupo normal (confíe por ahora respecto a esto). Primero, construya las clases laterales derechas (note que no se produce una respuesta):

```
G = DihedralGroup(8)
quarter_turn = G('(1,3,5,7)(2,4,6,8)')
S = G.subgroup([quarter_turn])
C = G.cosets(S)
```

Así `C` es una lista de listas, donde cada elemento del grupo `G` exactamente una vez en alguna parte. Podría pedirle a Sage que le muestre `C` si lo desea, pero acá trataremos de evitarlo. Queremos multiplicar dos clases (listas). ¿Cómo hacemos esto? Tomemos *cualquier* elemento de la primera lista, y *cualquier* elemento de la segunda lista y multipliquémoslos (lo que sabemos hacer pues son elementos de `G`). Ahora tenemos un elemento de `G`. ¿Qué hacemos con este elemento, si lo que realmente queremos obtener como resultado del producto de dos clases es otra clase? Simple — averigüamos a qué clase pertenece el producto. Veamos que pasa. Multiplicaremos la clase 1 con la clase 3 (hay 4 clases por el Teorema de Lagrange). Estudie cuidadosamente las siguientes líneas de código para ver si puede entender qué es lo que está haciendo, y *después* lea la explicación que sigue.

```
p = C[1][0]*C[3][0]
[i for i in srange(len(C)) if p in C[i]]
```

```
[2]
```

¿Qué hemos logrado? En la primera línea creamos `p` como el producto de dos elementos del grupo, uno de la clase 1 y uno de la clase 3 (`C[1]`, `C[3]`). Como podemos elegir *cualquier* elemento de cada clase, elegimos el primer elemento de cada una (`C[ ][0]`). Después recorremos la lista completa de clases, seleccionando solo aquellas clases que contengan `p`. Como `p` solo estará en una clase, esperamos obtener una lista con un solo elemento. En este caso, nuestra lista contiene solo el `2`. Decimos entonces que el producto de la clase 1 con la clase 3 es la clase 2.

La idea acá es que este resultado (clase 1 por clase 3 es clase 2) debiera ser siempre el mismo, *sin importar qué elementos escojamos de cada clase para formar el producto* `p`. Hagámoslo nuevamente, pero ahora no elegiremos el

primer elemento de cada clase, sino el tercero de la clase 1 y el segundo de la clase 3 (recuerde, contamos desde cero!).

```
p = C[1][2]*C[3][1]
[i for i in srange(len(C)) if p in C[i]]
```

```
[2]
```

Bien. Tenemos el mismo resultado. Si aún nos cree que `S` es un subgrupo normal de `G`, entonces este es el resultado que predice la teoría. Haga una copia de la celda de arriba y pruebe otras elecciones de representantes para cada clase. Pruebe también el producto de otras clases, con diversos representantes.Ahora es un buen momento para introducir una forma de extender Sage agrgándo nuevas funciones. Diseñaremos una función de multiplicación de clases laterales. Lea cuidadosamente lo que sigue y después vea la explicación que sigue.

```
def coset_product(i, j, C):
   p = C[i][0]*C[j][0]
   c = [k for k in srange(len(C)) if p in C[k]]
   return c[0]
```

La primera línea crea una nueva función en Sage llamada `coset_product`. Esto se logra con la palabra `def`, y note los dos puntos al final de la linea. Los parámetros para la función son los números de las clases que queremos multiplicar y la lista completa de clases laterales. Las dos líneas del medio debiesen vers familiares. Sabemos que `c` es una lista con un elemento, de manera que `c[0]` extraerá ese número de clase, y `return` es lo que determina que esta es la respuesta producida por la función. Note que la indentación debe ser exactamente como se muestra. Podríamos haber escrito todos estos cálculos en un sola línea, sin definir una nueva función, pero eso empieza a ser engorroso. Es necesario ejecutar el bloque de código de arriba para *definir* realmente la función, y no habrá salida si tiene éxito. Ahora podemos usar nuestra nueva función para repetir el trabajo de arriba:

```
coset_product(1, 3, C)
```

```
2
```

Ahora conoce lo básico sobre cómo agregar funcionalidad a Sage y hacer mucho más de lo que está diseñado para hacer. Con algo de práctico, incluso podría sugerir y contribuir nuevas funciones a Sage, pues es un proyecto de fuente abierta. Bien.

Ahora examinemos una situación en que el subgrupo no es normal. Veremos que nuestra definición de ptoducto de clases es insuficiente en este caso. Además nos daremos cuenta que nuestra nueva función `coset_product` también es inútil pues presupone que las clases laterales proviene de un subgrupo normal.

Considere el grupo alternante A_4 que podemos interpretar como el grupo de simetrías de un tetrahedro. Para un subgrupo, escoja un elemento que fija un vértice y rota la cara opuesta — esto generará un subgrupo cíclico de orden 3, y por el Teorema de Lagrange obtendremos cuatro clases laterales. Las calcularemos acá. (Nuevamente, no se pide ningna salida.)

```
G = AlternatingGroup(4)
face_turn = G("(1,2,3)")
S = G.subgroup([face_turn])
C = G.cosets(S)
```

Nuevamente, consideremos el producto de la clase 1 con la clase 3:

```
p = C[1][0]*C[3][0]
[i for i in srange(len(C)) if p in C[i]]
```

```
[0]
```

Nuevamente, pero ahora para la clase 3, escoja el segunso elemento de la clase para obtener el producto `p`:

```
p = C[1][0]*C[3][1]
[i for i in srange(len(C)) if p in C[i]]
```

```
[2]
```

¿Entonces, el producto de la clase 1 y la clase 3 es igual a la clase 0 o a la clase 2? No lo podemos determinar! Así es que no hay *ninguna forma* de construir un grupo cociente para este subgrupo. Usted puede esperimentar más con este subgrupo, pero en algún sentido, no tenemos nada más que hacer con este ejemplo — no queda nada que decir.

Métodos de Sage para Subgrupos Normales

Puede fácilmente preguntarle a Sage si un subgrupo es normal o no. Esto se considera una propiedad del subgrupo, pero le debe decir a Sage cuál es el "supergrupo", pues la respuesta puede cambiar según cuál sea. (Por ejemplo `H.is_normal(H)` siempre resulta `True`.) Acá están nuestros dos ejemplos de arriba.

```
G = DihedralGroup(8)
quarter_turn = G('(1,3,5,7)(2,4,6,8)')
S = G.subgroup([quarter_turn])
S.is_normal(G)
```

```
True
```

```
G = AlternatingGroup(4)
face_turn = G("(1,2,3)")
S = G.subgroup([face_turn])
S.is_normal(G)
```

```
False
```

El texto demuestra en la Sección 10.2 que A_5 es simple, i.e. A_5 no tiene subgrupos normales. Podríamos construir cada subgrupo de A_5 y preguntar si es normal en A_5 usando el método `.is_normal()`. Pero Sage ya tiene esto cubierto para nosotros.

```
G = AlternatingGroup(5)
G.is_simple()
```

```
True
```

Cuando tenemos un subgrupo normal, podemos también construir el grupo cociente.

```
G = DihedralGroup(8)
quarter_turn = G('(1,3,5,7)(2,4,6,8)')
S = G.subgroup([quarter_turn])
Q = G.quotient(S)
Q
```

```
Permutation Group with generators [(1,2)(3,4), (1,3)(2,4)]
```

Esto es útil, pero un poco desconcertante. Tenemos el grupo cociente, pero cualquier noción de clases laterales se perdió, pues `Q` es entregado como un nuevo grupo de permutaciones en un conjunto diferente de símbolos. No podemos presuponer que los número usados para el nuevo grupo de permutaciones `Q` tengan similitud alguna con las clases que obtenemos del método `.cosets()`. Pero podemos ver que el grupo cociente se describe como un grupo generado por dos elementos de orden dos. Podríamos pedir el orden del grupo, o usar el Teorema de Lagrange para saber que el orden es 4. Podemos decir ahora que hay solo dos grupos de orden 4, el grupo cíclico de order 4 y un grupo no cíclico de orden 4 que conocemos como el 4-grupo de Klein o como $\mathbb{Z}_2 \times \mathbb{Z}_2$. Este grupo cociente se ve como el grupo no cíclcio pues el grupo cíclio tiene solo un elemento de orden 2. Veamos que nos dice Sage.

```
Q.is_isomorphic(KleinFourGroup())
```

```
True
```

Si, esos es.

Finalmente, Sage nos puede hacer una lista de todos los subgrupos normales de un grupo. La lista de los grupos en sí, como hemos visto antes, puede ser una cantidad de información apabullante. A continuación simplemente listaremos los órdenes de lso subgrupos normales producidos.

```
G = DihedralGroup(8)
N = G.normal_subgroups()
[H.order() for H in N]
```

```
[1, 2, 4, 8, 8, 8, 16]
```

En particular, vemos que nuestro subgrupo de "cuarto de vuelta" es el *único* subgrupo normal de orden 4 en este grupo.

10.5 Ejercicios en Sage

1. Construya todos los subgrupos del grupo alternante en 5 símbolos, A_5, y verifique que, salvo los casos triviales, ninguno es normal. Este comando podría demorar un par de segundos en correr. Compare esto con el tiempo necesario para correr el método `.is_simple()` y constate que hay una buena dosis de teoría y astucia involucradas en acelerar comandos como este. (Es posible que su instalación de Sage no tenga la librería "Table of Marks" de GAP y sea imposible calcular la lista de subgrupos.)

2. Considere el grupo cociente del grupo de simetrías de un octógono regular, por el subgrupo cíclico de orden 4 generado por una rotación en un cuarto de vuelta. Use la función `coset_product` para determinar la tabla de Cayley para este grupo cociente. Use los números de cada clase lateral, resultantes del método `.cosets()` como nombres para los elementos del grupo cociente. Necesitará construir la tabla "a mano" pues no hay una forma fácil de lograr que los comandos de Sage hagan esto. Puede construir una tabla en el editor del notebook Sage Notebook (shift-click en una línea azul) o puede leer la documentación del método `html.table()`.

3. Considere el subgrupo cíclico de orden 4 en las simetrías de un octógono 8-gon. Verifique que el subgrupo es normal construyendo primero las clases

laterales izquierdas y derechas (sin usar el método `.cosets()`) y luego verificando su igualdad en Sage, todo con una línea de comando que use el comando `sorted()`.

4. Nuevamente, use el mismo subgrupo cíclico de orden 4 en el grupo de simetrías de un octógono. Verifique que el subgrupo es normal usando la parte (2) del Teorema 10.3. Construya un comando de una línea que haga la verificación completa y entregue `True`. Quizás deba ordenar los elementos del subgrupo `S` primero, luego paso a paso ir construyendo las listas, comandos, y condiciones necesarios. Note que esta verificación no requiere la construcción de las clases laterales en ningún momento.

5. Repita la demostración de la subsección anterior de que para las simetrías de un tetrahedro, un subgrupo cíclico de orden 3 resulta en una multiplicación mal definida de clases laterales. Arriba, por defecto el método `.cosets()` entrega las clases laterales derechas — pero en este problema, trabaje con las clases izquierdas. Debe escoger dos clases para multiplicarlas, y comprobar que elecciones diferentes de representantes llevan a resultados diferentes para el producto de las clases.

6. Construya algunos grupos dihedrales de orden $2n$ (i.e. simetrías de un n-ágono, D_n en el texto, `DihedralGroup(n)` en Sage). Podrían ser todos ellos para $3 \leq n \leq 100$. Para cada grupo dihedral, construya una llista de los órdenes de cada uno de los subgrupos normales (use `.normal_subgroups()`). Puede que demore en terminar de calcular - sea paciente. Observe suficiente ejemplos para conjeturar un patrón, verifique su hipótesis con cada uno de sus ejemplos y luego enúnciela claramente.
¿Puede predecir cuántos subgrupos normales que tiene el grupo dihedral D_{470448} sin usar Sage para obtener todos los subgrupos normales? ¿Puede *describir* todos los asubgrupos normales que tiene el grupo dihedral D_{470448} sin usar Sage?

11

Homomorfismos

Una de las ideas clásicas del álgebra es el concepto de homomorfismo, una generalización natural de isomorfismo. Si relajamos el requerimiento de que un isomorfismo sea biyectivo, obtenemos un homomorfismo.

11.1 Homomofismos de Grupos

Un ***homomorfismo*** entre los grupos $(G, \cdot)$ y $(H, \circ)$ es una función $\phi : G \to H$ tal que

$$\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2)$$

$g_1, g_2 \in G$. La imagen de ϕ en H se llama ***imagen homomorfa*** de ϕ.

Dos están relacionados de la forma más fuerte posible si son isomorfos; sin embargo nua relación más débil puede también existir entre dos grupos. Por ejemplo, el grupo simétrico S_n y el grupo $\mathbb{Z}_2$ están relacionados por el hecho de que S_n puede ser dividido en permutaciones pares e impares que exhiben una estructura de grupos similar a la de $\mathbb{Z}_2$, como se muestra en la siguiente tabla de multiplicación.

	even	odd
even	even	odd
odd	odd	even

Podemos usar homomorfismos para estudiar relaciones como la que acabamos de describir.

Ejemplo 11.1. Sea G un grupo y $g \in G$. Defina una función $\phi : \mathbb{Z} \to G$ by $\phi(n) = g^n$. Entonces ϕ es un homomorfismo de grupos, pues

$$\phi(m + n) = g^{m+n} = g^m g^n = \phi(m)\phi(n).$$

Este homomorfismo envía a $\mathbb{Z}$ sobre el subgrupo cíclico de G generado por g.

Ejemplo 11.2. Let $G = GL_2(\mathbb{R})$. If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

está en G, pues el determinante es distinto de cero; es decir, $\det(A) = ad - bc \neq 0$. Además, para dos elementos A y B en G, $\det(AB) = \det(A)\det(B)$. Usando el determinante, podemos definir un homomorfismo $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ por $A \mapsto \det(A)$.

Ejemplo 11.3. Recuerde que el grupo de la circunferencia $\mathbb{T}$ consiste de todos los números complejos z tales que $|z| = 1$. Podemos definir un homomorfismo ϕ del grupo aditivo de los números reales $\mathbb{R}$ a $\mathbb{T}$ por $\phi : \theta \mapsto \cos\theta + i\sin\theta$. De hecho,

$$\begin{aligned}\phi(\alpha+\beta) &= \cos(\alpha+\beta) + i\sin(\alpha+\beta)\\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta)\\ &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta)\\ &= \phi(\alpha)\phi(\beta).\end{aligned}$$

Geométricamente, simplemente estamos enrrollando la recta real sobre la circunferencia de forma grupística.

La siguiente proposición lista algunas propiedades básica de los homomorfismos de grupos.

Proposición 11.4. *Sea $\phi : G_1 \to G_2$ un homomorfismo de grupos. Entonces*

1. *Si e es la identidad de G_1, entonces $\phi(e)$ es la identidad de G_2;*
2. *Para cualquier elemento $g \in G_1$, $\phi(g^{-1}) = [\phi(g)]^{-1}$;*
3. *Si H_1 es un subgrupo de G_1, entonces $\phi(H_1)$ es un subgrupo de G_2;*
4. *Si H_2 es un subgrupo de G_2, entonces $\phi^{-1}(H_2) = \{g \in G_1 : \phi(g) \in H_2\}$ es un subgrupo de G_1. Más aún, si H_2 es normal en G_2, entonces $\phi^{-1}(H_2)$ es normal en G_1.*

Demostración. (1) Supongamos que e y e' son las identidades de G_1 y G_2, respectivamente; entonces

$$e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e).$$

Por cancelación, $\phi(e) = e'$.

(2) Es consecuencia del hecho que

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e) = e'.$$

(3) El conjunto $\phi(H_1)$ es no vacío pues la identidad de G_2 está en $\phi(H_1)$. Supongamos que H_1 es un subgrupo de G_1 y sean x e y en $\phi(H_1)$. Existen elementos $a, b \in H_1$ tales que $\phi(a) = x$ y $\phi(b) = y$. Como

$$xy^{-1} = \phi(a)[\phi(b)]^{-1} = \phi(ab^{-1}) \in \phi(H_1),$$

$\phi(H_1)$ es un subgrupo de G_2 por la Proposición 3.31.

(4) Sea H_2 un subgrupo de G_2 y defina H_1 como $\phi^{-1}(H_2)$; es decir, H_1 es el conjunto de todos los $g \in G_1$ tales que $\phi(g) \in H_2$. La identidad está en H_1 pues $\phi(e) = e'$. Si a y b están en H_1, entonces $\phi(ab^{-1}) = \phi(a)[\phi(b)]^{-1}$ está en H_2 pues H_2 es un subgrupo de G_2. Por lo tanto, $ab^{-1} \in H_1$ y H_1 es un subgrupo de G_1. Si H_2 es normal en G_2, debemos probar que $g^{-1}hg \in H_1$ para $h \in H_1$ y $g \in G_1$. Pero

$$\phi(g^{-1}hg) = [\phi(g)]^{-1}\phi(h)\phi(g) \in H_2,$$

pues H_2 es un subgrupo normal de G_2. Por lo tanto, $g^{-1}hg \in H_1$. □

Sea $\phi : G \to H$ un homomorfismo de grupos y supongamos que e es la identidad de H. Por la Proposición 11.4, $\phi^{-1}(\{e\})$ es un subgrupo de G. Este subgrupo se llama ***núcleo*** de ϕ y se denotará por $\ker \phi$. De hecho, este subgrupo es un subgrupo normal de G pues el subgrupo trivial es normal en H. Enunciamos este resultado en el siguiente teorema, que dice que a cada homomorfismo de grupos podemos asociar de forma natural un subgrupo normal.

Teorema 11.5. *Sea $\phi : G \to H$ un homomorfismo de grupos. Entonces el núcleo de ϕ es un subgrupo normal de G.*

Ejemplo 11.6. Examinemos el homorfismo $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ definido por $A \mapsto \det(A)$. Como 1 es la identidad de $\mathbb{R}^*$, el núcleo de este homomorfismo consiste de toda las matrices de 2×2 que tienen determinante uno. Es decir, $\ker \phi = SL_2(\mathbb{R})$.

Ejemplo 11.7. El núcleo del homomorfismo de grupos $\phi : \mathbb{R} \to \mathbb{C}^*$ definido por $\phi(\theta) = \cos\theta + i \sin\theta$ es $\{2\pi n : n \in \mathbb{Z}\}$. Note que $\ker \phi \cong \mathbb{Z}$.

Ejemplo 11.8. Supongamos que queremos determiar todos los posibles homomorfismos ϕ de $\mathbb{Z}_7$ a $\mathbb{Z}_{12}$. Como el núcleo de ϕ debe ser un subgrupo de $\mathbb{Z}_7$, solo hay dos núcleos posibles, $\{0\}$ y todo $\mathbb{Z}_7$. La imagen de un subgrupo de $\mathbb{Z}_7$ debe ser un subgrupo de $\mathbb{Z}_{12}$. Luego, no hay homomorfismos inyectivos; de lo contrario, $\mathbb{Z}_{12}$ tendría un subgrupo de orden 7, lo que es imposible. POr lo tanto, el único homomorfismo posible de $\mathbb{Z}_7$ a $\mathbb{Z}_{12}$ es el que envía todos los elementos cero.

Ejemplo 11.9. Sea G un grupo. Supongamos que $g \in G$ y ϕ es el homomorfismo de $\mathbb{Z}$ a G dado por $\phi(n) = g^n$. Si el orden de g es infinito, entonces el núcleo de este homomorfismo es $\{0\}$ como ϕ envía $\mathbb{Z}$ sobre el subgrupo cíclico de G generado por g. Si en cambio, el orden de g es finito, digamos n, entonces el núcleo de ϕ es $n\mathbb{Z}$.

11.2 Los Teoremas de Isomorfía

Si bien no es evidente al comienzo, los grupos cociente corresponden exactamente con las imágenes homomorfas, y podemos usar grupos cociente para estudiar homomorfismos. Ya sabemos que con cada homomorfismo de grupos $\phi : G \to H$ podemos asociar un subgrupo normal de G, $\ker \phi$. El recíproco también es cierto; es decir, todo subgrupo normal de un grupo G da lugar a un homomorfismo de grupos.

Sea H un subgrupo normal de G. Defina el ***homorfismo natural*** o ***homomorfismo canónico***

$$\phi : G \to G/H$$

por

$$\phi(g) = gH.$$

Este de hecho es un homomorfismo, pues

$$\phi(g_1 g_2) = g_1 g_2 H = g_1 H g_2 H = \phi(g_1)\phi(g_2).$$

El núcleo de este homomorfismo es H. Los siguientes teoremas describen la relación enter homomorfismos de grupos, subgrupos normales, y grupos cociente.

Teorema 11.10 (Primer Teorema de Isomorfía)**.** *Si $\psi : G \to H$ es un homomorfismo de grupos con $K = \ker\psi$, entonces K es normal en G. Sea $\phi : G \to G/K$ el homomorfismo canónico. Entonce eciste un único isomorfismo $\eta : G/K \to \psi(G)$ tal que $\psi = \eta\phi$.*

DEMOSTRACIÓN. Ya vimos que K es normal en G. Defina $\eta : G/K \to \psi(G)$ por $\eta(gK) = \psi(g)$. Primero demostraremos que η es una función bien definida. Si $g_1K = g_2K$, entonces existe $k \in K$, tal que $g_1k = g_2$; por lo tanto,

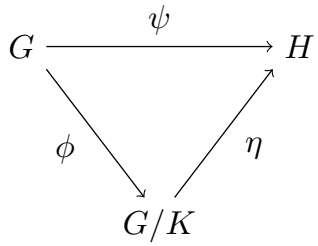
$$\eta(g_1K) = \psi(g_1) = \psi(g_1)\psi(k) = \psi(g_1k) = \psi(g_2) = \eta(g_2K).$$

Luego, η no depende de la elección de representante de la clase lateral y la función $\eta : G/K \to \psi(G)$ está únicamente definida pues $\psi = \eta\phi$. Debemos mostrar además que η es un homomorfismo, pero

$$\begin{aligned}\eta(g_1Kg_2K) &= \eta(g_1g_2K)\\ &= \psi(g_1g_2)\\ &= \psi(g_1)\psi(g_2)\\ &= \eta(g_1K)\eta(g_2K).\end{aligned}$$

Claramente, η es sobre $\psi(G)$. Para mostrar que η es 1-1, supongamos que $\eta(g_1K) = \eta(g_2K)$. Entonces $\psi(g_1) = \psi(g_2)$. Esto implica que $\psi(g_1^{-1}g_2) = e$, o $g_1^{-1}g_2$ está en el núcleo de ψ; luego, $g_1^{-1}g_2K = K$; es decir, $g_1K = g_2K$. □

Los matemáticos a menudo usan diagramas llamados ***diagramas conmutativos*** par describir teoremas como este. El siguiente diagrama "conmuta" pues $\psi = \eta\phi$.



Ejemplo 11.11. Sea G un grupo cíclico con generador g. Defina una función $\phi : \mathbb{Z} \to G$ por $n \mapsto g^n$. Esta función es un homomorfismo epiyectivo pues

$$\phi(m+n) = g^{m+n} = g^mg^n = \phi(m)\phi(n).$$

Claramente ϕ es sobre. Si $|g| = m$, entonces $g^m = e$. Luego, $\ker\phi = m\mathbb{Z}$ y $\mathbb{Z}/\ker\phi = \mathbb{Z}/m\mathbb{Z} \cong G$. Por otra parte, si el orden de g es infinito, entonces $\ker\phi = 0$ y ϕ es un isomorfismo de G y $\mathbb{Z}$. Luego, dos grupos cíclicos son isomorfos exactamente cunado tienen el mismo orden. Salvo isomorfismo, los únicos grupos cíclicos son $\mathbb{Z}$ y $\mathbb{Z}_n$.

Teorema 11.12 (Segundo Teorema de Isomorfía)**.** *Sea H un subgrupo G (no necesarimente normal en G) y N un subgrupo normal de G. Entonces HN es un subgrupo de G, $H \cap N$ es un subgrupo normal de H, y*

$$H/H \cap N \cong HN/N.$$

DEMOSTRACIÓN. Demostraremos primero que $HN = \{hn : h \in H, n \in N\}$ es un subgrupo de G. Supongamos que $h_1n_1, h_2n_2 \in HN$. Como N is normal, $(h_2)^{-1}n_1h_2 \in N$. Así

$$(h_1n_1)(h_2n_2) = h_1h_2((h_2)^{-1}n_1h_2)n_2$$

está en HN. El inverso de $hn \in HN$ está en HN pues

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1}).$$

A continuación, demostraremos que $H \cap N$ es normal en H. Sea $h \in H$ y $n \in H \cap N$. Entonces $h^{-1}nh \in H$ pues cada elemento está en H. Además, $h^{-1}nh \in N$ pues N es normal en G; por lo tanto, $h^{-1}nh \in H \cap N$.

Ahora defina una función ϕ de H a HN/N por $h \mapsto hN$. La función ϕ es sobre, pues cualquier clase lateral $hnN = hN$ es la imagen de h en H. También sabemos que ϕ es un homomorfismo pues

$$\phi(hh') = hh'N = hNh'N = \phi(h)\phi(h').$$

Por el Primer Teorema de Isomorfía, la imagen de ϕ es isomorfa a $H/\ker\phi$; es decir,

$$HN/N = \phi(H) \cong H/\ker\phi.$$

Como

$$\ker\phi = \{h \in H : h \in N\} = H \cap N,$$

$HN/N = \phi(H) \cong H/H \cap N$. □

Teorema 11.13 (Teorema de Correspondencia)**.** *Sea N un subgrupo normal de un grupo G. Entonces $H \mapsto H/N$ es una correspondencia 1-1 entre el conjunto de subgrupos H que contienen a N y el conjunto de subgrupos de G/N. Más aún, los subgrupos normales de G que contienen a N corresponden a los subgrupos normales de G/N.*

Demostración. Sea H un subgrupo de G que contiene a N. Como N es normal en H, H/N tiene sentido. Sean aN y bN elementos de H/N. Entonces $(aN)(b^{-1}N) = ab^{-1}N \in H/N$; luego, H/N es un subgrupo de G/N.

Sea S un subgrupo debe G/N. Este subgrupo es un conjunto de clases laterales de N. Si $H = \{g \in G : gN \in S\}$, entonces para $h_1, h_2 \in H$, tenemos que $(h_1N)(h_2N) = h_1h_2N \in S$ y $h_1^{-1}N \in S$. Por lo tanto, H debe ser un subgrupo de G. Claramente, H contiene a N. Por lo tanto, $S = H/N$. Concluimos que, la función $H \mapsto H/N$ es sobreyectiva.

Supongamos que H_1 y H_2 son subgrupos de G que contienen a N tales que $H_1/N = H_2/N$. Si $h_1 \in H_1$, entonces $h_1N \in H_1/N$. Luego, $h_1N = h_2N \subset H_2$ para algún h_2 en H_2. Pero, como N está contenido en H_2, sabemos que $h_1 \in H_2$ o $H_1 \subset H_2$. Similarmente, $H_2 \subset H_1$. Como $H_1 = H_2$, la función $H \mapsto H/N$ es 1-1.

Supongamos que H es normal en G y que N es un subgrupo de H. Entonces es fácil verificar que la función $G/N \to G/H$ definida por $gN \mapsto gH$ es un homomorfismo. El núncleo de este homomorfismo es H/N, lo que demuestra que H/N es normal en G/N.

Recíprocamente, supongamos que H/N es normal en G/N. El homomorfismo dado por

$$G \to G/N \to \frac{G/N}{H/N}$$

tiene núcleo H. Luego, H es normal en G. □

Note que en la demostración del Teorema 11.13, también hemos demostrado el siguiente teorema.

Teorema 11.14 (Tercer Teorema de Isomorfía)**.** *Sea G un grupo y sean N y H subgrupos normales de G con $N \subset H$. Entonces*

$$G/H \cong \frac{G/N}{H/N}.$$

Ejemplo 11.15. Por el Tercer Teorema de Isomorfía,

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}).$$

Como $|\mathbb{Z}/mn\mathbb{Z}| = mn$ y $|\mathbb{Z}/m\mathbb{Z}| = m$, tenemos $|m\mathbb{Z}/mn\mathbb{Z}| = n$.

Sage Sage puede crear homomorfismos entre grupos, los que pueden ser usados directamente como funciones, y cuya imagen y núcleo pueden ser consultados. Hay así gran potencial para explorar las muchas relaciones fundamentales entre grupos, subgrupos normales, grupos cociente y propiedades de homomorfismos.

11.3 Ejercicios

1. Demuestre que $\det(AB) = \det(A)\det(B)$ para $A, B \in GL_2(\mathbb{R})$. Esto muestra que el determinante es un homomorfismo de $GL_2(\mathbb{R})$ a $\mathbb{R}^*$.

2. ¿Cuál de las siguientes funciones son homomorfismos? Si la función es un homomorfismo, cuál es el núcleo?

(a) $\phi : \mathbb{R}^* \to GL_2(\mathbb{R})$ definida como

$$\phi(a) = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$$

(b) $\phi : \mathbb{R} \to GL_2(\mathbb{R})$ definida como

$$\phi(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

(c) $\phi : GL_2(\mathbb{R}) \to \mathbb{R}$ definida como

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a + d$$

(d) $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ definida como

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ad - bc$$

(e) $\phi : \mathbb{M}_2(\mathbb{R}) \to \mathbb{R}$ definida como

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = b,$$

donde $\mathbb{M}_2(\mathbb{R})$ es el grupo aditivo de las matrices de 2×2 con coeficientes en $\mathbb{R}$.

3. Sea A una matriz de $m \times n$. Muestre que la multiplicación de matrices, $x \mapsto Ax$, define un homomorfismo $\phi : \mathbb{R}^n \to \mathbb{R}^m$.

4. Sea $\phi : \mathbb{Z} \to \mathbb{Z}$ dada por $\phi(n) = 7n$. Demuestre que ϕ es un homomorfismo de grupos. Encuentre el núcleo y la imagen de ϕ.

5. Describa todos los homomorfismos de $\mathbb{Z}_{24}$ a $\mathbb{Z}_{18}$.

6. Describa todos los homomorfismos de $\mathbb{Z}$ a $\mathbb{Z}_{12}$.

7. En el grupo $\mathbb{Z}_{24}$, sean $H = \langle 4 \rangle$ y $N = \langle 6 \rangle$.

(a) Liste los elementos en HN (usualmente escribimos $H + N$ para estos grupos aditivos) y $H \cap N$.

(b) Liste las clases laterales en HN/N, mostrando los elementos en cada una de ellas.

(c) Liste las clases laterales en $H/(H \cap N)$, mostrando los elementos en cada una de ellas.

(d) Indique la correspondecia entre HN/N y $H/(H \cap N)$ descrita en la demostración del Segundo Teorema de Isomorfía.

8. Si G es un grupo abeliano y $n \in \mathbb{N}$, demuestre que $\phi : G \to G$ definida como $g \mapsto g^n$ es un homomorfismo de grupos.

9. Si $\phi : G \to H$ es un homomorfismo de grupos y G es abeliano, demuestre que $\phi(G)$ también es abeliano.

10. Si $\phi : G \to H$ es un homomorfismo de grupos y G es cíclico, demuestre que $\phi(G)$ también es cíclico.

11. Muestre que un homomorfismo definido en un grupo cíclico está completamente determinado por su acción en el generador del grupo.

12. Si un grupo G tiene exactamente un subgrupo H de orden k, demuestre que H es normal en G.

13. Demuestre o refute: $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}$.

14. Sea G un grupo finito y sea N un subgrupo normal de G. Si H es un subgrupo de G/N, demuestre que $\phi^{-1}(H)$ es un subgrupo en G de orden $|H| \cdot |N|$, donde $\phi : G \to G/N$ es el homomorfismo canónico.

15. Sean G_1 y G_2 grupos, y sean H_1 y H_2 subgrupos normales de G_1 y G_2 respectivamente. Sea $\phi : G_1 \to G_2$ un homomorfismo. Muestre que ϕ induce un homomorfismo natural $\overline{\phi} : (G_1/H_1) \to (G_2/H_2)$ si $\phi(H_1) \subset H_2$.

16. Si H y K son subgrupos normales de G y $H \cap K = \{e\}$, demuestre que G es isomorfo a un subgrupo de $G/H \times G/K$.

17. Sea $\phi : G_1 \to G_2$ un epimorfismo de grupos. Sea H_1 un subgrupo normal de G_1 y supongamos que $\phi(H_1) = H_2$. Demuestre o refute que $G_1/H_1 \cong G_2/H_2$.

18. Sea $\phi : G \to H$ un homomorfismo de grupos. Muestre que ϕ es 1-1 si y solo si $\phi^{-1}(e) = \{e\}$.

19. Dado un homomorfismo $\phi : G \to H$ defina una relación $\sim$ en G como $a \sim b$ si $\phi(a) = \phi(b)$ para $a, b \in G$. Muestre que esta relación es de equivalencia y describa las clases de equivalencia.

11.4 Ejercicios adicionales: Automorfismos

1. Sea $\mathrm{Aut}(G)$ el conjunto de todos los automorfismos de G; es decir, isomorfismos de G en si mismo. Demuestre que este conjunto forma un grupo y que es un subgrupo del grupo de permutaciones de G; es decir, $\mathrm{Aut}(G) \leq S_G$.

2. Un ***automorfismo interno*** de G,

$$i_g : G \to G,$$

está definido por la función

$$i_g(x) = gxg^{-1},$$

para $g \in G$. Demuestre que $i_g \in \text{Aut}(G)$.

3. El conjunto de todos los automorfismos internos se denota por $\text{Inn}(G)$. Muestre que $\text{Inn}(G)$ es un subgrupo de $\text{Aut}(G)$.

4. Enecuentre un automorfismo de un grupo G que no sea un automorfismo interno.

5. Sea G un grupo y sea i_g un automorfismo interno de G. Defina la función

$$G \to \text{Aut}(G)$$

por

$$g \mapsto i_g.$$

Demuestre que esta función es un homomorfismo con imagen $\text{Inn}(G)$ y núcleo $Z(G)$. Use este resultado para concluir que

$$G/Z(G) \cong \text{Inn}(G).$$

6. Calcule $\text{Aut}(S_3)$ y $\text{Inn}(S_3)$. Haga lo mismo para D_4.

7. Encuentre todos los homomorfismos $\phi : \mathbb{Z} \to \mathbb{Z}$. ¿Qué es $\text{Aut}(\mathbb{Z})$?

8. Encuentre todos los automorfismos de $\mathbb{Z}_8$. Demuestre que $\text{Aut}(\mathbb{Z}_8) \cong U(8)$.

9. Para $k \in \mathbb{Z}_n$, defina una función $\phi_k : \mathbb{Z}_n \to \mathbb{Z}_n$ por $a \mapsto ka$. Demuestre que ϕ_k es un homomorfismo.

10. Demuestre que ϕ_k es un isomorfismo si y solo si k es un generador de $\mathbb{Z}_n$.

11. Muestre que todo automorfismo de $\mathbb{Z}_n$ es de la forma ϕ_k, con k un generador de $\mathbb{Z}_n$.

12. Demuestre que $\psi : U(n) \to \text{Aut}(\mathbb{Z}_n)$ es un isomorfismo, donde $\psi : k \mapsto \phi_k$.

11.5 Sage

Sage es capaz de crear homomorfismos (y por ende, isomorfismos y automorfismos) entre grupos finitos de permutaciones. Hay pocos comandos disponibles para manipular estas funciones, pero aún así podremos ilustrar muchas de las ideas de este capítulo.

Homomorfismos

La principal forma de crear un homomorfismo es especificando las imágenes para el conjunto de generadores del dominio. Considere grupos cíclicos de órdenes 12 y 20:

$$G = \{a^i | a^{12} = e\} \qquad\qquad H = \{x^i | x^{20} = e\}$$

y defina un homomorfismo simplemente especificando la imagen para un generador de G, y extendiendo la función al resto del grupo via la propiedad de preservación de la operación de un homomorfismo.

$$\begin{aligned} \phi : G \to H, \quad & \phi(a) = x^5 \\ \Rightarrow \quad & \phi(a^i) = \phi(a)^i = (x^5)^i = x^{5i} \end{aligned}$$

El constructor `PermutationGroupMorphism` requiere los dos grupos, luego una lista de imágenes para cada generador (¡en orden!), y entonces creará el homomorfismo. Note que podemos usar el resultado como una función. En el ejemplo abajo, primero verificamos que `C12` tiene un único generador (ninguna novedad), el cuál enviamos a un elemento particular de orden 4 en el codominio. Sage entonces construye el único homomorfismo consistente con este requisito.

```
C12 = CyclicPermutationGroup(12)
C20 = CyclicPermutationGroup(20)
domain_gens = C12.gens()
[g.order() for g in domain_gens]
```

```
[12]
```

```
x = C20.gen(0)
y = x^5
y.order()
```

```
4
```

```
phi = PermutationGroupMorphism(C12, C20, [y])
phi
```

```
Permutation group morphism:
  From: Cyclic group of order 12 as a permutation group
  To:   Cyclic group of order 20 as a permutation group
  Defn: [(1,2,3,4,5,6,7,8,9,10,11,12)] ->
        [(1,6,11,16)(2,7,12,17)(3,8,13,18)(4,9,14,19)(5,10,15,20)]
```

```
a = C12("(1,6,11,4,9,2,7,12,5,10,3,8)")
phi(a)
```

```
(1,6,11,16)(2,7,12,17)(3,8,13,18)(4,9,14,19)(5,10,15,20)
```

```
b = C12("(1,3,5,7,9,11)(2,4,6,8,10,12)")
phi(b)
```

```
(1,11)(2,12)(3,13)(4,14)(5,15)(6,16)(7,17)(8,18)(9,19)(10,20)
```

```
c = C12("(1,9,5)(2,10,6)(3,11,7)(4,12,8)")
phi(c)
```

```
()
```

Note que el elemento `c` debe por lo tanto estar en el núcleo de `phi`.

Podemos calcular el subgrupo del dominio que es el núcleo, y en este caso un grupo cíclico de orden 3 al interior del grupo cíclico de orden 12. Podemos calcular la imagen de *cualquier* subgroup, pero acá construiremos la imagen homomorfa completa entregándole el dominio completo al método `.image()`. Acá la imagen es un subgrupo cíclico de orden 4 dentro del grupo cíclico de orden 20. Después podemos verificar el Primer Teorema de Isomorfía.

```
K = phi.kernel(); K
```

```
Subgroup of (Cyclic group of order 12 as a permutation group)
generated by [(1,5,9)(2,6,10)(3,7,11)(4,8,12)]
```

```
Im = phi.image(C12); Im
```

```
Subgroup of (Cyclic group of order 20 as a permutation group)
generated by
    [(1,6,11,16)(2,7,12,17)(3,8,13,18)(4,9,14,19)(5,10,15,20)]
```

```
Im.is_isomorphic(C12.quotient(K))
```

```
True
```

Ahora un ejemplo ligeramente más complicado. El grupo dihedral D_{20} es el grupo de simetrías de un polígono regular de 20 lados. Dentro de este grupo hay un subgrupo que es isomorfo al grupo de simetrías de un pentágono regular. ¿Es una sorpresa o es obvio? Acá hay una forma de precisar la afirmación de que "D_{20} contiene una copia de D_5."

Construimos el dominio y encontramos sus generadores, así sabemos cuántas imágenes proveer en la definición del homomorfismo. Despuñes construimos el codominio, del que construiremos imágenes. Nuestra elección acá es enviar una reflexión en una reflexión, y una rotación en una rotación. Pero las rotaciones deben ambas tener orden 5, y ambas ser rotaciones en 72 grados.

```
G = DihedralGroup(5)
H = DihedralGroup(20)
G.gens()
```

```
[(1,2,3,4,5), (1,5)(2,4)]
```

```
H.gens()
```

```
[(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20),
 (1,20)(2,19)(3,18)(4,17)(5,16)(6,15)(7,14)(8,13)(9,12)(10,11)]
```

```
x = H.gen(0)^4
y = H.gen(1)
rho = PermutationGroupMorphism(G, H, [x, y])
rho.kernel()
```

```
Subgroup of (Dihedral group of order 10 as a permutation
    group)
generated by [()]
```

Como el núcleo en trivial, `rho` es una función 1-1 (ver el Ejercicio 11.3.18). Pero más importante, por el Primer Teorema de Isomorfía, `G` es isomorfo a la imagen del homomorfismo. Calcularemos la imagen para verificar la afirmación.

```
Im = rho.image(G); Im
```

```
Subgroup of (Dihedral group of order 40 as a permutation
    group)
generated by
[(1,5,9,13,17)(2,6,10,14,18)(3,7,11,15,19)(4,8,12,16,20),
(1,20)(2,19)(3,18)(4,17)(5,16)(6,15)(7,14)(8,13)(9,12)(10,11)]
```

```
Im.is_subgroup(H)
```

```
True
```

```
Im.is_isomorphic(G)
```

```
True
```

Simplemente dando una lista de imágenes para los generadores del dominio no es una garantía de que la función pueda extenderse a un homomorfismo. Para empezar, el orden de cada imagen debe dividir al orden de la preimagen correspondiente. (¿Puede demostrar esto?) Similarmente, si el dominio es abeliano, entonces la imagen debe también ser abeliana, así en este caso las imágenes no debiesen generar un subgrupo no abeliano. Acá hay un ejemplo. No hay homomorfismos de un grupo cíclico de orden 7 a un grupo cíclico de orden 4 (salvo la función trivial que lleva a todos los elementos a la identidad). Para ver esto, considere los posibles órdenes del núcleo, y de las dos posibilidades, vea que una es imposible y que la otra se realiza con el homomorfismo trivial. Desafortunadamente, Sage actúa como si no hubiera nada malo en crear un homomorfismo entre estos dos grupos, pero lo que Sage crea es inútil y produce errores si trata de usarlo.

```
G = CyclicPermutationGroup(7)
H = CyclicPermutationGroup(4)
tau = PermutationGroupMorphism_im_gens(G, H, H.gens())
tau
```

```
Permutation group morphism:
  From: Cyclic group of order 7 as a permutation group
  To:   Cyclic group of order 4 as a permutation group
  Defn: [(1,2,3,4,5,6,7)] -> [(1,2,3,4)]
```

```
tau.kernel()
```

```
Traceback (most recent call last):
...
RuntimeError: Gap produced error output
...
```

En lugar de crear homomorfismos por nosotros mismos, en ciertas situaciones Sage sabe de la existencia de homomorfismos naturales y los creará para nosotros. Un caso de estos es la construcción del producto directo. Dado un grupo `G`, el método `.direct_product(H)` creará el producto directo $G \times H$. (Este no es el mismo comando que la función `direct_product_permgroups()` from before.) Este comando no solo crea el producto directo, sino que además construye *cuatro* homomorfismos, uno con dominio G, uno con dominio H y dos con dominio $G \times H$. Así la salida consiste de cinco objetos, el primero de los cuales es el grupo en sí, y los restantes son homomorfismos. Mostraremos un ejemplo acña y dejaremos una investigación más exhaustiva para los ejercicios.

```
G = CyclicPermutationGroup(3)
H = DihedralGroup(4)
results = G.direct_product(H)
results[0]
```

```
Permutation Group with generators [(4,5,6,7), (4,7)(5,6),
    (1,2,3)]
```

```
results[1]
```

```
Permutation group morphism:
  From: Cyclic group of order 3 as a permutation group
  To:   Permutation Group with generators
        [(4,5,6,7), (4,7)(5,6), (1,2,3)]
  Defn: Embedding( Group( [ (1,2,3), (4,5,6,7), (4,7)(5,6) ]
      ), 1 )
```

```
results[2]
```

```
Permutation group morphism:
  From: Dihedral group of order 8 as a permutation group
  To:   Permutation Group with generators
        [(4,5,6,7), (4,7)(5,6), (1,2,3)]
  Defn: Embedding( Group( [ (1,2,3), (4,5,6,7), (4,7)(5,6) ]
      ), 2 )
```

```
results[3]
```

```
Permutation group morphism:
  From: Permutation Group with generators
        [(4,5,6,7), (4,7)(5,6), (1,2,3)]
  To:   Cyclic group of order 3 as a permutation group
  Defn: Projection( Group( [ (1,2,3), (4,5,6,7), (4,7)(5,6) ]
      ), 1 )
```

```
results[4]
```

```
Permutation group morphism:
  From: Permutation Group with generators
        [(4,5,6,7), (4,7)(5,6), (1,2,3)]
  To:   Dihedral group of order 8 as a permutation group
  Defn: Projection( Group( [ (1,2,3), (4,5,6,7), (4,7)(5,6) ]
      ), 2 )
```

11.6 Ejercicios Sage

1. Un automorfismo es un isomorfismo de un grupo en si mismo. La función identidad ($x \mapsto x$) siempre es un isomorfismo, que consideramos trivial. Use Sage para construir un automrfismo no trivial del grupo cíclico de orden 12. Verfique que la función es biyectiva calculando su imagen y su núcleo y realizando pruebas en estos subgrupos. Ahora construya todos los posibles automorfismos del grupos cíclico de orden 12 sin repeticiones.

2. Los cuatro homomorfismos creados por la construcción del producto directo son cada uno un ejemplo de una construcció más general de homomorfismos que involucran los grupos G, H y $G \times H$. Usando los mismos grupos del ejemplo en la subsección anterior, vea si puede descubrir y describir estas construcciones con definiciones exactas de los cuatro homomorfismos en general.
Las herramientas para investigar homomorfismos de grupos en Sage group son limitadas, se puede tomar cada generador del dominio y ver cuál es su imagen. A continuación un ejemplo de este tipo de cálculo que puede realizar repetidamente. Investigaremos el segundo homomorfismo. El dominio es el grupo dihedral, y calcularemos la imagen del primer generador.

```
G = CyclicPermutationGroup(3)
H = DihedralGroup(4)
results = G.direct_product(H)
phi = results[2]
H.gens()
```

```
[(1,2,3,4), (1,4)(2,3)]
```

```
a = H.gen(0); a
```

```
(1,2,3,4)
```

```
phi(a)
```

```
(4,5,6,7)
```

3. Considere dos grupos de permutaciones. El primero es el subgrupo de S_7 generado por $(1, 2, 3)$ y $(4, 5, 6, 7)$. El segundo es el subgrupo de S_{12} generado por $(1, 2, 3)(4, 5, 6)(7, 8, 9)(10, 11, 12)$ y $(1, 10, 7, 4)(2, 11, 8, 5)(3, 12, 9, 6)$. Construya estos dos grupos y use el comando Sage apropiado para ver que son isomorfos. Después construya un homomorfismo entre estos dos grupos que sea un isomorfismo e incluya suficientes detalles para verificar que la función es realmente un isomorfismo.

4. El segundo párrafo de este capítulo describe informalmente un homomorfismo de S_n a $\mathbb{Z}_2$, donde las permutaciones pares se envían todas en uno de los elementos y las impares en el otro elemento. Reemplace S_n por S_6 y reemplace $\mathbb{Z}_2$ por la versión permutacional del grupo cíclico de orden 2, y construya un homomorfismo no trivial entre estos dos grupos. Evalúe su homomorfismo en suficientes permutaciones pares e impares para convencerse de que está correcto. Después construya el núcleo y verifique que es el grupo que espera que sea.
Hints: Primero, decida que elementos del grupo de orden 2 estará asociado con las permutaciones pares y cuál con las impares. Examine los generadores de S_6 para ayudarle a decidir como definir el homomorfismo.

5. El grupo dihedral D_{20} tiene varios subgrupos normales, como se ve más abajo. Cada uno de estos es el núcleo de un homomorfismo cuyo dominio es D_{20}. Para cada subgrupo normal de D_{20} construya un homomorfismo de D_{20} a D_{20} que tenga el subgrupo normal como su núcleo. Incluya verificaciones en su trabajo de que está obteniendo los núcleos deseados. Hay un patrón en muchos de estos, pero los tres de orden 20 serán un desafío.

```
G = DihedralGroup(20)
[H.order() for H in G.normal_subgroups()]
```

```
[1, 2, 4, 5, 10, 20, 20, 20, 40]
```

12

Grupos de Matrices y Simetría

Cuando Felix Klein (1849–1925) aceptó una cátedra en la Universidad de Erlangen, en su discurso inaugural, describió un programa para clasificar diferentes geometrías. Central al programa de Klein era la teoría de grupos: él consideraba que la geometría consiste en estudiar las propiedades que quedan invariantes bajo grupos de transformaciones. Los grupos, especialmente los grupos de matrices, ha ganado mucha importancia en el estudio de simetrías y tienen aplicaciones en otras disciplinas tales como química y física. En la primera parte de este capítulo, examinaremos algunos de los grupos de matrices clásicos, tales como el grupo lineal general, el grupo lineal especial, y el grupo ortogonal. Usaremos luego estos grupos para estudiar algunas de las ideas detrás de la simetría geométrica.

12.1 Grupos de Matrices

Algunos Resultados de Álgebra Lineal

Antes de estudiar grupos de matrices, debemos ercordar algunos resultados básicos de álgebra lineal. Una de las ideas fundamentales de álgebra lineal es la de una transformación lineal. Una ***transformación lineal*** o ***función lineal*** $T : \mathbb{R}^n \to \mathbb{R}^m$ es una función que respeta (o preserva) la suma de vectores y la multiplicación por escalares; es decir, para vectores $\mathbf{x}$ e $\mathbf{y}$ en $\mathbb{R}^n$ y un escalar $\alpha \in \mathbb{R}$,

$$\begin{aligned} T(\mathbf{x}+\mathbf{y}) &= T(\mathbf{x}) + T(\mathbf{y}) \\ T(\alpha\mathbf{y}) &= \alpha T(\mathbf{y}). \end{aligned}$$

Una matriz de $m \times n$ con coeficientes en $\mathbb{R}$ representa una transformación lineal de $\mathbb{R}^n$ a $\mathbb{R}^m$. Si escribimos vectores $\mathbf{x} = (x_1, \ldots, x_n)^{\mathrm{t}}$ e $\mathbf{y} = (y_1, \ldots, y_n)^{\mathrm{t}}$ en $\mathbb{R}^n$ como matrices de una columna, entonces una matriz de $m \times n$

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

envía a los vectores en $\mathbb{R}^m$ linealmente por multiplicación matricial. Observe que si α es un número real,

$$A(\mathbf{x}+\mathbf{y}) = A\mathbf{x} + A\mathbf{y} \qquad \text{and} \qquad \alpha A\mathbf{x} = A(\alpha\mathbf{x}),$$

donde

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Con frecuencia abreviaremos la matriz A escribiendo (a_{ij}).

Recíprocamente, si $T : \mathbb{R}^n \to \mathbb{R}^m$ es una función lineal, podemos asociar una matriz A con T considerando lo que T le hace a los vectores

$$\begin{aligned} \mathbf{e}_1 &= (1, 0, \ldots, 0)^{\mathrm{t}} \\ \mathbf{e}_2 &= (0, 1, \ldots, 0)^{\mathrm{t}} \\ &\vdots \\ \mathbf{e}_n &= (0, 0, \ldots, 1)^{\mathrm{t}}. \end{aligned}$$

Podemos escribir cualquier vector $\mathbf{x} = (x_1, \ldots, x_n)^{\mathrm{t}}$ como

$$x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \cdots + x_n\mathbf{e}_n.$$

Así, si

$$\begin{aligned} T(\mathbf{e}_1) &= (a_{11}, a_{21}, \ldots, a_{m1})^{\mathrm{t}}, \\ T(\mathbf{e}_2) &= (a_{12}, a_{22}, \ldots, a_{m2})^{\mathrm{t}}, \\ &\vdots \\ T(\mathbf{e}_n) &= (a_{1n}, a_{2n}, \ldots, a_{mn})^{\mathrm{t}}, \end{aligned}$$

entonces

$$\begin{aligned} T(\mathbf{x}) &= T(x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \cdots + x_n\mathbf{e}_n) \\ &= x_1T(\mathbf{e}_1) + x_2T(\mathbf{e}_2) + \cdots + x_nT(\mathbf{e}_n) \\ &= \left(\sum_{k=1}^{n} a_{1k}x_k, \ldots, \sum_{k=1}^{n} a_{mk}x_k \right)^{\mathrm{t}} \\ &= A\mathbf{x}. \end{aligned}$$

Ejemplo 12.1. Si $T : \mathbb{R}^2 \to \mathbb{R}^2$ es la función dada por

$$T(x_1, x_2) = (2x_1 + 5x_2, -4x_1 + 3x_2),$$

los axiomas que T debe satisfacer para ser una transformación lineal se verifican fácilmente. Los vectores columna $T\mathbf{e}_1 = (2, -4)^{\mathrm{t}}$ y $T\mathbf{e}_2 = (5, 3)^{\mathrm{t}}$ nos dicen que T está dada por la matriz

$$A = \begin{pmatrix} 2 & 5 \\ -4 & 3 \end{pmatrix}.$$

Como estamos interesados en grupos de matrices, necesitamos saber qué matrices tienen inverso multiplicativo. Recuerde que una matriz A de $n \times n$ es ***invertible*** si y solo si existe otra matriz A^{-1} tal que $AA^{-1} = A^{-1}A = I$, donde

$$I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

es la matriz identidad de $n \times n$. De álgebra lineal sabemos que A es invertible si y solo si el determinante de A es distinto de cero. También se dice que una matriz invertible es ***no singular***.

Ejemplo 12.2. Si A es la matriz

$$\begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix},$$

entonces la inversa de A es

$$A^{-1} = \begin{pmatrix} 3 & -1 \\ -5 & 2 \end{pmatrix}.$$

Sabemos que A^{-1} existe, pues $\det(A) = 2 \cdot 3 - 5 \cdot 1 = 1$ no es cero.

Algunos otros hechos sobre determinantes resultarán útiles en el transcurso de este capítulo. Sean A y B matrices de $n \times n$. De álgebra lineal tenemos las siguientes propiedades de los determinantes.

- El determinante es un homomorfismo al grupo multiplicativo de los números reales; es decir, $\det(AB) = (\det A)(\det B)$.
- Si A es una matriz invertible, entonces $\det(A^{-1}) = 1/\det A$.
- Si definimos la transpuesta de una matriz $A = (a_{ij})$ como $A^{\mathrm{t}} = (a_{ji})$, entonces $\det(A^{\mathrm{t}}) = \det A$.
- Sea T la transformación lineal asociada con una matriz A de $n \times n$. Entonces T multiplica volúmenes por un facor de $|\det A|$. En el caso de $\mathbb{R}^2$, esto quiere decir que T multiplica áreas por $|\det A|$.

Funciones lineales, matrices, y determinantes se pasan en un curso elemental de álgebra lineal; pero, si no ha tenido un curso así, es un proceso simple verificar estas propiedades directamente para matrices de 2×2, que es el caso que más nos interesará.

El Grupo Lineal General y el Grupo Lineal Especial

El conjunto de todas las matrices invertibles de $n \times n$ forma un grupo llamado ***grupo lineal general***. Denotaremos este grupo por$GL_n(\mathbb{R})$. El grupo lineal general tiene varios subgrupos importantes. La propiedad multiplicativa del determinante implica que el conjunto de las matrices cuyo determinante es uno es un subgrupo del grupo lineal general. Dicho de otra forma, supongamos que $\det(A) = 1$ y que $\det(B) = 1$. Entonces $\det(AB) = \det(A)\det(B) = 1$ y $\det(A^{-1}) = 1/\det A = 1$. Este subgrupo se llama ***grupo lineal especial*** y se denota por $SL_n(\mathbb{R})$.

Ejemplo 12.3. Dada una matriz de 2×2

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

el determinante de A es $ad-bc$. El grupo $GL_2(\mathbb{R})$ consiste de aquellas matrices para las que $ad - bc \neq 0$. La inversa de A es

$$A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Si A está en $SL_2(\mathbb{R})$, entonces

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Geométricamente, $SL_2(\mathbb{R})$ es el grupo que preserva las áreas de los paralelógramos. Sea

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

en $SL_2(\mathbb{R})$. En la Figura 12.4, el cuadrado unitario correspondiente a los vectores $\mathbf{x} = (1,0)^t$ y $\mathbf{y} = (0,1)^t$ es enviado por A al paralelógramo con lados $(1,0)^t$ y $(1,1)^t$; es decir, $A\mathbf{x} = (1,0)^t$ y $A\mathbf{y} = (1,1)^t$. Note que estos dos paralelógramos tienen la misma área.

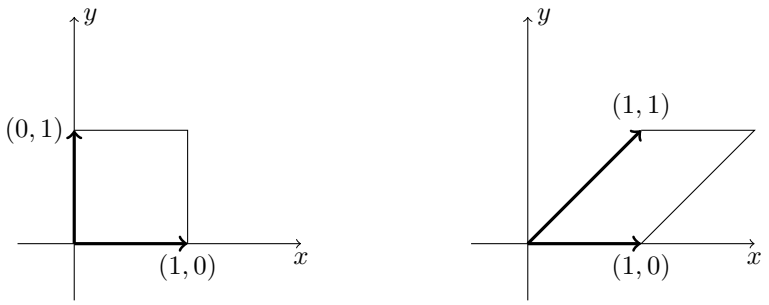


Figura 12.4: $SL_2(\mathbb{R})$ actuando en el cuadrado unitario

El Grupo Ortogonal $O(n)$

Otro subgrupo de $GL_n(\mathbb{R})$ es el grupo ortogonal. Una matriz A es ***ortogonal*** si $A^{-1} = A^t$. El ***grupo ortogonal*** consiste en el conjunto de todas las matrices ortogonales. Escribimos $O(n)$ para el grupo ortogonal de $n \times n$. Dejamos como ejercicio demostrar que $O(n)$ es un subgrupo de $GL_n(\mathbb{R})$.

Ejemplo 12.5. Las siguiente matrices son ortogonales:

$$\begin{pmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{pmatrix}, \quad \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}, \quad \begin{pmatrix} -1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 1/\sqrt{6} & -2/\sqrt{6} & 1/\sqrt{6} \\ 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \end{pmatrix}.$$

Hay una forma más geométrica de ver el grupo $O(n)$. Las matrices ortogonales son exactamente aquellas que preservan lad longitudes de los vectores. Podemos definir la longitud de un vector usando el ***producto interno Euclideano***, o ***producto punto***, de dos vectores. El producto interno Euclideano de dos vectores $\mathbf{x} = (x_1, \ldots, x_n)^t$ y $\mathbf{y} = (y_1, \ldots, y_n)^t$ es

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^t \mathbf{y} = (x_1, x_2, \ldots, x_n) \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = x_1 y_1 + \cdots + x_n y_n.$$

Definimos la longitud de un vector $\mathbf{x} = (x_1, \ldots, x_n)^t$ como

$$\|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle} = \sqrt{x_1^2 + \cdots + x_n^2}.$$

Asociada a la noción de longitud de un vector está la idea de distancia entre dos vectores. Definimos la ***distancia*** entre dos vectores $\mathbf{x}$ e $\mathbf{y}$ como $\|\mathbf{x}-\mathbf{y}\|$. Dejamos como ejercicio demostrar la siguiente proposición sobre las propiedades de los productos internos Euclideanos.

Proposición 12.6. *Sean* $\mathbf{x}$, $\mathbf{y}$, *y* $\mathbf{w}$ *vectores en* $\mathbb{R}^n$ *y* $\alpha \in \mathbb{R}$. *Entonces*

1. $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$.
2. $\langle \mathbf{x}, \mathbf{y} + \mathbf{w} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{x}, \mathbf{w} \rangle$.
3. $\langle \alpha\mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{x}, \alpha\mathbf{y} \rangle = \alpha \langle \mathbf{x}, \mathbf{y} \rangle$.
4. $\langle \mathbf{x}, \mathbf{x} \rangle \geq 0$ *con igualdad exactamente cuando* $\mathbf{x} = 0$.
5. *Si* $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ *para todo* $\mathbf{x}$ *en* $\mathbb{R}^n$, *entonces* $\mathbf{y} = 0$.

Ejemplo 12.7. El vector $\mathbf{x} = (3, 4)^{\mathrm{t}}$ tiene longitud $\sqrt{3^2 + 4^2} = 5$. Podemos también ver que la matriz ortogonal

$$A = \begin{pmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{pmatrix}$$

preserva la longitud de este vector. El vector $A\mathbf{x} = (-7/5, 24/5)^{\mathrm{t}}$ también tiene longitud 5.

Como $\det(AA^{\mathrm{t}}) = \det(I) = 1$ y $\det(A) = \det(A^{\mathrm{t}})$, el determinante de cualquier matriz ortogonal es 1 o -1. Considere los vectores columna

$$\mathbf{a}_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix}$$

de la matriz ortogonal $A = (a_{ij})$. Since $AA^{\mathrm{t}} = I$, $\langle \mathbf{a}_r, \mathbf{a}_s \rangle = \delta_{rs}$, donde

$$\delta_{rs} = \begin{cases} 1 & r = s \\ 0 & r \neq s \end{cases}$$

es la delta de Kronecker . Así, los vectores columna de una matriz ortogonal todos tienen longitud 1; y el producto interno Euclideano de vectores columna distintos es cero. Cualquier conjunto de vectores que satisface esta propiedad se llama ***conjunto ortonormal***. Recíprocamente, dada una matriz A de $n \times n$ cuyas columnas forman un conjunto ortonormal, se tiene que $A^{-1} = A^{\mathrm{t}}$.

Decimos que una matriz A ***preserva distancias***, o ***preserva el producto interno*** cuando $\|T\mathbf{x} - T\mathbf{y}\| = \|\mathbf{x} - \mathbf{y}\|$, $\|T\mathbf{x}\| = \|\mathbf{x}\|$, o $\langle T\mathbf{x}, T\mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle$, respectivamente. El siguiente teorema, que caracteriza el grupo ortogonal, establece que estos conceptos son iguales.

Teorema 12.8. *Sea* A *una matriz de* $n \times n$. *Los siguientes enunciados son equivalentes.*

1. *Las columnas de la matriz* A *forman un conjunto ortonormal.*
2. $A^{-1} = A^{\mathrm{t}}$.
3. *Para vectores cualquiera* $\mathbf{x}$ *e* $\mathbf{y}$, $\langle A\mathbf{x}, A\mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle$.
4. *Para vectores cualquiera* $\mathbf{x}$ *e* $\mathbf{y}$, $\|A\mathbf{x} - A\mathbf{y}\| = \|\mathbf{x} - \mathbf{y}\|$.

5. Para cualquier vector $\mathbf{x}$, $\|A\mathbf{x}\| = \|\mathbf{x}\|$.

DEMOSTRACIÓN. Ya hemos mostrado la equivalencia de (1) y (2).

(2) $\Rightarrow$ (3).

$$\begin{aligned}\langle A\mathbf{x}, A\mathbf{y}\rangle &= (A\mathbf{x})^{\mathrm{t}} A\mathbf{y} \\ &= \mathbf{x}^{\mathrm{t}} A^{\mathrm{t}} A\mathbf{y} \\ &= \mathbf{x}^{\mathrm{t}}\mathbf{y} \\ &= \langle \mathbf{x}, \mathbf{y}\rangle.\end{aligned}$$

(3) $\Rightarrow$ (2). Como

$$\begin{aligned}\langle \mathbf{x}, \mathbf{x}\rangle &= \langle A\mathbf{x}, A\mathbf{x}\rangle \\ &= \mathbf{x}^{\mathrm{t}} A^{\mathrm{t}} A\mathbf{x} \\ &= \langle \mathbf{x}, A^{\mathrm{t}} A\mathbf{x}\rangle,\end{aligned}$$

sabemos que $\langle \mathbf{x}, (A^{\mathrm{t}}A - I)\mathbf{x}\rangle = 0$ para todo $\mathbf{x}$. Por lo tanto, $A^{\mathrm{t}}A - I = 0$ o $A^{-1} = A^{\mathrm{t}}$.

(3) $\Rightarrow$ (4). Si A preserva el producto interno, entonces A preserva distancias, pues

$$\begin{aligned}\|A\mathbf{x} - A\mathbf{y}\|^2 &= \|A(\mathbf{x} - \mathbf{y})\|^2 \\ &= \langle A(\mathbf{x} - \mathbf{y}), A(\mathbf{x} - \mathbf{y})\rangle \\ &= \langle \mathbf{x} - \mathbf{y}, \mathbf{x} - \mathbf{y}\rangle \\ &= \|\mathbf{x} - \mathbf{y}\|^2.\end{aligned}$$

(4) $\Rightarrow$ (5). Si A preserva distancias, entonces A preserva longitudes. Tomando $\mathbf{y} = 0$, tenemos

$$\|A\mathbf{x}\| = \|A\mathbf{x} - A\mathbf{y}\| = \|\mathbf{x} - \mathbf{y}\| = \|\mathbf{x}\|.$$

(5) $\Rightarrow$ (3). Usamos la siguiente identidad para mostrar que la preservación de longitudes implica la preservación del producto interno:

$$\langle \mathbf{x}, \mathbf{y}\rangle = \frac{1}{2}\left[\|\mathbf{x} + \mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2\right].$$

Observe que

$$\begin{aligned}\langle A\mathbf{x}, A\mathbf{y}\rangle &= \frac{1}{2}\left[\|A\mathbf{x} + A\mathbf{y}\|^2 - \|A\mathbf{x}\|^2 - \|A\mathbf{y}\|^2\right] \\ &= \frac{1}{2}\left[\|A(\mathbf{x} + \mathbf{y})\|^2 - \|A\mathbf{x}\|^2 - \|A\mathbf{y}\|^2\right] \\ &= \frac{1}{2}\left[\|\mathbf{x} + \mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2\right] \\ &= \langle \mathbf{x}, \mathbf{y}\rangle.\end{aligned}$$

□

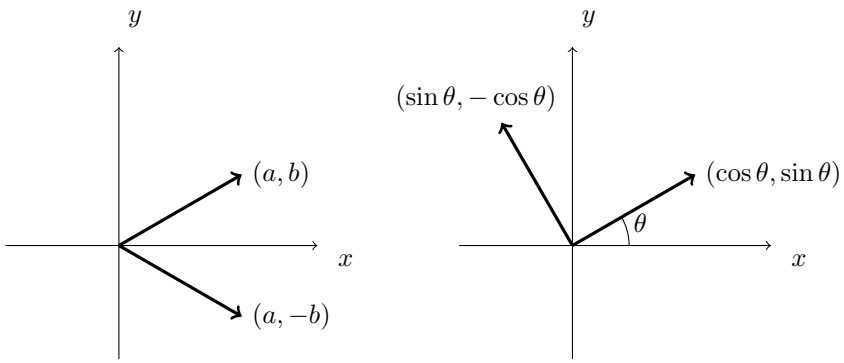


Figura 12.9: $O(2)$ actuando en $\mathbb{R}^2$

Ejemplo 12.10. Examinemos el grupo ortogonal en$\mathbb{R}^2$ en mayor detalle. Un elemento $T \in O(2)$ está determinado por su acción en $\mathbf{e}_1 = (1,0)^t$ y $\mathbf{e}_2 = (0,1)^t$. Si $T(\mathbf{e}_1) = (a,b)^t$, entonces $a^2 + b^2 = 1$ y $T(\mathbf{e}_2) = (-b,a)^t$. Luego, T puede ser representada por

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$

donde $0 \leq \theta < 2\pi$. Una matriz T en $O(2)$ ya sea refleja o rota un vector en $\mathbb{R}^2$ (Figura 12.9). Una reflexión respecto al eje horizontal está dada por la matriz

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

mientras una rotación en un ángulo θ en sentido antihorario debe venir de una matriz de la forma

$$\begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

Una reflexión respecto a una recta ℓ es simplemente una relfexión respecto al eje horizontal seguida de una rotación. Si $\det A = -1$, entonces A corresponde a una reflexión.

Dos de los otros grupos de matrices o relacionados a matrices que consideraremos son el grupo ortogonal especial y el grupo de movimientos Euclideanos. El ***grupo ortogonal especial***, $SO(n)$, e simplemente la intersección de $O(n)$ y $SL_n(\mathbb{R})$; es decir, aquellos elementos en $O(n)$ con determinante uno. El ***grupo Euclideano***, $E(n)$, puede ser escrito como pares ordenados $(A, \mathbf{x})$, donde A está en $O(n)$ y $\mathbf{x}$ está en $\mathbb{R}^n$. Definimos la multiplicación como

$$(A, \mathbf{x})(B, \mathbf{y}) = (AB, A\mathbf{y} + \mathbf{x}).$$

La identidad del grupo es $(I, \mathbf{0})$; el inverso de $(A, \mathbf{x})$ es $(A^{-1}, -A^{-1}\mathbf{x})$. En el Ejercicio 12.3.6, debe verificar que $E(n)$ es realmente un grupo con esta operación.

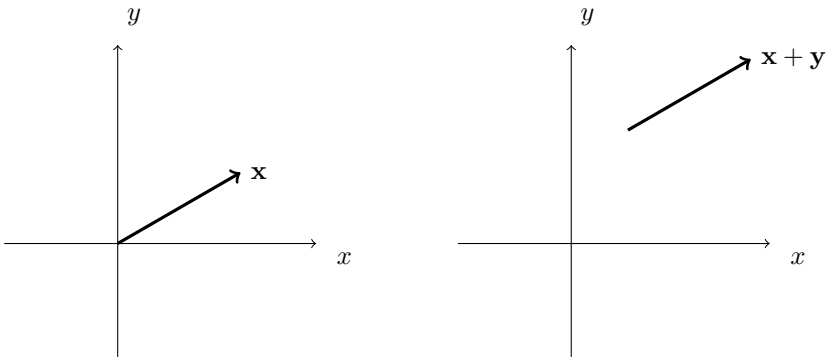


Figura 12.11: Traslaciones en $\mathbb{R}^2$

12.2 Simetría

Una ***isometría*** o ***movimiento rígido*** en $\mathbb{R}^n$ es una función f de $\mathbb{R}^n$ en $\mathbb{R}^n$ que preserva distancias. Esto quiere decir que f debe satisfacer

$$\|f(\mathbf{x}) - f(\mathbf{y})\| = \|\mathbf{x} - \mathbf{y}\|$$

para todo $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. No es difícil mostrar que f debe ser inyectiva. Por el Teorema 12.8, cualquier elemento en $O(n)$ es una isometría en $\mathbb{R}^n$; pero, $O(n)$ no incluye todas las posibles isometrías en $\mathbb{R}^n$. La traslación por un vector $\mathbf{x}$, $T_{\mathbf{y}}(\mathbf{x}) = \mathbf{x}+\mathbf{y}$ también es una isometría (Figura 12.11); Pero, T no puede estar en $O(n)$ pues no es una función lineal.

Estamos fundamentalmente interesados en las isometrías en $\mathbb{R}^2$. De hecho, las únicas isometrías en $\mathbb{R}^2$ son rotaciones en torno al origen, reflexiones respecto a rectas, traslaciones y combinaciones de estas. Por ejemplo, una ***reflexión deslizante*** es una traslación seguida de una reflexión (Figura 12.12). En $\mathbb{R}^n$ todas las isometrías están dadas de la misma forma. La demostrción se generaliza fácilmente.

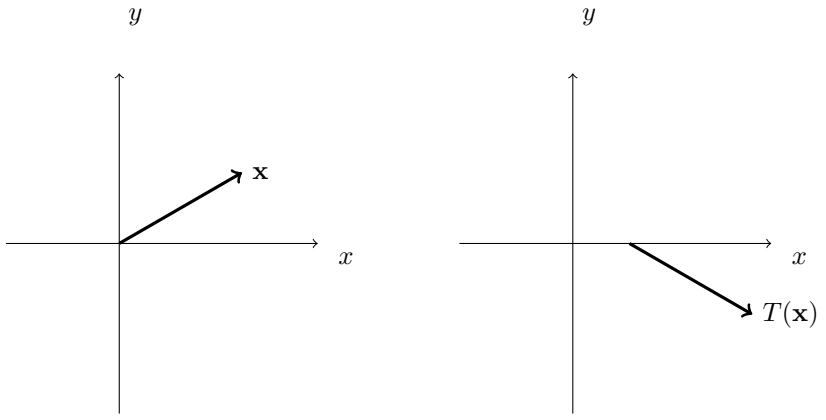


Figura 12.12: Reflexión deslizante

Lema 12.13. *Una isometríaf que fija el origen en $\mathbb{R}^2$ es una transformación lineal. En particular, f está dada por un elemento en $O(2)$.*

Demostración. Sea f una isometría en $\mathbb{R}^2$ que fija el origen. Mostraremos primero que f preserva el producto interno. Como $f(0) = 0$, $\|f(\mathbf{x})\| = \|\mathbf{x}\|$;

por lo tanto,

$$\begin{aligned}\|\mathbf{x}\|^2 - 2\langle f(\mathbf{x}), f(\mathbf{y})\rangle + \|\mathbf{y}\|^2 &= \|f(\mathbf{x})\|^2 - 2\langle f(\mathbf{x}), f(\mathbf{y})\rangle + \|f(\mathbf{y})\|^2 \\ &= \langle f(\mathbf{x}) - f(\mathbf{y}), f(\mathbf{x}) - f(\mathbf{y})\rangle \\ &= \|f(\mathbf{x}) - f(\mathbf{y})\|^2 \\ &= \|\mathbf{x} - \mathbf{y}\|^2 \\ &= \langle \mathbf{x} - \mathbf{y}, \mathbf{x} - \mathbf{y}\rangle \\ &= \|\mathbf{x}\|^2 - 2\langle \mathbf{x}, \mathbf{y}\rangle + \|\mathbf{y}\|^2.\end{aligned}$$

Así,

$$\langle f(\mathbf{x}), f(\mathbf{y})\rangle = \langle \mathbf{x}, \mathbf{y}\rangle.$$

Sean $\mathbf{e}_1$ y $\mathbf{e}_2$ $(1,0)^t$ y $(0,1)^t$, respectivamente. Si

$$\mathbf{x} = (x_1, x_2) = x_1\mathbf{e}_1 + x_2\mathbf{e}_2,$$

entonces

$$f(\mathbf{x}) = \langle f(\mathbf{x}), f(\mathbf{e}_1)\rangle f(\mathbf{e}_1) + \langle f(\mathbf{x}), f(\mathbf{e}_2)\rangle f(\mathbf{e}_2) = x_1 f(\mathbf{e}_1) + x_2 f(\mathbf{e}_2).$$

La linealidad de f se deduce fácilmente. □

Para una isometría arbitraria, f, $T_{\mathbf{x}}f$ fijará el origen para algún vector $\mathbf{x}$ en $\mathbb{R}^2$; luego, $T_{\mathbf{x}}f(\mathbf{y}) = A\mathbf{y}$ para alguna matriz $A \in O(2)$. Así, $f(\mathbf{y}) = A\mathbf{y} + \mathbf{x}$. Dadas las isometrías

$$\begin{aligned}f(\mathbf{y}) &= A\mathbf{y} + \mathbf{x}_1 \\ g(\mathbf{y}) &= B\mathbf{y} + \mathbf{x}_2,\end{aligned}$$

s composición es

$$f(g(\mathbf{y})) = f(B\mathbf{y} + \mathbf{x}_2) = AB\mathbf{y} + A\mathbf{x}_2 + \mathbf{x}_1.$$

Este último cálculo nos permite identificar el grupo de isometrías en $\mathbb{R}^2$ con $E(2)$.

Teorema 12.14. *El grupo de isometrías en $\mathbb{R}^2$ es el grupo Euclideano, $E(2)$.*

Un ***grupo de simetría*** en $\mathbb{R}^n$ es un subgrupo del grupo de isometrías en $\mathbb{R}^n$ que fija un conjunto de puntos $X \subset \mathbb{R}^n$. Es importante darse cuenta que el grupo de simetría de X depende *tanto* de $\mathbb{R}^n$ como de X. Por ejemplo, el grupo de simetría del origen en $\mathbb{R}^1$ es $\mathbb{Z}_2$, pero el grupo de simetría del origen en $\mathbb{R}^2$ es $O(2)$.

Teorema 12.15. *Los únicos grupos de simetría finitos en $\mathbb{R}^2$ son $\mathbb{Z}_n$ y D_n.*

Demostración. Sea $G = \{f_1, f_2, \ldots, f_n\}$ un grupo de simetría finito que fija un conjunto de puntos $X \subset \mathbb{R}^2$. Escoja un punto $\mathbf{x} \in X$. Este punto puede no ser un punto fijo—puede ser llevado por G a otro punto en X. Definamos un conjunto $S = \{\mathbf{y}_1, \mathbf{y}_2, \ldots \mathbf{y}_n\}$, donde $\mathbf{y}_i = f_i(\mathbf{x})$. Ahora, sea

$$\mathbf{z} = \frac{1}{n}\sum_{i=1}^{n} \mathbf{x}_i.$$

Si bien el punto $\mathbf{z}$ no necesariamente está en el conjunto X, queda fijo por todos los elementos del grupo de simetría. Sin pérdida de generalidad, podemos suponer que $\mathbf{z}$ es el origen.

Un grupo de simetría finito G en $\mathbb{R}^2$ que fija el origen debe ser un subgrupo finito de $O(2)$, pues las traslaciones y tralaciones deslizantes tienen orden infinito. NO ENTIENDO Por el Ejemplo 12.10, los elementos en $O(2)$ son ya sea rotaciones de la forma

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

o reflexiones de la forma

$$T_\phi = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{pmatrix}.$$

Notemos que $\det(R_\theta) = 1$, $\det(T_\phi) = -1$, y $T_\phi^2 = I$. Podemos dividir la demostración en dos casos. En el primer caso, todos los elementos en G tienen determinante uno. En el segundo caso, existe al menos un elemento en G con determinante -1.

Caso 1. El determinante de cada elemento en G es uno. En este caso todo elemento en G debe ser una rotación. Como G es finito, existe un ángulo positivo mínimo, digamos θ_0, tal que el correspondiente elemento R_{θ_0} es la menor rotación en la dirección positiva. Afirmamos que R_{θ_0} genera a G. Si no, para algún entero positivo n hay un ángulo θ_1 entre $n\theta_0$ y $(n+1)\theta_0$. Si es así, entonces $(n+1)\theta_0 - \theta_1$ corresponde a una rotación menor a θ_0, lo que contradice la minimalidad de θ_0.

Caso 2. El grupo G contiene una reflexión T. El núcleo del homomorfismo $\phi : G \to \{-1, 1\}$ dado por $A \mapsto \det(A)$ consiste de los elmentos cuyo determinante es 1. Por lo tanto, $|G/\ker\phi| = 2$. Sabemos que el núcleo es cíclico por el caso 1 y es un subgrupo de G de, digamos, orden n. Luego, $|G| = 2n$. Los elementos de G son

$$R_\theta, \ldots, R_\theta^{n-1}, TR_\theta, \ldots, TR_\theta^{n-1}.$$

Estos elementos satisfacen la relación

$$TR_\theta T = R_\theta^{-1}.$$

De manera que, G es isomorfo a D_n en este caso. □

Los Grupos Cristalográficos del Plano

Supongamos que queremos deseamos estudiar los patrones de empapelamiento del plano o los cristales en tres dimensiones. Los patrones de empapelamiento son simplemente patrones que se repiten en el plano (Figura 12.16). Los análogos de estos patrones en $\mathbb{R}^3$ son cristales, que podemos entender como patrones repetidos de moléculas en tres dimensiones (Figura 12.17). El equivalente matemático de un empapelamiento o patrón cristalográfico se llama reticulado.

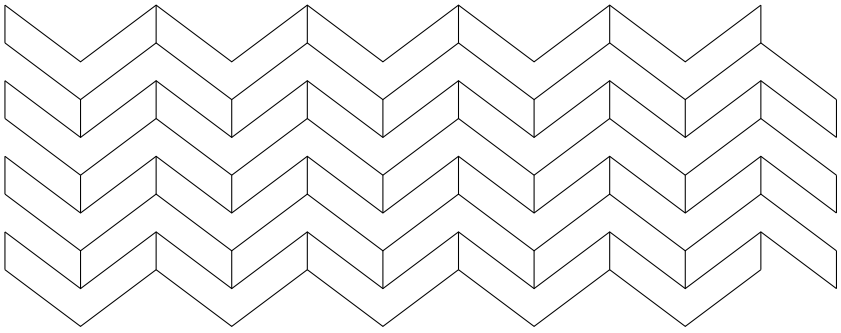


Figura 12.16: Un patrón de empapelamiento en $\mathbb{R}^2$

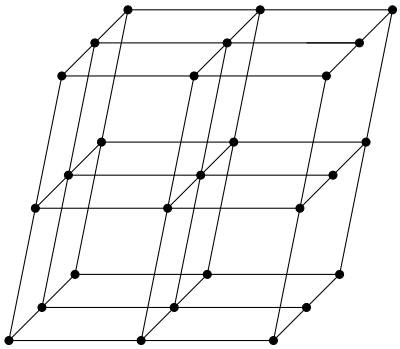


Figura 12.17: Una estructura cristalina en $\mathbb{R}^3$

Examinemos los patrones en el plano con un poco más de detalle. Supongamos que $\mathbf{x}$ e $\mathbf{y}$ son vectores linealmente independientes en $\mathbb{R}^2$; es decir, uno de ellos no puede ser un múltiplo escalar del otro. El ***reticulado*** de $\mathbf{x}$ e $\mathbf{y}$ es el conjunto de todas las combinaciones lineales $m\mathbf{x} + n\mathbf{y}$, donde m y n son enteros. Los vectores $\mathbf{x}$ e $\mathbf{y}$ se dice que son una ***base*** para el reticulado.

Note que un reticulado puede tener diferentes bases. Por ejemplo, los vectores $(1,1)^t$ y $(2,0)^t$ forman el mismo reticulado que los vectores $(-1,1)^t$ y $(-1,-1)^t$ (Figura 12.18). Pero, cualquier reticulado está completamente determinado por una base. Dadas dos bases para el mismo reticulado, digamos $\{\mathbf{x}_1, \mathbf{x}_2\}$ y $\{\mathbf{y}_1, \mathbf{y}_2\}$, podemos escribir

$$\begin{aligned} \mathbf{y}_1 &= \alpha_1\mathbf{x}_1 + \alpha_2\mathbf{x}_2 \\ \mathbf{y}_2 &= \beta_1\mathbf{x}_1 + \beta_2\mathbf{x}_2, \end{aligned}$$

donde α_1, α_2, β_1, y β_2 son enteros. La matriz correspondiente a esta transformación es

$$U = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix}.$$

Si queremos expresar $\mathbf{x}_1$ y $\mathbf{x}_2$ en términs de $\mathbf{y}_1$ e $\mathbf{y}_2$, solo debemos calcular U^{-1}; es decir,

$$U^{-1}\begin{pmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \end{pmatrix} = \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{pmatrix}.$$

Como U tiene coeficientes enteros, U^{-1} también debe tener coeficientes enteros; luego los determinantes de U y U^{-1} deben ser enteros. Como $UU^{-1} = I$,

$$\det(UU^{-1}) = \det(U)\det(U^{-1}) = 1;$$

de manera que, $\det(U) = \pm 1$. Una matriz con determinante ± 1 y coeficientes enteros se llama ***unimodular***. Por ejemplo, la matriz

$$\begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$$

es unimodular. Debería ser claro que hay una longitud mínima para los vectores en un reticulado.

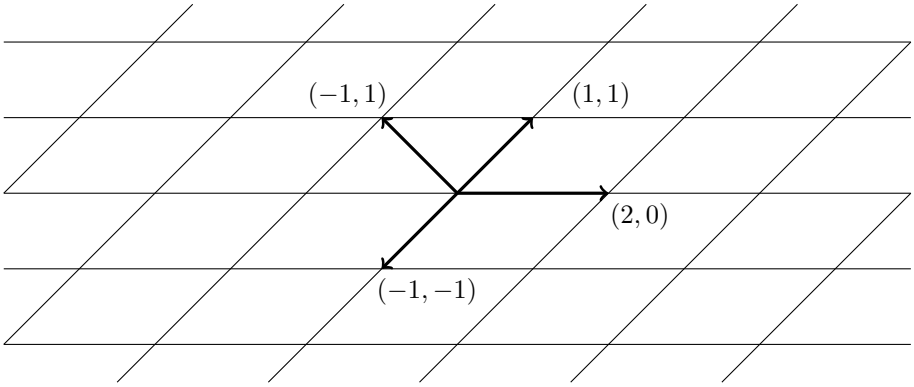


Figura 12.18: Un reticulado en $\mathbb{R}^2$

Podemos clasificar los reticulados estudiando sus grupos de simetría. El grupo de simetría de un reticulado es el subgrupo de $E(2)$ que envía el reticulado en sí mismo. Consideramos que dos reticulados en $\mathbb{R}^2$ son equivalentes si tienen el mismo grupo de simetría. De forma similar, la clasificación de cristales en $\mathbb{R}^3$ se obtiene asociando un grupo de simetría, llamado ***grupo espacial***, con cada tipo de cristal. Dos reticulados se consideran diferentes si sus grupos espaciales no son iguales. La pregunta natural que surge ahora es cuántos grupos espaciales existen.

Un grupo espacial está compuesto de dos partes: un ***subgrupo de traslación*** y uno ***puntual***. Un subgrupo de traslación es un subgrupo abeliano infinito del grupo espacial formado por las simetrias traslacionales del cristal; el grupo puntual es un grupo finito que consiste de rotaciones y reflexiones del cristal en torno a un punto. Más específicamente, un grupo espacial es un subgrupo $G \subset E(2)$ cuyas traslaciones son un conjunto de la forma $\{(I,t) : t \in L\}$, donde L es un reticulado. Los grupos espaciales son, por supuesto, infinitos. Usando argumentos geométricos, podemos demostrar el siguiente teorema (ver [5] o [6]).

Teorema 12.19. *Todo grupo d etraslación en $\mathbb{R}^2$ es isomorfo a $\mathbb{Z} \times \mathbb{Z}$.*

El grupo puntual de G es $G_0 = \{A : (A,b) \in G \text{ for some } b\}$. En particular, G_0 es un subgrupo de $O(2)$. Supongamos que $\mathbf{x}$ es un vector en un reticulado L con grupo espacial G, grupo de traslación H, y grupo puntual G_0. Para cualquier elemento $(A, \mathbf{y})$ en G,

$$\begin{aligned}(A,\mathbf{y})(I,\mathbf{x})(A,\mathbf{y})^{-1} &= (A, A\mathbf{x}+\mathbf{y})(A^{-1}, -A^{-1}\mathbf{y}) \\ &= (AA^{-1}, -AA^{-1}\mathbf{y} + A\mathbf{x} + \mathbf{y}) \\ &= (I, A\mathbf{x});\end{aligned}$$

luego, $(I, A\mathbf{x})$ está en el grupo de traslación de G. Más específicamente, $A\mathbf{x}$ deve estar en el reticulado L. IEs importante notar que G_0 no es usualmente

un subgrupo del grupo espacial G; pero, si T es el grupo de traslación de G, entonces $G/T \cong G_0$. La demostración del siguiente teorema se puede encontrar en [2], [5], o [6].

Teorema 12.20. *El grupo puntual en un grupo cristalográfico plano es isomorfo a $\mathbb{Z}_n$ o a D_n, donde $n = 1, 2, 3, 4, 6$.*

Para contestar la pregunta de cómo los grupos puntuales y los grupos de trslación pueden ser combinados, debemos mirar los distintos tipos de reticulados. Los reticulados pueden ser clasificados por la estructura de una celda del reticulado. Las posibles formas de celda son paralelógramo, rectangular, cuadrada, rómbica y hexagonal (Figura 12.21). Los grupos cristalográficos planos pueden ahora ser clasificados de acuerdo a los tipos de reflexiones que ocurren en cada grupo: estas son reflexiones ordinarias, reflexiones deslizantes, ambas o ninguna.

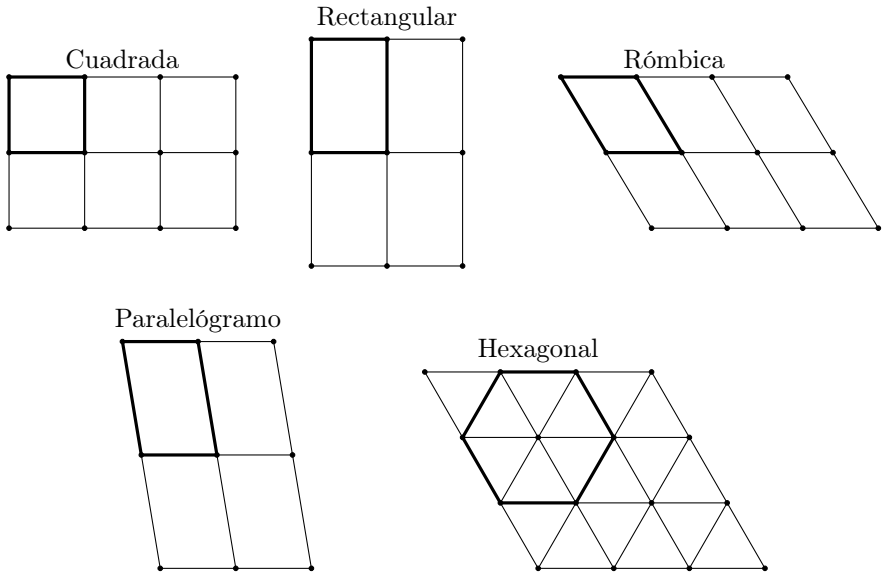
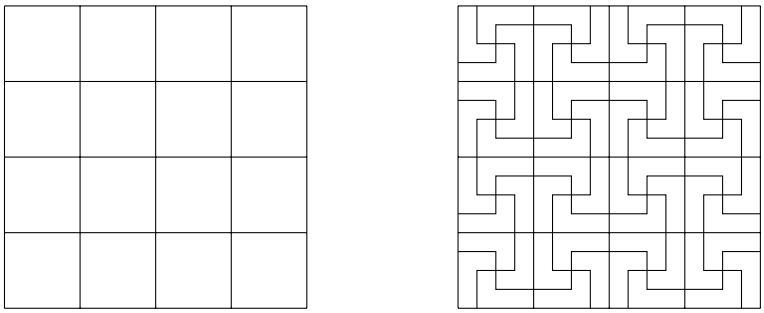


Figura 12.21: Types of lattices in $\mathbb{R}^2$

Notación y Grupos Espaciales	Grupo Puntual	Tipo de Reticulado	Reflexiones o Reflexiones Deslizantes?
p1	$\mathbb{Z}_1$	paralelógramo	ninguna
p2	$\mathbb{Z}_2$	paralelógramo	ninguna
p3	$\mathbb{Z}_3$	hexagonal	ninguna
p4	$\mathbb{Z}_4$	cuadrada	ninguna
p6	$\mathbb{Z}_6$	hexagonal	ninguna
pm	D_1	rectangular	reflexiones
pg	D_1	rectangular	reflexiones deslizantes
cm	D_1	rómbica	ambas
pmm	D_2	rectangular	reflexiones
pmg	D_2	rectangular	reflexiones deslizantes
pgg	D_2	rectangular	ambas
c2mm	D_2	rómbica	ambas
p3m1, p31m	D_3	hexagonal	ambas
p4m, p4g	D_4	cuadrada	ambas
p6m	D_6	hexagonal	ambas

Cuadro 12.22: The 17 wallpaper groups

Teorema 12.23. *Hay exactamente 17 grupos critalográficos planos.*



p4m *p4g*

Figura 12.24: Los grupos cristalográficos p4m y p4g

Los 17 grupos critalográficos planos están listados en la Tabla 12.22. Los grupos p3m1 y p31m pueden ser distinguidos según si todos sus centros triples están en los ejes de reflexión: los de p3m1 deben estar, mientras los de p31m puede que no. Similarmente, los centros cuuádruples de p4m deben estar en los ejes de reflexión mientras los de p4g no necesariamente (Figura 12.24). La demostración completa de este teorema se puede encontar en varias de las referencias la final de este capítulo, incluyendo [5], [6], [10], y [11].

Sage Aún no hemos incluido material Sage para este capítulo.

Nota Histórica

Los grupos de simetría han intrigado a matemáticos por mucho tiempo. Leonardo da Vinci fue probablemente la primera persona en conocer todos los grupos puntuales. En el Congreso Internacional de Matemáticos en 1900, David Hilbert dio una ahora famosa charla indicando los 23 problemas apra guiar las

matemáticas en el siglo XX. El problema 18 de Hilbertpreguntaba si los grupos critalograficos en dimensión n serían siempre un número finito. En 1910, L. Bieberbach demostró que los grupos cristalográficos son un número finito en cada dimensión. Descubrir cuñantos de estos grupos existen en cada dimensión es harina de otro costal. En $\mathbb{R}^3$ hay 230 grupos espaciales diferentes; en $\mathbb{R}^4$ hay 4783. Nadie ha sido capaz de calcular el número de grupos espaciales para $\mathbb{R}^5$ y más allá. Es interesante notar que los grupos cristalográficos fueron encontrados matemáticamente para $\mathbb{R}^3$ antes de que los 230 diferentes tipos de cristales hubieran sido descubiertos en la naturaleza.

12.3 Ejercicios

1. Demuestre la identidad

$$\langle \mathbf{x}, \mathbf{y} \rangle = \frac{1}{2} \left[\|\mathbf{x} + \mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 \right].$$

2. Muestre que $O(n)$ es un grupo.

3. Demuestre que las siguientes matrices son ortogonales. ¿Está alguna de estas matrices en $SO(n)$?

(a)
$$\begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$$

(b)
$$\begin{pmatrix} 1/\sqrt{5} & 2/\sqrt{5} \\ -2/\sqrt{5} & 1/\sqrt{5} \end{pmatrix}$$

(c)
$$\begin{pmatrix} 4/\sqrt{5} & 0 & 3/\sqrt{5} \\ -3/\sqrt{5} & 0 & 4/\sqrt{5} \\ 0 & -1 & 0 \end{pmatrix}$$

(d)
$$\begin{pmatrix} 1/3 & 2/3 & -2/3 \\ -2/3 & 2/3 & 1/3 \\ -2/3 & 1/3 & 2/3 \end{pmatrix}$$

4. Determine el grupo de simetría de cada una de las figuras en la Figura 12.25.

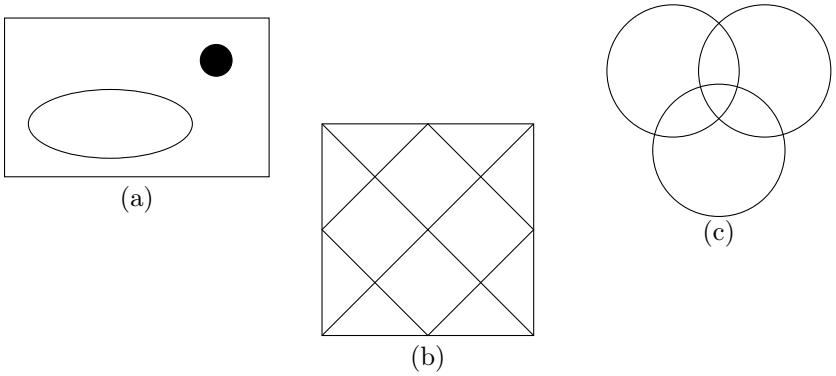


Figura 12.25

5. Sean $\mathbf{x}$, $\mathbf{y}$, y $\mathbf{w}$ vectores en $\mathbb{R}^n$ y $\alpha \in \mathbb{R}$. Demuestre las siguientes propiedades de los productos internos.

(a) $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$.

(b) $\langle \mathbf{x}, \mathbf{y} + \mathbf{w} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{x}, \mathbf{w} \rangle$.

(c) $\langle \alpha\mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{x}, \alpha\mathbf{y} \rangle = \alpha \langle \mathbf{x}, \mathbf{y} \rangle$.

(d) $\langle \mathbf{x}, \mathbf{x} \rangle \geq 0$ con igualdad exactamente cuando $\mathbf{x} = 0$.

(e) If $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ para todo $\mathbf{x}$ en $\mathbb{R}^n$, then $\mathbf{y} = 0$.

6. Compruebe que

$$E(n) = \{(A, \mathbf{x}) : A \in O(n) \text{ y } \mathbf{x} \in \mathbb{R}^n\}$$

es un grupo.

7. Demuestre que $\{(2,1),(1,1)\}$ y $\{(12,5),(7,3)\}$ son bases para el mismo reticulado.

8. Sea G un subgrupo de $E(2)$ y supongamos que T es el subgrupo de traslaciones de G. Demuestre que el grupo puntual de G es isomorfo a G/T.

9. Sea $A \in SL_2(\mathbb{R})$ y supongamos que los vectores $\mathbf{x}$ y $\mathbf{y}$ forman dos lados de un paralelogramo en $\mathbb{R}^2$. Demuestre que el área de este paralelogramo es la misma la del paralelogramo de lados $A\mathbf{x}$ y $A\mathbf{y}$.

10. Demuestre que $SO(n)$ es un subgrupo normal de $O(n)$.

11. Muestre que cualquier isometría f en $\mathbb{R}^n$ es una función inyectiva

12. Demuestre o refute: Un elemento en $E(2)$ de la forma $(A, \mathbf{x})$, donde $\mathbf{x} \neq 0$, tiene orden infinito.

13. Demuestre o refute: Existe un subgrupo abeliano infinito de $O(n)$.

14. Sea $\mathbf{x} = (x_1, x_2)$ un punto del círculo unitario en $\mathbb{R}^2$; es decir, $x_1^2 + x_2^2 = 1$. Si $A \in O(2)$, muestre que $A\mathbf{x}$ también pertenece al círculo unitario.

15. Sea G un grupo con un subgrupo H (no necesariamente normal) y un subgrupo normal N. Entonces G es un ***producto semidirecto*** de N por H si

- $H \cap N = \{\text{id}\}$;
- $HN = G$.

Muestre que se cumple lo siguiente.

(a) S_3 es el producto semidirecto de A_3 por $H = \{(1), (12)\}$.

(b) El grupo de cuaterniones, Q_8, no puede ser escrito como un producto semidirecto (no trivial).

(c) $E(2)$ es el producto semidirecto de $O(2)$ por H, donde H consiste de todas las traslaciones en $\mathbb{R}^2$.

16. Determine cuál de los 17 grupos cristalográficos del plano preserva la simetría del patrón en la Figura 12.16.

17. Determine cuál de los 17 grupos cristalográficos del plano preserva la simetría del patrón en la Figura 12.26.

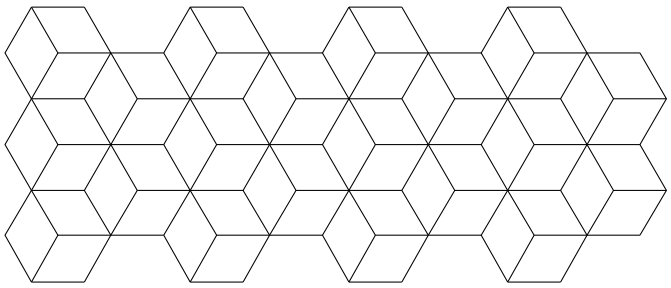


Figura 12.26

18. Encuentre el grupo de rotaciones de un dodecahedro.

19. Para cada uno de los 17 grupos cristalográficos del plano, dibuje un patrón mural que tenga ese grupo como grupo de simetría.

12.4 Referencias y Lecturas Recomendadas

[1] Coxeter, H. M. and Moser, W. O. J. *Generators and Relations for Discrete Groups*, 3rd ed. Springer-Verlag, New York, 1972.

[2] Grove, L. C. and Benson, C. T. *Finite Reflection Groups.* 2nd ed. Springer-Verlag, New York, 1985.

[3] Hiller, H. "Crystallography and Cohomology of Groups," *American Mathematical Monthly* **93** (1986), 765–79.

[4] Lockwood, E. H. and Macmillan, R. H. *Geometric Symmetry.* Cambridge University Press, Cambridge, 1978.

[5] Mackiw, G. *Applications of Abstract Algebra.* Wiley, New York, 1985.

[6] Martin, G. *Transformation Groups: An Introduction to Symmetry.* Springer-Verlag, New York, 1982.

[7] Milnor, J. "Hilbert's Problem 18: On Crystallographic Groups, Fundamental Domains, and Sphere Packing," *t Proceedings of Symposia in Pure Mathematics* **18**, American Mathematical Society, 1976.

[8] Phillips, F. C. *An Introduction to Crystallography.* 4th ed. Wiley, New York, 1971.

[9] Rose, B. I. and Stafford, R. D. "An Elementary Course in Mathematical Symmetry," *American Mathematical Monthly* **88** (1980), 54–64.

[10] Schattschneider, D. "The Plane Symmetry Groups: Their Recognition and Their Notation," *American Mathematical Monthly* **85**(1978), 439–50.

[11] Schwarzenberger, R. L. "The 17 Plane Symmetry Groups," *Mathematical Gazette* **58**(1974), 123–31.

[12] Weyl, H. *Symmetry.* Princeton University Press, Princeton, NJ, 1952.

12.5 Sage

No hay material Sage para este capítulo.

12.6 Ejercicios en Sage

No hay ejercicios en Sage para este capítulo.

13

La Estructura de Grupos

El objetivo máximo de la teoría de grupos es el de clasificar todos los grupos módulo ismorfismo; es decir, dado un grupo particular, queremos ser capaces de identificarlo con un grupo conocido por medio de un isomorfismo. Por ejemplo, ya demostramos que cualquier grupo cíclico finito de orden n es isomorfo a $\mathbb{Z}_n$; luego, "conocemos" todos los grupos cíclicos finitos. Probablemente no es razonable suponer que jamás vayamos a conocer todos los gruos; sin embargo, podemos clasificar ciertos tipos de grupos o distinguir entre grupos en casos especiales.

En este capítulo caracterizaremos todos los grupos abelianos finitos. También investigaremos grupos con sucesiones de subgrupos. Si un grupo contiene una sucesión de subgrupos, digamos

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\},$$

donde cada H_i es normal en H_{i+1} y cada uno de los grupos cociente H_{i+1}/H_i es abelian, entonces G es un grupo soluble. Además de permitirnos distinguir entre ciertas clases de grupos, los grupos solubles resultan tener papel central en el estudio de las soluciones de ecuaciones polinomiales.

13.1 Grupos Abelianos Finitos

Estudiando los grupos cíclicos descubrimos que todo grupo de orden primo es isomorfo a $\mathbb{Z}_p$, done p es un número primo. También establecimos que $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ cuando $\text{mcd}(m, n) = 1$. De hecho, hay mucho más. Todo grupo abeliano finito es isomorfo a un producto directo de grupos cíclicos cuyos órdenes son potencias de primos; es decir, todo grupo abeliano finito es isomorfo a un grupo del tipo

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}},$$

donde cada p_k es primo (no necesariamente distintos).

Primero examinemos una leve generalización de los grupos abelianos finitos. Supongamos que G es un grupo y sea $\{g_i\}$ un conjunto de elementos en G, con i en algún conjunto de índices I (no necesariamente finito). El menor subgrupo de G que contenga todos los g_i es el subgrupo de G ***generado*** por los g_i. Si este subgrupo de G es todo G, entonces G es generado por el conjunto $\{g_i : i \in I\}$. En este caso diremos que los g_i son ***generadores*** de G. Si existe un conjunto finito $\{g_i : i \in I\}$ que genere a G, entonces G es ***finitamente generado***.

Ejemplo 13.1. Obviamente, todos los grupos finitos son finitamente generados. Por ejemplo, el grupo S_3 es generado por las permutaciones (12) y (123). El grupo $\mathbb{Z} \times \mathbb{Z}_n$ es un grupo infinito pero es finitamente generado por $\{(1, 0), (0, 1)\}$.

Ejemplo 13.2. No todos los grupos son finitamente generados. Consideremos los números racionales $\mathbb{Q}$ con la suma. Supongamos que $\mathbb{Q}$ es finitamente generado con generadores $p_1/q_1, \ldots, p_n/q_n$, donde cada p_i/q_i es una fracción reducida. Sea p un primo que no divide a ninguno de los denominadores $q_1, \ldots, q_n$. Afirmamos que $1/p$ no puede estar en el subgrupo de $\mathbb{Q}$ generado por $p_1/q_1, \ldots, p_n/q_n$, pues p no divide al denominador de ningún elemento de este subgrupo. Esto es fácil de ver pues la suma de dos generadores cualquiera es

$$p_i/q_i + p_j/q_j = (p_i q_j + p_j q_i)/(q_i q_j).$$

Proposición 13.3. *Sea H el subgrupo de un grupo G generado por $\{g_i \in G : i \in I\}$. Entonces $h \in H$ si y solo si es un producto de la forma*

$$h = g_{i_1}^{\alpha_1} \cdots g_{i_n}^{\alpha_n},$$

donde los g_{i_k} no son necesariamente diferentes.

Demostración. Sea K el conjunto de todos los productos de la forma $g_{i_1}^{\alpha_1} \cdots g_{i_n}^{\alpha_n}$, donde los g_{i_k} no son necesariamente diferentes. Ciertamente K es un subconjunto de H. Solo debemos mostrar que K es un subgrupo de G. Si es así, entonces $K = H$, pues H es el menor subgrupo que contiene todos los g_is.

Claramente, K es cerrado bajo la operación del grupo. Como $g_i^0 = 1$, la identidad está en K. Falta mostrar que el inverso de un elemento $g = g_{i_1}^{k_1} \cdots g_{i_n}^{k_n}$ en K también está en K. Pero,

$$g^{-1} = (g_{i_1}^{k_1} \cdots g_{i_n}^{k_n})^{-1} = (g_{i_n}^{-k_n} \cdots g_{i_1}^{-k_1}). \qquad \square$$

El motivo por el que potencias de un cierto g_i podrían ocurrir varias veces en el producto es que el grupo podría no ser abeliano. Pero, si el grupo es abeliano, entonces los g_i solo necesitan aparecer una vez. Por ejemplo, un producto como $a^{-3}b^5a^7$ en un grupo abeliano siempre se puede simplificar (en este caso, como a^4b^5).

Nos concentraremos ahora en los grupos abelianos finitos. Podemos expresar cualquier grupo abeliao finito como un producto directo finito de grupos cíclicos. Más específicamente, si p es un número primo, diremos que un grupo G es un ***p*-grupo** si todo elemento en G tiene como su orden una potencia de p. Por ejemplo, tanto $\mathbb{Z}_2 \times \mathbb{Z}_2$ como $\mathbb{Z}_4$ son 2-grupos, mientras $\mathbb{Z}_{27}$ es un 3-group. Demostraremos el Teorema Fundamental de los Grupos Abelianos Finitos que nos dice que todo grupo abeliano finito es isomorfo a un producto directo de p-groups. cíclicos

Teorema 13.4 (Teorema Fundamental de los Grupos Abelianos Finitos)**.** *Todo grupo abeliano finito G es isomorfo a un producto directo de grupos cíclicos de la forma*

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}}$$

acá los p_i son primos (no necesariamente diferentes).

Ejemplo 13.5. Supongamos que queremos clasificar todos los grupos abelianos de orden $540 = 2^2 \cdot 3^3 \cdot 5$. El Teorema Fundamental de los Grupos Abelianos Finitos nos dice que tenemos las siguientes seis posibilidades.

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$;
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$;
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$;
- $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$;

- $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$;
- $\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$.

La demostración del Teorema Fundamental de los Grupos Abelianos Finitos depende de varios lemas.

Lema 13.6. *Sea G un grupo abeliano finito de orden n. Si p es un primo que divide a n, entonces G contiene un elemento de orden p.*

Demostración. Demostraremos este lema por inducción. Si $n = 1$, entonces no hay nada que demostrar. Ahora supongamos que el orden de G es n y que el lema es verdadero para todos los grupos de orden k, donde $k < n$. Más aún, sea p un primo que divide a n.

Si G no tiene subgrupos propios no triviales, entonces $G = \langle a \rangle$, donde a es cualquier elemento distinto de la identidad. Por el Ejercicio 4.4.39, el orden de G es primo. Como p divide a n, sabemos que $p = n$, y G contiene $p - 1$ elementos de orden p.

Ahora supongamos que G contiene un subgrupo no trivial propio H. Entonces $1 < |H| < n$. Si $p \mid |H|$, entonces H contiene un elemento de orden p por la hipótesis de inducción y el lema se cumple para G. Supongamos que p no divide el orden de H. Como G es abeliano, H es un subgrupo normal de G, y $|G| = |H| \cdot |G/H|$. De manera que p divide a $|G/H|$. Como $|G/H| < |G| = n$, sabemos que G/H contiene un elemento aH de orden p por la hipótesis de inducción. Luego,

$$H = (aH)^p = a^p H,$$

y $a^p \in H$ pero $a \notin H$. Si $|H| = r$, entonces p y r son relativamente primos, y existen enteros s y t tales que $sp + tr = 1$. Además, el orden de a^p divide a r, y $(a^p)^r = (a^r)^p = 1$.

Afirmamos que a^r tiene orden p. Debemos mostrar que $a^r \neq 1$. Supongamos que $a^r = 1$. Entonces

$$\begin{aligned} a &= a^{sp+tr} \\ &= a^{sp} a^{tr} \\ &= (a^p)^s (a^r)^t \\ &= (a^p)^s 1 \\ &= (a^p)^s. \end{aligned}$$

Como $a^p \in H$, tenemos $a = (a^p)^s \in H$, lo que es una contradicción. Por lo tanto, $a^r \neq 1$ es un elemento de orden p in G. □

El Lema 13.6 es un caso particular del Teorema de Cauchy (Teorema 15.1, que dice que si G es un grupo finito y p es un primoque divide el orden de G, entonces G contiene un subgrupo de orden p. Demostraremos el Teorema de Cauchy en el Capítulo 15.

Lema 13.7. *Un grupo abeliano finito es un p-grupo si y solo si su orden es una potencia de p.*

Demostración. Si $|G| = p^n$ entonces, por el teorema de Lagrange, el orden de cualquier $g \in G$ divide a p^n, y por lo tantoes una potencia de p. Recíprocamente, si $|G|$ no es una potencia de p, entonces tiene algún otro divisor primo q, y por el Lema 13.6, G tiene un elemento de orden q por lo que no es un p-grupo. □

Lema 13.8. *Sea G un grupo abeliano finito de orden $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, con $p_1, \ldots, p_k$ primos distintos y $\alpha_1, \alpha_2, \ldots, \alpha_k$ enteros positivos. Entonces G es el producto directo interno de subgrupos $G_1, G_2, \ldots, G_k$, donde G_i es el subgrupo de G que consiste de todos los elementos de orden p_i^k para algún entero k.*

DEMOSTRACIÓN. Como G es un grupo abeliano, tenemos que G_i es un subgrupo de G para $i = 1, \ldots, n$. Como la identidad tiene orden $p_i^0 = 1$, sabemos que $1 \in G_i$. Si $g \in G_i$ tiene orden p_i^r, entonces g^{-1} también debe tener orden p_i^r. Finalmente, si $h \in G_i$ tiene orden p_i^s, entonces

$$(gh)^{p_i^t} = g^{p_i^t} h^{p_i^t} = 1 \cdot 1 = 1,$$

donde t es el mayor entre r y s.

Debemos mostrar que

$$G = G_1 G_2 \cdots G_n$$

y $G_i \cap G_j = \{1\}$ para $i \neq j$. Supongamos que $g_1 \in G_1$ está en el subgrupo generado por $G_2, G_3, \ldots, G_k$. Entonces $g_1 = g_2 g_3 \cdots g_k$ para $g_i \in G_i$. Como g_i tiene orden p^{α_i}, sabemos que $g_i^{p^{\alpha_i}} = 1$ para $i = 2, 3, \ldots, k$, y $g_1^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}} = 1$. Como el orden de g_1 es una potencia de p_1 y $\mcd(p_1, p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = 1$, tenemos que $g_1 = 1$ y la intersección de G_1 con cualquiera de los subgrupos $G_2, G_3, \ldots, G_k$ ies la identidad. Un argumento similar muestra que $G_i \cap G_j = \{1\}$ para $i \neq j$. Luego, $G_1 G_2 \cdots G_n$ es un producto directo interno de subgrupos. Como

$$|G_1 G_2 \cdots G_k| = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = |G|,$$

tenemos que $G = G_1 G_2 \cdots G_k$. □

Nos falta determinar la posible estructura de cada uno de los p_i-grupos G_i en el Lema 13.8.

Lema 13.9. *Sea G un p-grupo abeliano finito y supongamos que $g \in G$ tiene orden maximal. Entonces G es isomorfo a $\langle g \rangle \times H$ para algún subgrupo H de G.*

DEMOSTRACIÓN. Por el Lema 13.7, podemos suponer que el orden de G es p^n. Procederemos por inducción en n. Si $n = 1$, entonces G es cíclico de orden p y debe estar generado por g. Supongamos ahora que el lema se cumple para todos los enteros k con $1 \leq k < n$ y sea g de orden maximal en G, digamos $|g| = p^m$. Entonces $a^{p^m} = e$ para todo $a \in G$. Ahora elijamos h en G tal que $h \notin \langle g \rangle$, donde h tiene el menor orden posible. Ciertamente podemos suponer que tal h existe; de otra manera, $G = \langle g \rangle$ y estamos listos. Sea $H = \langle h \rangle$.

Afirmamos que $\langle g \rangle \cap H = \{e\}$. Es suficiente con mostrar que $|H| = p$. Como $|h^p| = |h|/p$, el orden de h^p es menor que el orden de h y debe estar en $\langle g \rangle$ por la minimalidad del orden de h; es decir, $h^p = g^r$ para algún r. Luego,

$$(g^r)^{p^{m-1}} = (h^p)^{p^{m-1}} = h^{p^m} = e,$$

y el orden de g^r es menor o igual a p^{m-1}. Por lo tanto, g^r no puede generar $\langle g \rangle$. Notemos que p debe ser un divisor de r, digamos $r = ps$, y $h^p = g^r = g^{ps}$. Definamos a como $g^{-s}h$. Entonces a no puede estar en $\langle g \rangle$; de otra manera, h también estaría en $\langle g \rangle$. Además,

$$a^p = g^{-sp} h^p = g^{-r} h^p = h^{-p} h^p = e.$$

Hemos formado un elemento a de orden p tal que $a \notin \langle g \rangle$. Como h fue elegido de orden minimal entre todos los elementos fuera de $\langle g \rangle$, $|H| = p$.

Ahora mostraremos que el orden de gH en el grupo cociente G/H debe ser el mismo que el orden de g en G. Si $|gH| < |g| = p^m$, entonces

$$H = (gH)^{p^{m-1}} = g^{p^{m-1}} H;$$

luego, $g^{p^{m-1}}$ está en $\langle g\rangle \cap H = \{e\}$, lo que contradice el hecho de que el orden de g es p^m. Por lo tanto, gH tiene orden maximal en G/H. Por el Teorema de Correspondencia y la hipótesis de inducción ,

$$G/H \cong \langle gH\rangle \times K/H$$

para algún subgrupo K de G que contiene a H. Afirmamos que $\langle g\rangle \cap K = \{e\}$. Si $b \in \langle g\rangle \cap K$, entonces $bH \in \langle gH\rangle \cap K/H = \{H\}$ y $b \in \langle g\rangle \cap H = \{e\}$. Concluimos que $G = \langle g\rangle K$ implica que $G \cong \langle g\rangle \times K$. □

La demostración del Teorema Fundamental de los Grupos Abelianos Finitos sigue rápidamente del Lema 13.9. Procediendo por inducción en el orden del grupo, supongamos que G es un grupo abeliano finito y sea g un elemento de orden maximal en G. Si $\langle g\rangle = G$, estamos listos; de lo contrario, $G \cong \mathbb{Z}_{|g|} \times H$ para algún subgrupo H contenido en G por el lema. Como $|H| < |G|$, podemos usar la hipótesis de inducción.

Ahora enunciamos el teorema más general que vale para todos los grupos abelianos finitamente generados. La demostración de este teorema se puede encontrar en cualquiera de las referencias al final del capítulo.

Teorema 13.10 (Teorema Fundamental de los Grupos Abelianos Finitamente Generados)**.** *Todo grupo abeliano finitamente generado G es isomorfo a un producto directo de grupos cíclicos de la forma*

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

donde los p_i son primos (no necesariamente distintos).

13.2 Grupos Solubles

Una ***serie subnormal*** de un grupo G es una sucesión finita de subgrupos

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\},$$

donde H_i es un subgrupo normal de H_{i+1}. Si cada subgrupo H_i es normal en G, entonces la serie se llama ***serie normal***. El ***largo*** de una serie subnormal o normal es el número de inclusiones propias.

Ejemplo 13.11. Toda serie de subgrupos de un grupo abeliano es una serie normal. Considere las siguientes series de grupos:

$$\mathbb{Z} \supset 9\mathbb{Z} \supset 45\mathbb{Z} \supset 180\mathbb{Z} \supset \{0\},$$
$$\mathbb{Z}_{24} \supset \langle 2\rangle \supset \langle 6\rangle \supset \langle 12\rangle \supset \{0\}.$$

Ejemplo 13.12. Una serie subnormal no es necesariamente una serie normal. Considere la sguiente serie subnormal del grupo D_4:

$$D_4 \supset \{(1), (12)(34), (13)(24), (14)(23)\} \supset \{(1), (12)(34)\} \supset \{(1)\}.$$

El subgrupo $\{(1), (12)(34)\}$ no es normal en D_4; en consecuencia, esta no es una serie normal.

Una serie subnormal (normal) $\{K_j\}$ es un ***refinamiento de una serie subnormal (normal)*** $\{H_i\}$ si $\{H_i\} \subset \{K_j\}$. Es decir, cada H_i es uno de los K_j.

Ejemplo 13.13. Las serie

$$\mathbb{Z} \supset 3\mathbb{Z} \supset 9\mathbb{Z} \supset 45\mathbb{Z} \supset 90\mathbb{Z} \supset 180\mathbb{Z} \supset \{0\}$$

es un refinamiento de la serie

$$\mathbb{Z} \supset 9\mathbb{Z} \supset 45\mathbb{Z} \supset 180\mathbb{Z} \supset \{0\}.$$

La mejor forma de estudiar una serie subnormal o normal de subgrupos, $\{H_i\}$ de G, es realmente estudiar los grupos cociente H_{i+1}/H_i. Se dice que dos series subnormales (normales) $\{H_i\}$ y $\{K_j\}$ de un grupo G son ***isomorfas*** si existe una correspondencia 1-1 entre las colecciones de grupos cociente $\{H_{i+1}/H_i\}$ y $\{K_{j+1}/K_j\}$.

Ejemplo 13.14. Las dos series normales

$$\mathbb{Z}_{60} \supset \langle 3\rangle \supset \langle 15\rangle \supset \{0\}$$
$$\mathbb{Z}_{60} \supset \langle 4\rangle \supset \langle 20\rangle \supset \{0\}$$

del grupo $\mathbb{Z}_{60}$ son isomorfas pues

$$\mathbb{Z}_{60}/\langle 3\rangle \cong \langle 20\rangle/\{0\} \cong \mathbb{Z}_3$$
$$\langle 3\rangle/\langle 15\rangle \cong \langle 4\rangle/\langle 20\rangle \cong \mathbb{Z}_5$$
$$\langle 15\rangle/\{0\} \cong \mathbb{Z}_{60}/\langle 4\rangle \cong \mathbb{Z}_4.$$

Una serie subnormal $\{H_i\}$ de un grupo G es una ***serie de composición*** si todos los grupos cociente son simples; es decir, ninguno de ellos contiene un subgrupo normal. Una serie normal $\{H_i\}$ de G es una ***serie principal*** si todos los cocientes son simples.

Ejemplo 13.15. El grupo $\mathbb{Z}_{60}$ tiene una serie de composición

$$\mathbb{Z}_{60} \supset \langle 3\rangle \supset \langle 15\rangle \supset \langle 30\rangle \supset \{0\}$$

con grupos cociente

$$\mathbb{Z}_{60}/\langle 3\rangle \cong \mathbb{Z}_3$$
$$\langle 3\rangle/\langle 15\rangle \cong \mathbb{Z}_5$$
$$\langle 15\rangle/\langle 30\rangle \cong \mathbb{Z}_2$$
$$\langle 30\rangle/\{0\} \cong \mathbb{Z}_2.$$

Como $\mathbb{Z}_{60}$ es un grupo abeliano, esta serie es automáticamente una serie principal. Notemos que una serie de composición no es necesariamente única. La serie

$$\mathbb{Z}_{60} \supset \langle 2\rangle \supset \langle 4\rangle \supset \langle 20\rangle \supset \{0\}$$

también es una serie de composición.

Ejemplo 13.16. Para $n \geq 5$, la serie

$$S_n \supset A_n \supset \{(1)\}$$

es una serie de composición para S_n pues $S_n/A_n \cong \mathbb{Z}_2$ y A_n es simple.

Ejemplo 13.17. No todo grupo tiene una serie de composición o una serie principal. Supongamos que

$$\{0\} = H_0 \subset H_1 \subset \cdots \subset H_{n-1} \subset H_n = \mathbb{Z}$$

es ua serie subnormal de los enteros bajo la suma. Entonces H_1 debe ser de la forma $k\mathbb{Z}$ para algún $k \in \mathbb{N}$. En ese caso $H_1/H_0 \cong k\mathbb{Z}$ es un grupo cíclico infinito con muchos subgrupos normales propios no triviales.

Si bien una serie de composición no es necesariamente única como en el caso de $\mathbb{Z}_{60}$, resulta que dos series de composición cualquiera están relacionadas. Los cocientes de las dos series de composición para $\mathbb{Z}_{60}$ son $\mathbb{Z}_2$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, y $\mathbb{Z}_5$; es decir, las dos series de composición son isomorfasEl Teorema de Jordan-Hölder dice que esto siempre se cumple.

Teorema 13.18 (Jordan-Hölder)**.** *Any two composition series of G are isomorphic.*

Demostración. We shall employ mathematical induction on the length of the composition series. If the length of a composition series is 1, then G must be a simple group. In this case any two composition series are isomorphic.

Suppose now that the theorem is true for all groups having a composition series of length k, where $1 \leq k < n$. Let

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\}$$
$$G = K_m \supset K_{m-1} \supset \cdots \supset K_1 \supset K_0 = \{e\}$$

be two composition series for G. We can form two new subnormal series for G since $H_i \cap K_{m-1}$ is normal in $H_{i+1} \cap K_{m-1}$ and $K_j \cap H_{n-1}$ is normal in $K_{j+1} \cap H_{n-1}$:

$$G = H_n \supset H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_0 \cap K_{m-1} = \{e\}$$
$$G = K_m \supset K_{m-1} \supset K_{m-1} \cap H_{n-1} \supset \cdots \supset K_0 \cap H_{n-1} = \{e\}.$$

Since $H_i \cap K_{m-1}$ is normal in $H_{i+1} \cap K_{m-1}$, the Second Isomorphism Theorem (Theorem 11.12) implies that

$$\begin{aligned}(H_{i+1} \cap K_{m-1})/(H_i \cap K_{m-1}) &= (H_{i+1} \cap K_{m-1})/(H_i \cap (H_{i+1} \cap K_{m-1})) \\ &\cong H_i(H_{i+1} \cap K_{m-1})/H_i,\end{aligned}$$

where H_i is normal in $H_i(H_{i+1} \cap K_{m-1})$. Since $\{H_i\}$ is a composition series, H_{i+1}/H_i must be simple; consequently, $H_i(H_{i+1} \cap K_{m-1})/H_i$ is either H_{i+1}/H_i or H_i/H_i. That is, $H_i(H_{i+1} \cap K_{m-1})$ must be either H_i or H_{i+1}. Removing any nonproper inclusions from the series

$$H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_0 \cap K_{m-1} = \{e\},$$

we have a composition series for H_{n-1}. Our induction hypothesis says that this series must be equivalent to the composition series

$$H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\}.$$

Hence, the composition series

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\}$$

and

$$G = H_n \supset H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_0 \cap K_{m-1} = \{e\}$$

are equivalent. If $H_{n-1} = K_{m-1}$, then the composition series $\{H_i\}$ and $\{K_j\}$ are equivalent and we are done; otherwise, $H_{n-1}K_{m-1}$ is a normal subgroup of G properly containing H_{n-1}. In this case $H_{n-1}K_{m-1} = G$ and we can apply the Second Isomorphism Theorem once again; that is,

$$K_{m-1}/(K_{m-1} \cap H_{n-1}) \cong (H_{n-1}K_{m-1})/H_{n-1} = G/H_{n-1}.$$

Therefore,

$$G = H_n \supset H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_0 \cap K_{m-1} = \{e\}$$

and

$$G = K_m \supset K_{m-1} \supset K_{m-1} \cap H_{n-1} \supset \cdots \supset K_0 \cap H_{n-1} = \{e\}$$

are equivalent and the proof of the theorem is complete. □

A group G is ***solvable*** if it has a subnormal series $\{H_i\}$ such that all of the factor groups H_{i+1}/H_i are abelian. Solvable groups will play a fundamental role when we study Galois theory and the solution of polynomial equations.

Ejemplo 13.19. The group S_4 is solvable since

$$S_4 \supset A_4 \supset \{(1), (12)(34), (13)(24), (14)(23)\} \supset \{(1)\}$$

has abelian factor groups; however, for $n \geq 5$ the series

$$S_n \supset A_n \supset \{(1)\}$$

is a composition series for S_n with a nonabelian factor group. Therefore, S_n is not a solvable group for $n \geq 5$.

Sage Sage is able to create direct products of cyclic groups, though they are realized as permutation groups. This is a situation that should improve. However, with a classification of finite abelian groups, we can describe how to construct in Sage every group of order less than 16.

13.3 Ejercicios

1. Encuentre todos los grupos abelianos de orden menor o igual a 40.

2. Encuentre todos los grupos abelianos de orden 200.

3. Encuentre todos los grupos abelianos de orden 720.

4. Encuentre todas las series de composición para cada uno de los siguientes grupos.

(a) $\mathbb{Z}_{12}$
(b) $\mathbb{Z}_{48}$
(c) Los cuaterniones, Q_8
(d) D_4
(e) $S_3 \times \mathbb{Z}_4$
(f) S_4
(g) S_n, $n \geq 5$
(h) $\mathbb{Q}$

5. Demuestre que el producto directo infinito $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$ no es finitamente generado.

6. Sea G un grupo abeliano de orden m. Si n divide a m, demuestre que G tiene un subgrupo de orden n.

7. Un grupo G es un ***grupo de torsión*** si todo elemento de G tiene orden finito. Demuestre que un grupo de torsión abeliano finitamente generado tiene que ser finito.

8. Sean G, H, y K grupos abelianos finitamente generados. Muestre que si $G \times H \cong G \times K$, entonces $H \cong K$. Encuentre un contraejemplo para mostrar que esto no es verdadero en general.

9. Sean G y H grupos solubles. Muestre que $G \times H$ también es soluble.

10. Si G tiene una serie de composición (principal) y si N es un subgrupo normal propio de G, muestre que existe una serie de composición (principal) que contiene a N.

11. Demuestre o refute: Sea N un subgrupo normal de G. Si N y G/N tienen series de composición, entonces G también tiene serie de composición.

12. Sea N un subgrupo normal de G. Si N y G/N son grupos solubles, muestre que G también es un grupo soluble.

13. Demuestre que G es un grupo soluble si y solo si G tiene una serie de subgrupos

$$G = P_n \supset P_{n-1} \supset \cdots \supset P_1 \supset P_0 = \{e\}$$

donde P_i es normal en P_{i+1} y el orden de P_{i+1}/P_i es primo.

14. Sea G un grupo soluble. Demuestre que cualquier subgrupo de G también es soluble.

15. Sea G un grupo soluble y N un subgrupo normal de G. Demuestre que G/N es soluble.

16. Demuestre que D_n es soluble para todo entero n.

17. Supongamos que G tiene una serie de composición. Si N es un subgrupo normal de G, muestre que N y G/N también tienen series de composición.

18. Sea G un p-grupo cíclico con subgrupos H y K. Demuestre que ya sea H está contenido en K o K está contenido en H.

19. Supuongamos que G es un grupo soluble de orden $n \geq 2$. Muestre que G contiene un subgrupo normal abeliano no trivial.

20. Recuerde que el ***subgrupo conmutador*** G' de un grupo G está definido como el subgrupo de G generado por los elementos de la forma $a^{-1}b^{-1}ab$ para $a, b \in G$. Podemos definir una serie de subgrupos de G como $G^{(0)} = G$, $G^{(1)} = G'$, y $G^{(i+1)} = (G^{(i)})'$.

(a) Demuestre que $G^{(i+1)}$ es normal en $(G^{(i)})'$. La serie de subgrupos

$$G^{(0)} = G \supset G^{(1)} \supset G^{(2)} \supset \cdots$$

se llama ***serie derivada*** de G.

(b) Muestre que G es soluble si y solo si $G^{(n)} = \{e\}$ para algún entero n.

21. Supongamos que G es un grupo soluble de orden $n \geq 2$. Muestre que G tiene un grupo cociente abeliano no trivial.

22. (Lema de Zassenhaus) Sean H y K subgrupos de un grupo G. Supongamos admás que H^* y K^* son subgrupos normales de H y K respectivamente. Entonces

(a) $H^*(H \cap K^*)$ es un subgrupo normal de $H^*(H \cap K)$.

(b) $K^*(H^* \cap K)$ es un subgrupo normal de $K^*(H \cap K)$.

(c) $H^*(H \cap K)/H^*(H \cap K^*) \cong K^*(H \cap K)/K^*(H^* \cap K) \cong (H \cap K)/(H^* \cap K)(H \cap K^*)$.

23. (Teorema de Schreier) Use el Lema de Zassenhaus para demostrar que dos series subnormales (normales) de un grupo G tienen refinamientos isomorfos.

24. Use el Teorema de Schreier para demostrar el Teorema de Jordan-Hölder.

13.4 Programming Exercises

1. Write a program that will compute all possible abelian groups of order n. What is the largest n for which your program will work?

13.5 Referencias y Lecturas Recomendadas

[1] Hungerford, T. W. *Algebra*. Springer, New York, 1974.

[2] Lang, S. *Algebra*. 3rd ed. Springer, New York, 2002.

[3] Rotman, J. J. *An Introduction to the Theory of Groups*. 4th ed. Springer, New York, 1995.

13.6 Sage

Los grupos cíclicos, y los productos directos de grupos cíclicos, están implementados en Sage como grupos de permutaciones. Pero, estos grupos rápidamente se conviertenen representaciones muy incómodas y debiese haber una mejor forma de trabajar con grupos abelianos finitos en Sage. Postergaremos la discusión de detalles para este capítulo hasta cuando eso ocurra. Sin embargo, ahora que entendemos la noción de grupos isomorfos y la estructura de los grupos abelianos finitos, podemos volver a nuestra misión de clasificar todos los grupos de orden menor a 16.

Clasificación de Grupos Finitos

No se requieren herramientas sofisticadas para entender los grupos de orden $2p$, donde p es un primo impar. Hay dos posibilidades — un grupo cíclico de orden $2p$ y el grupo dihedral de orden $2p$ que es el conjunto de simetrías del polígono regular de p lados. La demostración requiere un razonamiento detallado y cuidadoso, pero los teoremas requeridos se refieren principalmente a los órdenes de los elementos, al Teoremas de Lagrange y a clases laterales. Vea el Ejercicio 9.3.55. Esto resuelve los órdenes $n = 6$, 10, 14.

Para $n = 9$, el Corolario 14.16 que viene, nos dirá que todo grupo de orden p^2 (donde p es un primo) es abeliano. Así, por lo que sabemos de esta sección, las únicas dos posibilidades son $\mathbb{Z}_9$ y $\mathbb{Z}_3 \times \mathbb{Z}_3$. Similarmente, el Teorema 15.10 que viene, nos dirá que todo grupo de orden $n = 15$ es abeliano. Eso solo deja una posibilidad para este orden: $\mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$.

Solo nos quedan dos órdenes para analizar: $n = 8$ y $n = 12$. Las posibilidades son grupos que ya conocemos, con una excepción. Pero el análisis de que estas son las *únicas* posibilidades es más complicado, y no lo completaremos ahora, ni en los próximos capítulos. Notemos que $n = 16$ es aún más complicado, con 14 posibilidades diferentes (lo que explica por qué nos detuvimos

acá).

Para $n = 8$ existen 3 grupos abelianos, y los dos grupos no-abelianos son el grupo dihedral (simetrías de un cuadrado) y el grupo de los cuaterniones.

Para $n = 12$ existen 2 grupos abelianos, y 3 no-abelianos. Conocemos dos de los grupos no-abelianos, el grupo dihedral y en grupo alternante en 4 símbolos (que también es el grupo de simetrías de un tetrahedro). El tercer grupo no-abeliano es un ejemplo de un grupo "dicíclico", que es una familia infinita de grupos, cada uno de orden divisible por 4. El grupo dicíclico de orden 12 también puede ser construido como un "producto semidirecto" de dos grupos cíclicos — esta es una construcción que vale la pena conocer a medida que prosiga sus estudios de teoría de grupos. El grupo dicíclico de orden 8 es el grupo de los cuaterniones y más en general, los grupos dicíclicos de orden 2^k, $k > 2$ se conocen como "grupos de cuaterniones generalizados."

Los siguientes ejemplos le mostrarán como construir algunos de estos grupos, mientras ejercita algunos de los comandos y nos permite a la vez estar más seguros que la siguiente tabla es correcta.

```
S = SymmetricGroup(3)
D = DihedralGroup(3)
S.is_isomorphic(D)
```

```
True
```

```
C3 = CyclicPermutationGroup(3)
C5 = CyclicPermutationGroup(5)
DP = direct_product_permgroups([C3, C5])
C  = CyclicPermutationGroup(15)
DP.is_isomorphic(C)
```

```
True
```

```
Q  = QuaternionGroup()
DI = DiCyclicGroup(2)
Q.is_isomorphic(DI)
```

```
True
```

Grupos de Orden Pequeño como grupos de Permutaciones

Acá listamos construcciones, como grupos de permutaciones en Sage, para todos los grupos de orden menor a 16.

Orden	Construcción	Notas, Alternativas
1	`CyclicPermutationGroup(1)`	Trivial
2	`CyclicPermutationGroup(2)`	`SymmetricGroup(2)`
3	`CyclicPermutationGroup(3)`	Orden primo
4	`CyclicPermutationGroup(4)`	Cíclico
4	`KleinFourGroup()`	Abeliano, no-cíclico
5	`CyclicPermutationGroup(5)`	Orden primo
6	`CyclicPermutationGroup(6)`	Cíclico
6	`SymmetricGroup(3)`	No-abeliano
		`DihedralGroup(3)`
7	`CyclicPermutationGroup(7)`	Orden primo
8	`CyclicPermutationGroup(8)`	Cíclico
8	`C2=CyclicPermutationGroup(2)`	
	`C4=CyclicPermutationGroup(4)`	
	`G=direct_product_permgroups([C2,C4])`	Abeliano, no-cíclico
8	`C2=CyclicPermutationGroup(2)`	
	`G=direct_product_permgroups([C2,C2,C2])`	Abeliano, no-cíclico
8	`DihedralGroup(4)`	No-abeliano
8	`QuaternionGroup()`	Cuaterniones
		`DiCyclicGroup(2)`
9	`CyclicPermutationGroup(9)`	Cíclico
9	`C3=CyclicPermutationGroup(3)`	
	`G=direct_product_permgroups([C3,C3])`	Abeliano, no-cíclico
10	`CyclicPermutationGroup(10)`	Cíclico
10	`DihedralGroup(5)`	No-abeliano
11	`CyclicPermutationGroup(11)`	Orden primo
12	`CyclicPermutationGroup(12)`	Cíclico
12	`C2=CyclicPermutationGroup(2)`	
	`C6=CyclicPermutationGroup(6)`	
	`G=direct_product_permgroups([C2,C6])`	Abeliano, no-cíclico
12	`DihedralGroup(6)`	No-abeliano
12	`AlternatingGroup(4)`	No-abeliano
		Simetrías del tetrahedro
12	`DiCyclicGroup(3)`	No-abeliano
		Producto semidirecto $Z_3 \rtimes Z_4$
13	`CyclicPermutationGroup(13)`	Orden primo
14	`CyclicPermutationGroup(14)`	Cíclico
14	`DihedralGroup(7)`	No-abeliano
15	`CyclicPermutationGroup(15)`	Cyclic

Cuadro 13.20: Los Grupos de Orden **15** o Menos en Sage

13.7 Ejercicios en Sage

No hay ejercicios en Sage para este capítulo.

14

Acciones de Grupo

Las acciones de grupo generalizan la multiplicación en el grupo. Si G es un grupo y X es un conjunto arbitrario, entonces una acción de grupo de un elemento $g \in G$ en un elemento $x \in X$ es un producto, gx, que está en X. Muchos problemas en álgebra se pueden enfrentar mejor con acciones de grupo. Por ejemplo, las demostraciones de los teoremas de Sylow y del Teorema de Conteo de Burnside se entiende de mejor forma si son formuladas en términos de acciones de grupo.

14.1 Grupos Actuando sobre Conjuntos

Sea X un conjunto y sea G un grupo. Una ***acción (izquierda)*** de G sobre X es una función $G \times X \to X$ dade por $(g, x) \mapsto gx$, donde

1. $ex = x$ para todo $x \in X$;
2. $(g_1 g_2)x = g_1(g_2 x)$ para todo $x \in X$ y todo $g_1, g_2 \in G$.

Con estas condiciones X se denomina ***G-conjunto***. Notemos que no pedimos que X esté relacionado con G de ninguna forma. Es verdad que cualquier grupo G actúa sobre cualquier X con la acción trivial $(g, x) \mapsto x$; pero, las acciones de grupo resultan más interesantes si el conjunto X tiene alguna relación con G.

Ejemplo 14.1. Sean $G = GL_2(\mathbb{R})$ y $X = \mathbb{R}^2$. Entonces G actúa sobre X por multiplicación a la izquierda. Si $v \in \mathbb{R}^2$ e I es la matriz identidad, entonces $Iv = v$. Si A y B son matrices invertibles de 2×2, entonces $(AB)v = A(Bv)$ pues la multiplicación de matrices es asociativa.

Ejemplo 14.2. Sea $G = D_4$ el grupo de simentría de un cuadrado. Si $X = \{1, 2, 3, 4\}$ es el conjunto de vértices del cuadrado, entonces podemos considerar D_4 como el conjunto de las siguientes permutaciones:

$$\{(1), (13), (24), (1432), (1234), (12)(34), (14)(23), (13)(24)\}.$$

Los elementos de D_4 actúan sobre X como funciones. La permutación $(13)(24)$ actúa en el vértice 1 enviándolo al vértice 3, en el vértice 2 enviándolo al vértice 4, y así sucesivamente. Es fácil ver que se satisfacen los axiomas de acción de grupo.

En general, si X es cualquier conjunto y G es un subgrupo de S_X, el grupo de todas las permutaciones actuando en X, entonces X es un G-conjunto con la acción de grupo

$$(\sigma, x) \mapsto \sigma(x)$$

para $\sigma \in G$ y $x \in X$.

Ejemplo 14.3. Si tomamos $X = G$, entonces cualquier grupo G actúa sobre sí mismo por medio de su representación regular izquierda; es decir, $(g, x) \mapsto \lambda_g(x) = gx$, donde λ_g es multiplicación a la izquierda:

$$e \cdot x = \lambda_e x = ex = x$$
$$(gh) \cdot x = \lambda_{gh} x = \lambda_g \lambda_h x = \lambda_g(hx) = g \cdot (h \cdot x).$$

Si H es un subgrupo de G, entonces G es un H-conjunto bajo multiplicación izquierda por elementos de H.

Ejemplo 14.4. Sea G un grupo y supongamos que $X = G$. Si H es un subgrupo de G, entonces G es un H-conjunto bajo ***conjugación***; es decir, podemos definir una acción de H sobre G,

$$H \times G \to G,$$

via

$$(h, g) \mapsto hgh^{-1}$$

para $h \in H$ y $g \in G$. Claramente, se satisface el primer axioma para una acción de grupo. Observando que

$$\begin{aligned}(h_1h_2, g) &= h_1h_2g(h_1h_2)^{-1} \\ &= h_1(h_2gh_2^{-1})h_1^{-1} \\ &= (h_1, (h_2, g)),\end{aligned}$$

vemos que la segunda condición también se satisface.

Ejemplo 14.5. Sea H un subgrupo de G y $\mathcal{L}_H$ el conjunto de clases laterales izquierdas de H. El conjunto $\mathcal{L}_H$ es un G-conjunto bajo la acción

$$(g, xH) \mapsto gxH.$$

Nuevamente, es fácil ver que se satisface el primer axioma. Como $(gg')xH = g(g'xH)$, el segundo axioma también es válido.

Si G actúa en un conjunto X y $x, y \in X$, entonces x se dice ***G-equivalente*** a y si existe $g \in G$ tal que $gx = y$. Escribimos $x \sim_G y$ o $x \sim y$ si dos elementos son G-equivalentes.

Proposición 14.6. *Sea X un G-conjunto. Entonces la G-equivalencia es una relación de equivalencia en X.*

Demostración. La relación $\sim$ es refleja pues $ex = x$. Supongamos que $x \sim y$ para $x, y \in X$. Entonces existe g tal que $gx = y$. En ese caso $g^{-1}y = x$; por lo que $y \sim x$. PAra mostrar que la relación es transitiva, supongamos que $x \sim y$ e $y \sim z$. Entonces existen elementos g y h del grupo tale que $gx = y$ y $hy = z$. Así $z = hy = (hg)x$, y x es equivalente a z. □

Si X es un G-conjunto, entonces cualquier parte de la partición de X asociada a la G-equivalencia se denomina ***órbita*** de X bajo G. A la órbita que contiene un elemento x de X la denotaremos como $\mathcal{O}_x$.

Ejemplo 14.7. Sea G el grupo de permutaciones definido por

$$G = \{(1), (123), (132), (45), (123)(45), (132)(45)\}$$

y $X = \{1, 2, 3, 4, 5\}$. Entonces X es un G-conjunto. Las órbitas son $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$ y $\mathcal{O}_4 = \mathcal{O}_5 = \{4, 5\}$.

Ahora supongamos que G es un grupo actuando en un conjunto X y sea g un elemento de G. El ***conjunto de puntos fijos*** de g en X, denotado po X_g, es el conjunto de todos los $x \in X$ tales que $gx = x$. Podemos también estudiar los elementos g del grupo que fijan un $x \in X$*dado*. Este conjunto es más que un subconjunto de G, es un subgrupo. Este subgrupo se llama el ***subgrupo estabilizador*** o ***subgrupo de isotropía*** de x. Denotaremos el subgrupo estabilizador de x por G_x.

Nota 14.8. Es importante recordar que $X_g \subset X$ y $G_x \subset G$.

Ejemplo 14.9. Sea $X = \{1, 2, 3, 4, 5, 6\}$ y supongamos que G es el grupo de permutaciones dado por las permutaciones

$$\{(1), (12)(3456), (35)(46), (12)(3654)\}.$$

Entonces los conjuntos de puntos fijos de X bajo la acción de G son

$$\begin{aligned} X_{(1)} &= X, \\ X_{(35)(46)} &= \{1, 2\}, \\ X_{(12)(3456)} &= X_{(12)(3654)} = \emptyset, \end{aligned}$$

y los subgrupos estabilizadores son

$$\begin{aligned} G_1 = G_2 &= \{(1), (35)(46)\}, \\ G_3 = G_4 = G_5 = G_6 &= \{(1)\}. \end{aligned}$$

Es fácil ver que G_x es un subgrupo de G para cada $x \in X$.

Proposición 14.10. *Sea G un grupo actuando en un conjunto X y sea $x \in X$. El estabilizador de x, G_x, es un subgrupo de G.*

Demostración. Claramente, $e \in G_x$ pues la identidad deja fijo cada elemento en el conjunto X. Sean $g, h \in G_x$. Entonces $gx = x$ y $hx = x$. Entonces $(gh)x = g(hx) = gx = x$; luego, el producto de dos elementos en G_x también está en G_x. Finalmente, si $g \in G_x$, entonces $x = ex = (g^{-1}g)x = (g^{-1})gx = g^{-1}x$. Así g^{-1} está en G_x. □

El número de elementos en el conjunto de puntos fijos de un elemento $g \in G$ lo denotaremos por $|X_g|$ y el número de elementos en la órbita de $x \in X$ lo denotaremos por $|\mathcal{O}_x|$. Los siguientes teoremas establecen la relación entre las órbitas de un elemento $x \in X$ y las clases laterales izquierdas de G_x en G.

Teorema 14.11. *Sea G un grupo finito y sea X un G-conjunto finito. Si $x \in X$, entonces $|\mathcal{O}_x| = [G : G_x]$.*

Demostración. Sabemos que $|G|/|G_x|$ es el número de clases laterales izquierdas de G_x en G por el Teorema de Lagrange (Teorema 6.10). Definiremos una función biyetiva ϕ de la órbita $\mathcal{O}_x$ de x al conjunto de clases laterales izquierdas $\mathcal{L}_{G_x}$ de G_x en G. Sea $y \in \mathcal{O}_x$. Entonces existe g en G tal que $gx = y$. Definamos ϕ de forma que $\phi(y) = gG_x$. Para mostrar que ϕ es 1-1, supongamos que $\phi(y_1) = \phi(y_2)$. Entonces

$$\phi(y_1) = g_1G_x = g_2G_x = \phi(y_2),$$

donde $g_1x = y_1$ y $g_2x = y_2$. Como $g_1G_x = g_2G_x$, existe $g \in G_x$ tal que $g_2 = g_1g$,

$$y_2 = g_2x = g_1gx = g_1x = y_1;$$

por lo tanto, la función ϕ es 1-1. Finalmente, debemos mostrar que ϕ es sobreyectiva. Sea gG_x una clase lateral izquierda. Si $gx = y$, entonces $\phi(y) = gG_x$. □

14.2 La Ecuación de Clase

Sea X un G-conjunto finito y X_G el conjunto de puntos fijos en X; es decir,

$$X_G = \{x \in X : gx = x \text{ para todo } g \in G\}.$$

Como las óribitas de la acción particionan a X,

$$|X| = |X_G| + \sum_{i=k}^{n} |\mathcal{O}_{x_i}|,$$

donde $x_k, \ldots, x_n$ son representantes de las distintas órbitas no triviales de X.

Ahora consideremos el caso especial en el que G actúa sobre sí mismo por conjugación, $(g, x) \mapsto gxg^{-1}$. El ***centro*** de G,

$$Z(G) = \{x : xg = gx \text{ para todo } g \in G\},$$

es el conjunto de puntos que quedan fijos por conjugación. La órbitas de la acción se llaman ***clases de conjugación*** de G. Si $x_1, \ldots, x_k$ son representantes de cada una de las clases de conjugación no-triviales de G y $|\mathcal{O}_{x_1}| = n_1, \ldots, |\mathcal{O}_{x_k}| = n_k$, entonces

$$|G| = |Z(G)| + n_1 + \cdots + n_k.$$

Cada uno de los subgrupos estabilizadores de uno de los x_i, $C(x_i) = \{g \in G : gx_i = x_i g\}$, se llama ***subgrupo centralizador*** de x_i. Por el Teorema 14.11, obtenemos la ***ecuación de clase***:

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)].$$

Una de las consecuencias de la ecuación de clase es que el orden de cada clase de conjugación divide el orden de G.

Ejemplo 14.12. Es fácil verificar que las clases de conjugación en S_3 son las siguientes:

$$\{(1)\}, \quad \{(123), (132)\}, \quad \{(12), (13), (23)\}.$$

La ecuación de clase es $6 = 1 + 2 + 3$.

Ejemplo 14.13. El centro de D_4 es $\{(1), (13)(24)\}$, y las clases de conjugación

$$\{(13), (24)\}, \quad \{(1432), (1234)\}, \quad \{(12)(34), (14)(23)\}.$$

Por lo tanto, la ecuación de clase para D_4 es $8 = 2 + 2 + 2 + 2$.

Ejemplo 14.14. Para S_n toma algo de esfuerzo encontrar las clases de conjugación. Empezamos con los ciclos. Supongamos que $\sigma = (a_1, \ldots, a_k)$ es un ciclo y sea $\tau \in S_n$. Por el Teorema 6.16,

$$\tau\sigma\tau^{-1} = (\tau(a_1), \ldots, \tau(a_k)).$$

En consecuencia, cualquiera dos ciclos del mismo largo son conjugados. Ahora, sea $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$ una descomposición en ciclos, donde el largo de cada ciclo σ_i es r_i. Entonces σ es conjugado a cualquier otro $\tau \in S_n$ cuya descomposición en ciclos tiene los mismos largos.

El número de clases de conjugación en S_n es igual al número de formas en que n puede ser particionado como suma de enteros positivos. En el caso de S_3 por ejemplo, podemos particionar el entero 3 en las siguientes tres sumas:

$$3 = 1 + 1 + 1$$

$$3 = 1 + 2$$
$$3 = 3;$$

Por lo tanto, existen tres clases de conjugación. El problema de determinar el número de tales particiones para un entero dado n es lo que se conoce como ***NP-completo***. Esto en la práctica quiere decir que el problema no se puede resolver para valores grandes de n pues los cálculos tomarían demasiado tiempo incluso para un computador enorme.

Teorema 14.15. *Sea G un grupo de orden p^n donde p es primo. Entonces G tiene centro no-trivial.*

Demostración. Aplicamos la ecuación de clase

$$|G| = |Z(G)| + n_1 + \cdots + n_k.$$

Como cada $n_i > 1$ y $n_i \mid |G|$, concluimos que p divide a cada n_i. Además, $p \mid |G|$; luego, p divide a $|Z(G)|$. Como la identidad siempre está en el centro de G, $|Z(G)| \geq 1$. Por lo tanto, $|Z(G)| \geq p$, y existe algún $g \in Z(G)$ tal que $g \neq 1$. □

Corolario 14.16. *Sea G un grupo de orden p^2 donde p es primo. Entonces G es abeliano.*

Demostración. Por el Teorema 14.15, $|Z(G)| = p$ o p^2. Si $|Z(G)| = p^2$, estamos listos. Supongamos que $|Z(G)| = p$. Entonces $Z(G)$ y $G/Z(G)$ ambos tienen orden p y por ende son ambos cíclicos. Eligiendo un generador $aZ(G)$ para $G/Z(G)$, podemos escribir cualquier elemento $gZ(G)$ en el cociente como $a^m Z(G)$ para algún entero m; luego, $g = a^m x$ para algún x en el centro de G. Similarmente, si $hZ(G) \in G/Z(G)$, entonces existe y en $Z(G)$ tal que $h = a^n y$ para algún entero n. Como x e y están en el centro de G, conmutan con todos los elementos de G; por lo tanto,

$$gh = a^m x a^n y = a^{m+n} xy = a^n y a^m x = hg,$$

y G es abeliano. □

14.3 Teorema de Conteo de Burnside

Supongamos que deseamos pintar los vértices de un cuadrado con dos colores diferentes, digamos blanco y negro. Podríamos sospechar que habría $2^4 = 16$ coloreados diferentes. Pero, algunos de estos son equivalentes. Si pintamos el primer vértices negro y los demás vértices blancos, es lo mismo que pintar el segundo vértices negro y los demás blancos pues podemos obtener el segundo coloreado simplemente rotando el cuadrado 90° (Figura 14.17).

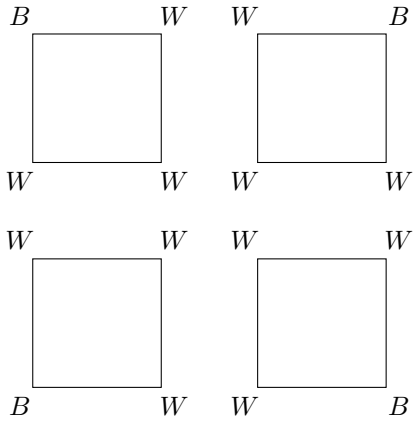


Figura 14.17: Coloramientos equivalentes del cuadrado

El Teorema de Conteo de Burnside ofrece un método de calcular el número de maneras distinguibles en que algo puede ser realizado. Además de sus aplicaciones geométricas, el teorema tiene interesantes aplicaciones en teoría de conmutación (switching theory) y en química. La demostración del Teorema de Conteo de Burnside depende del siguiente lema.

Lema 14.18. *Sea X un G-conjunto y supongamos que $x \sim y$. Entonces G_x es isomorfo a G_y. En particular, $|G_x| = |G_y|$.*

Demostración. Supongamos que la acción de G en X está dada por $(g, x) \mapsto g \cdot x$. Como $x \sim y$, existe $g \in G$ tal que $g \cdot x = y$. Sea $a \in G_x$. Como

$$gag^{-1} \cdot y = ga \cdot g^{-1}y = ga \cdot x = g \cdot x = y,$$

podemos definir una función $\phi : G_x \to G_y$ por $\phi(a) = gag^{-1}$. La función ϕ es un homomorfismo pues

$$\phi(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \phi(a)\phi(b).$$

Supongamos que $\phi(a) = \phi(b)$. Entonces $gag^{-1} = gbg^{-1}$ y $a = b$; es decir, la función es inyectiva. Para mostrar que ϕ es sobreyectiva, sea b en G_y; entonces $g^{-1}bg$ está en G_x pues

$$g^{-1}bg \cdot x = g^{-1}b \cdot gx = g^{-1}b \cdot y = g^{-1} \cdot y = x;$$

y $\phi(g^{-1}bg) = b$. □

Teorema 14.19 (Burnside)**.** *Sea G un grupo finito que actuando en un conjunto X y sea k el número de órbitas de X. Entonces*

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

Demostración. Consideramos todos los puntos fijos de x para cada elemento $g \in G$; es decir, consideramos todos los g y todos los x tales que $gx = x$. En términos de conjuntos de puntos fijos, el número de todos los g que fijan a x es

$$\sum_{g \in G} |X_g|.$$

Pero, en términos de subgrupos estabilizadores, este número es

$$\sum_{x \in X} |G_x|;$$

luego, $\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|$. Por el Lema 14.18,

$$\sum_{y \in \mathcal{O}_x} |G_y| = |\mathcal{O}_x| \cdot |G_x|.$$

Por el Teorema 14.11 y el Teorema de Lagrange, esta expresión es igual a $|G|$. Sumando sobre las k órbitas distintas, concluimos que

$$\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x| = k \cdot |G|. \qquad \square$$

Ejemplo 14.20. Sea $X = \{1, 2, 3, 4, 5\}$ y supongamos que G es el grupo de permutaciones $G = \{(1), (13), (13)(25), (25)\}$. Las órbitas en X son $\{1, 3\}$, $\{2, 5\}$, y $\{4\}$. Los conjuntos de puntos fijos son

$$\begin{aligned} X_{(1)} &= X \\ X_{(13)} &= \{2, 4, 5\} \\ X_{(13)(25)} &= \{4\} \\ X_{(25)} &= \{1, 3, 4\}. \end{aligned}$$

El Teorema de Burnside dice que

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g| = \frac{1}{4}(5 + 3 + 1 + 3) = 3.$$

Un Ejemplo Geométrico

Antes de aplicar el Teorema de Burnside a problemas de teoría de conmutación, examinemos el número de maneras en que se pueden colorear los vértices de un cuadrado utilizando dos colores, blanco y negro. Notemos que a veces obtendremos coloreados equivalentes simplemente aplicando un movimiento rígido al cuadrado. Por ejemplo, como mencionamos antes, si pintamos un vértice negro y los restantes blancos, no importa cuál es el vértices negro pues una rotación nos dará una forma equivalente de pintarlos.

El grupo de simetría de un cuadrado, D_4, está dado por las siguientes permutaciones:

(1)	(13)	(24)	(1432)
(1234)	(12)(34)	(14)(23)	(13)(24)

El grupo G actúa en el conjunto de vértices $\{1, 2, 3, 4\}$ en la forma usual. Podemos describir los diferentes coloreados como funciones de X en $Y = \{N, B\}$ donde N y B representan los colores negro y blango, respectivamente. Cada función $f : X \to Y$ describe una forma de colorear las esquinas del cuadrado. Cada $\sigma \in D_4$ induce una permutación $\widetilde{\sigma}$ de los posibles coloreados dada por $\widetilde{\sigma}(f) = f \circ \sigma$ for $f : X \to Y$. Por ejemplo, supongamos que f está definida por

$$\begin{aligned} f(1) &= N \\ f(2) &= B \\ f(3) &= B \end{aligned}$$

$$f(4) = B$$

y $\sigma = (12)(34)$. Entonces $\widetilde{\sigma}(f) = f \circ \sigma$ envía el vértice 2 en N y los restantes vértices en B. El conjunto de tales $\widetilde{\sigma}$ es un grupo de permutaciones $\widetilde{G}$ en el conjunto de los posibles coloreados. Digamos que $\widetilde{X}$ denota el conjunto de todos los posibles coloreados; es decir, $\widetilde{X}$ es el conjunto de todas las posibles funciones de X en Y. Ahora debemos calcular el número de clases de equivalencia respecto a $\widetilde{G}$.

1. $\widetilde{X}_{(1)} = \widetilde{X}$ pues la identidad fija todos los posibles coloreados. $|\widetilde{X}| = 2^4 = 16$.

2. $\widetilde{X}_{(1234)}$ consiste de todas las $f \in \widetilde{X}$ tales que f no cambia al aplicarle la permutación (1234). En este caso $f(1) = f(2) = f(3) = f(4)$, de manera que todos los valores de f deben ser iguales; es decir, ya sea $f(x) = N$ o $f(x) = B$ para todos los vértices x del cuadrado. Así $|\widetilde{X}_{(1234)}| = 2$.

3. $|\widetilde{X}_{(1432)}| = 2$.

4. For $\widetilde{X}_{(13)(24)}$, $f(1) = f(3)$ and $f(2) = f(4)$. Luego, $|\widetilde{X}_{(13)(24)}| = 2^2 = 4$.

5. $|\widetilde{X}_{(12)(34)}| = 4$.

6. $|\widetilde{X}_{(14)(23)}| = 4$.

7. Para $\widetilde{X}_{(13)}$, $f(1) = f(3)$ y las demás esquinas pueden ser de cualquier color; luego, $|\widetilde{X}_{(13)}| = 2^3 = 8$.

8. $|\widetilde{X}_{(24)}| = 8$.

Por el Teorema de Burnside, podemos conluir que hay exactamente

$$\frac{1}{8}(2^4 + 2^1 + 2^2 + 2^1 + 2^2 + 2^2 + 2^3 + 2^3) = 6$$

maneras de colorear los vértices del cuadrado.

Proposición 14.21. *Sea G un grupo de permutaciones de X y $\widetilde{X}$ el conjunto de funciones de X en Y. Entonces existe un grupo de permutaciones $\widetilde{G}$ actuando en $\widetilde{X}$, donde $\widetilde{\sigma} \in \widetilde{G}$ está definido por $\widetilde{\sigma}(f) = f \circ \sigma$ para $\sigma \in G$ y $f \in \widetilde{X}$. Más aún, si n es el número de ciclos en la descomposición cíclica de σ, entonces $|\widetilde{X}_\sigma| = |Y|^n$.*

Demostración. Sea $\sigma \in G$ y $f \in \widetilde{X}$. Claramente, $f \circ \sigma$ también está en $\widetilde{X}$. Supongamos que g es otra función de X en Y tal que $\widetilde{\sigma}(f) = \widetilde{\sigma}(g)$. Entonces para cada $x \in X$,

$$f(\sigma(x)) = \widetilde{\sigma}(f)(x) = \widetilde{\sigma}(g)(x) = g(\sigma(x)).$$

Como σ es una permutación de X, todo elemento x' en X es la imagen de algún x en X por σ; luego, f y g coinciden en los elementos de X. Por lo tanto, $f = g$ y $\widetilde{\sigma}$ es inyectiva. La función $\sigma \mapsto \widetilde{\sigma}$ es sobre, pues los dos conjuntos son del mismo tamaño (finito).

Supongamos que σ es una permutación de X con descomposición cíclica $\sigma = \sigma_1\sigma_2 \cdots \sigma_n$. Cualquier f en $\widetilde{X}_\sigma$ debe tener el mismo valor en cada ciclo de σ. Como hay n ciclos e $|Y|$ valores posibles para cada ciclo, $|\widetilde{X}_\sigma| = |Y|^n$. □

Ejemplo 14.22. Sea $X = \{1, 2, \ldots, 7\}$ y supongamos que $Y = \{A, B, C\}$. Si g es la permutación de X dada por $(13)(245) = (13)(245)(6)(7)$, entonces $n = 4$. Cualquier $f \in \widetilde{X}_g$ debe tener el mismo valor para cada ciclo en g. Existen $|Y| = 3$ elecciones para cada valor, así $|\widetilde{X}_g| = 3^4 = 81$.

Ejemplo 14.23. Supongamos que queremos colorear los vértices de un cuadrado usando cuatro colores diferentes. Por la Proposición 14.21, podemos decidir inmediatamente que existen

$$\frac{1}{8}(4^4 + 4^1 + 4^2 + 4^1 + 4^2 + 4^2 + 4^3 + 4^3) = 55$$

maneras posibles.

Funciones de Conmutación

En la teoría de conmutación, estamos interesados en el diseño de circuitos electrónicos con entradas y salidas binarias. El más simple de tales circuitos es una función de conmutación que tiene n entradas y una sola salida (Figura 14.24). Circuitos electrónicos grandes con frecuencia se pueden construir combinando módulos más pequeños de este tipo. El problema inherente acá es que incluso para un circuito simple existe un gran número de funciones de conmutación. Con solo cuatro entradas y una salida, podemos construir 65,536 funciones de conmutación diferentes. Pero, muchas veces podemos transformar una función de conmutación en otra simplemente permutando las entradas del circuito (Figura 14.25).

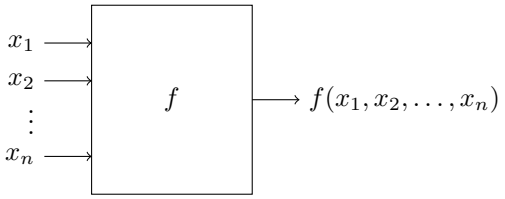


Figura 14.24: Una función de conmutación de n variables

Definimos una ***función de conmutación*** o ***función Booleana*** de n variables como una función de $\mathbb{Z}_2^n$ en $\mathbb{Z}_2$. Como cualquier función de conmutación puede tomar dos valores para cada n-tupla binaria y hay 2^n n-tuplas binarias, existen 2^{2^n} funciones de conmutación para n variables. En general, permitir las permutaciones de las entradas, reduce dramáticamente el número de módulos de diferente tipo requeridos para construir un circuito grande.

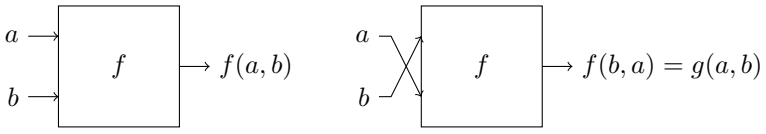


Figura 14.25: Una función de conmutación de dos variables

Las posibles funciones de conmutación con dos variables de entrada a y b se listan en la Tabla 14.26. Dos funciones de conmutación f y g son equivalentes si g puede ser obtenida a partir de f por una permutación de las variables de entrada. Por ejemplo, $g(a, b, c) = f(b, c, a)$. En este caso $g \sim f$ via la permutación (acb). En el caso de funciones de permutación de dos variables,

la permutación (ab) reduce las 16 posibles funciones de permutación a 12 funciones no-equivalentes pues

$$f_2 \sim f_4$$
$$f_3 \sim f_5$$
$$f_{10} \sim f_{12}$$
$$f_{11} \sim f_{13}.$$

Entradas		Salidas							
		f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1
Entradas		Salidas							
		f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1

Cuadro 14.26: Funciones de conmutación en dos variables

Para tres variables de entrada hay $2^{2^3} = 256$ funciones de conmutación posibles; en el caso de cuatro variables hay $2^{2^4} = 65{,}536$. El número de clases de equivalencia es demasiado grande para que sea razonable calcularlo directamente. Es necesario emplear el Teorema de Burnside.

Considere la función de conmutación con tres entradas posibles, a, b, y c. Como mencionamos, dos funciones de conmutación f y g son equivalentes si una permutación de las variables de entrada de f da g. Es importante notar que una permutación de las funciones de conmutación no es simplemente una permutación de los valores de entrada $\{a, b, c\}$. Una función de conmutación es un conjunto de valores de salida para las entradas a, b, y c, así, cuando consideramos funciones de conmutación equivalentes, estamos permutando 2^3 salidas posibles, no solo tres valores de entrada. Por ejemplo, cada tripleta binaria (a, b, c) tiene asociada una salida específica. La permutación (acb) cambia la salida como sigue:

$$(0,0,0) \mapsto (0,0,0)$$
$$(0,0,1) \mapsto (0,1,0)$$
$$(0,1,0) \mapsto (1,0,0)$$
$$\vdots$$
$$(1,1,0) \mapsto (1,0,1)$$
$$(1,1,1) \mapsto (1,1,1).$$

Sea X el conjunto de valores de salida para una función de conmutación en n variables. Entonces $|X| = 2^n$. Podemos enumerar estos valores como sigue:

$$(0,\ldots,0,1) \mapsto 0$$
$$(0,\ldots,1,0) \mapsto 1$$

$$(0,\ldots,1,1) \mapsto 2$$
$$\vdots$$
$$(1,\ldots,1,1) \mapsto 2^n - 1.$$

Ahora consideremos un circuito con cuatro variables de entrada y una sola salida. Supongamos que podemos permutar los cables de cualquier circuito de acuerdo al siguiente grupo de permutaciones:

$$(a) \quad (ac) \quad (bd) \quad (adcb)$$
$$(abcd) \quad (ab)(cd) \quad (ad)(bc) \quad (ac)(bd).$$

Las permutaciones de las cuatro variables de entrada posible inducen las permutaciones de los valores de salida en la Tabla 14.27.

Lugo, existen

$$\frac{1}{8}(2^{16} + 2 \cdot 2^{12} + 2 \cdot 2^6 + 3 \cdot 2^{10}) = 9616$$

funciones de conmutación posibles de cuatro variables bajo este grupo de permutaciones. Este número será incluso menor si consideramos el grupo completo de simetrías en cuatro símbolos.

Permutación en el grupo	Permutación de función de conmutación	Número de Ciclos
(a)	(0)	16
(ac)	$(2,8)(3,9)(6,12)(7,13)$	12
(bd)	$(1,4)(3,6)(9,12)(11,14)$	12
$(adcb)$	$(1,2,4,8)(3,6.12,9)(5,10)(7,14,13,11)$	6
$(abcd)$	$(1,8,4,2)(3,9,12,6)(5,10)(7,11,13,14)$	6
$(ab)(cd)$	$(1,2)(4,8)(5,10)(6,9)(7,11)(13,14)$	10
$(ad)(bc)$	$(1,8)(2,4)(3,12)(5,10)(7,14)(11,13)$	10
$(ac)(bd)$	$(1,4)(2,8)(3,12)(6,9)(7,13)(11,14)$	10

Cuadro 14.27: Permutaciones de funciones de conmutación en cuatro variables

Sage Sage has many commands related to conjugacy, which is a group action. It also has commands for orbits and stabilizers of permutation groups. In the supplement, we illustrate the automorphism group of a (combinatorial) graph as another example of a group action on the vertex set of the graph.

Nota Histórica

William Burnside nació en Londres en 1852. Estudió en la Universidad de Cambridge desde 1871 hasta 1875 y ganó el Smith's Prize en su último año. Después de graduarse dio clases en Cambridge. Se convirtió en miebro de la Royal Society en 1893. Burnside escribió aproximadamente 150 artículos en matemáticas aplicadas, geometría diferencial y probabilidades, pero sus contribuciones más famosas fueron en teoría de grupos. Varias de las conjeturas de Burnside han estimulado la investigación hasta hoy. Una conjetura fue que todo grupo de orden impar es soluble; es decir, para un grupo G de orden impar, existe una sucesión de subgrupos

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\}$$

tales que H_i es normal en H_{i+1} y H_{i+1}/H_i es abeliano. TEsta conjetura fue finalmente demostrada por W. Feit y J. Thompson en 1963. El libro *The Theory of Groups of Finite Order* de Burnside, publicado en 1897, fue uno de los primeros libros en dar un tratamiento moderno a los grupos en lugar de verlos solo como grupos de permutaciones. La segunda edición, publicada en 1911, es todavía un clásico.

14.4 Exercises

1. Examples 14.1–14.5 in the first section each describe an action of a group G on a set X, which will give rise to the equivalence relation defined by G-equivalence. For each example, compute the equivalence classes of the equivalence relation, the ***G-equivalence classes***.

2. Compute all X_g and all G_x for each of the following permutation groups.

(a) $X = \{1, 2, 3\}$, $G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$

(b) $X = \{1, 2, 3, 4, 5, 6\}$, $G = \{(1), (12), (345), (354), (12)(345), (12)(354)\}$

3. Compute the G-equivalence classes of X for each of the G-sets in Exercise 14.4.2. For each $x \in X$ verify that $|G| = |\mathcal{O}_x| \cdot |G_x|$.

4. Let G be the additive group of real numbers. Let the action of $\theta \in G$ on the real plane $\mathbb{R}^2$ be given by rotating the plane counterclockwise about the origin through θ radians. Let P be a point on the plane other than the origin.

(a) Show that $\mathbb{R}^2$ is a G-set.

(b) Describe geometrically the orbit containing P.

(c) Find the group G_P.

5. Let $G = A_4$ and suppose that G acts on itself by conjugation; that is, $(g, h) \mapsto ghg^{-1}$.

(a) Determine the conjugacy classes (orbits) of each element of G.

(b) Determine all of the isotropy subgroups for each element of G.

6. Find the conjugacy classes and the class equation for each of the following groups.

(a) S_4 (b) D_5 (c) $\mathbb{Z}_9$ (d) Q_8

7. Write the class equation for S_5 and for A_5.

8. If a square remains fixed in the plane, how many different ways can the corners of the square be colored if three colors are used?

9. How many ways can the vertices of an equilateral triangle be colored using three different colors?

10. Find the number of ways a six-sided die can be constructed if each side is marked differently with $1, \ldots, 6$ dots.

11. Up to a rotation, how many ways can the faces of a cube be colored with three different colors?

12. Consider 12 straight wires of equal lengths with their ends soldered together to form the edges of a cube. Either silver or copper wire can be used for each edge. How many different ways can the cube be constructed?

13. Suppose that we color each of the eight corners of a cube. Using three different colors, how many ways can the corners be colored up to a rotation of the cube?

14. Each of the faces of a regular tetrahedron can be painted either red or white. Up to a rotation, how many different ways can the tetrahedron be painted?

15. Suppose that the vertices of a regular hexagon are to be colored either red or white. How many ways can this be done up to a symmetry of the hexagon?

16. A molecule of benzene is made up of six carbon atoms and six hydrogen atoms, linked together in a hexagonal shape as in Figure 14.28.

(a) How many different compounds can be formed by replacing one or more of the hydrogen atoms with a chlorine atom?

(b) Find the number of different chemical compounds that can be formed by replacing three of the six hydrogen atoms in a benzene ring with a CH_3 radical.

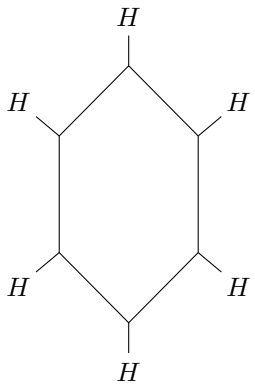


Figura 14.28: A benzene ring

17. How many equivalence classes of switching functions are there if the input variables x_1, x_2, and x_3 can be permuted by any permutation in S_3? What if the input variables x_1, x_2, x_3, and x_4 can be permuted by any permutation in S_4?

18. How many equivalence classes of switching functions are there if the input variables x_1, x_2, x_3, and x_4 can be permuted by any permutation in the subgroup of S_4 generated by the permutation $(x_1x_2x_3x_4)$?

19. A striped necktie has 12 bands of color. Each band can be colored by one of four possible colors. How many possible different-colored neckties are there?

20. A group acts ***faithfully*** on a G-set X if the identity is the only element of G that leaves every element of X fixed. Show that G acts faithfully on X if and only if no two distinct elements of G have the same action on each element of X.

21. Let p be prime. Show that the number of different abelian groups of order p^n (up to isomorphism) is the same as the number of conjugacy classes in S_n.

22. Let $a \in G$. Show that for any $g \in G$, $gC(a)g^{-1} = C(gag^{-1})$.

23. Let $|G| = p^n$ be a nonabelian group for p prime. Prove that $|Z(G)| < p^{n-1}$.

24. Let G be a group with order p^n where p is prime and X a finite G-set. If $X_G = \{x \in X : gx = x \text{ for all } g \in G\}$ is the set of elements in X fixed by the group action, then prove that $|X| \equiv |X_G| \pmod{p}$.

25. If G is a group of order p^n, where p is prime and $n \geq 2$, show that G must have a proper subgroup of order p. If $n \geq 3$, is it true that G will have a proper subgroup of order p^2?

14.5 Ejercicio de Programación

1. Escriba un programa para calcular el número de clases de conjugación en S_n. ¿Cuál es el mayor valor de n para el que funciona su programa?

14.6 Referencias y Lecturas Recomendadas

[1] De Bruijin, N. G. "Pólya's Theory of Counting," in *Applied Combinatorial Mathematics*, Beckenbach, E. F., ed. Wiley, New York, 1964.

[2] Eidswick, J. A. "Cubelike Puzzles—What Are They and How Do You Solve Them?" *American Mathematical Monthly* **93**(1986), 157–76.

[3] Harary, F., Palmer, E. M., and Robinson, R. W. "Pólya's Contributions to Chemical Enumeration," in *Chemical Applications of Graph Theory*, Balaban, A. T., ed. Academic Press, London, 1976.

[4] Gårding, L. and Tambour, T. *Algebra for Computer Science*. Springer-Verlag, New York, 1988.

[5] Laufer, H. B. *Discrete Mathematics and Applied Modern Algebra*. PWS-Kent, Boston, 1984.

[6] Pólya, G. and Read, R. C. *Combinatorial Enumeration of Groups, Graphs, and Chemical Compounds*. Springer-Verlag, New York, 1985.

[7] Shapiro, L. W. "Finite Groups Acting on Sets with Applications," *Mathematics Magazine*, May–June 1973, 136–47.

14.7 Sage

Los grupos se pueden presentar de diversas formas, tales como conjuntos de permutaciones, como conjuntos de matrics o como conjuntos de símbolos abstractos relacionados por ciertas reglas ("presentaciones") y en muchas otras formas más. Nos hemos concentrado en grupos de permutaciones por su tangibilidad, con elementos escritos como funciones, y por lo bien implementados que están en Sage. Las acciones de grupo son de gran interés cuando el conjunto en el que se actúa es el grupo mismo, y la acción de grupos figura de forma prominente en las demostraciones de los principales teoremas del próximo capítulo. Pero, cada vez que tenemos una acción de un grupo en un conjunto, podemos pensar el grupo como un grupo de permutaciones en los elementos del conjunto. Por esto los grupos de permutaciones forman un área

de teoría de grupos de interés independiente, con sus propias definiciones y teoremas.

Describiremos los comandos de Sage's aplicables cuando un acción de grupo aparece naturalmente via conjugación, y luego pasaremos a la situación más general.

Conjugación como Acción de Grupo

Podemos creer que debemos ser cuidadosos con la forma en que Sage define la conjugación (gxg^{-1} versus $g^{-1}xg$) y la diferencia entre Sage y el texto sobre el orden de los productos. Pero, si nos fijamos en la definición de centro y de subgrupo centralizador podemos notar que cualquier diferencia de orden es irrelevante. (Por algo no tenemos conjugación izquierda y derecha como conceptos) A continuación los comandos de acción de grupos para la acción particular de conjugar elementos del grupo.

Sage tiene un método `.center()` que entrega el subgrupo de los puntos fijos. El método `.centralizer(g)`, entrega un subgrupo que es el estabilizador del elemento `g`. Finalmente, las órbitas están dadas por clases de conjugación, pero Sage no nos inundará con las clases de conjugación completas y en su lugar nos entrega una lista que contiene un elemento por clase de conjugación, es decir una lista de representantes, por medio del método `.conjugacy_classes_representatives()`. Podemos reconstruir manualmente una clase de conjugación a partir de un elemento, como haremos en el ejemplo de abajo.

Acá los comandos de arriba en acción. Notemos que un grupo abeliano sería una mala elección para este ejemplo.

```
D = DihedralGroup(8)
C = D.center(); C
```

```
Subgroup of (Dihedral group of order 16 as a permutation
    group)
generated by [(1,5)(2,6)(3,7)(4,8)]
```

```
C.list()
```

```
[(), (1,5)(2,6)(3,7)(4,8)]
```

```
a = D("(1,2)(3,8)(4,7)(5,6)")
C1 = D.centralizer(a); C1.list()
```

```
[(), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)(4,8),
    (1,6)(2,5)(3,4)(7,8)]
```

```
b = D("(1,2,3,4,5,6,7,8)")
C2 = D.centralizer(b); C2.order()
```

```
8
```

```
CCR = D.conjugacy_classes_representatives(); CCR
```

```
[(), (2,8)(3,7)(4,6), (1,2)(3,8)(4,7)(5,6), (1,2,3,4,5,6,7,8),
 (1,3,5,7)(2,4,6,8), (1,4,7,2,5,8,3,6), (1,5)(2,6)(3,7)(4,8)]
```

```
r = CCR[2]; r
```

```
(1,2)(3,8)(4,7)(5,6)
```

```
conj = []
x = [conj.append(g^-1*r*g) for g in D if not g^-1*r*g in
    conj]
conj
```

```
[(1,2)(3,8)(4,7)(5,6), (1,4)(2,3)(5,8)(6,7),
 (1,6)(2,5)(3,4)(7,8), (1,8)(2,7)(3,6)(4,5)]
```

Note que en la clase de conjugación construida todos los elementos tienen la misma estructura de ciclos, lo que no es accidental. Note además que `rep` y `a` son el mismo elemento, y que el producto del orden del centralizador (4) por el tamaño de la clase (4) es igual al orden del grupo (16), lo que es una variante de la conclusión del Teorema 14.11.

Compruebe que la siguiente es una ejemplificación de la ecuación de clase en el caso especial de acción por conjugación, pero sería válida para cualquier grupo, en lugar de `D`.

```
sizes = [D.order()/D.centralizer(g).order()
             for g in D.conjugacy_classes_representatives()]
sizes
```

```
[1, 4, 4, 2, 2, 2, 1]
```

```
D.order() == sum(sizes)
```

```
True
```

Autmorfismos de un Grafo

Como ya mencionamos, la acción de grupo puede ser aún más interesante cuando el conjunto en el que se actúa es diferente al grupo mismo. Una clase de ejemplos es el grupo de simetrías de un sólido geométrico, donde los objetos en el conjunto son los vértices del sólido, o quizás otro aspecto de éste como aristas, caras o diagonales. En este caso, el grupo está formado por el conjunto de auqellas permutaciones que mueven el sólido pero lo dejan ocupando el mismo espacio que antes del movimiento (“movimientos rígidos”).

En esta sección examinaremos algo muy similar. Un ***grafo*** es un objeto matemático, que consiste de vértices y aristas, pero la única estructura es si un par de vértices dado está o no conectado por una arista. El grupo consiste de aquellas permutaciones de los vértices que preservan la estructura, es decir, permutaciones de vértices que lleva aristas en aristas y no-aristas en no-aristas. Es muy similar a un grupo de simetría, pero no hay noción alguna de relación geométrica que se preserve.

Acá hay un ejemplo. Deberá ejecutar la primera celda para definir el grafo y obetner una representación gráfica.

```
Q = graphs.CubeGraph(3)
Q.plot(layout='spring')
```

```
A = Q.automorphism_group()
A.order()
```

```
48
```

Se debiera ver como los vértices y aristas de un cubo, pero puede que no se vea del todo regular, lo que está bien, pues la geometría no es relevante. Los vértices están etiquetados con cadenas de tres dígitos binarios, 0 o 1, y dos vétrices están conectados por una arista si sus etiquetas diferen en exactamente una posición. Podríamos esperar que el grupo de simetría tuviera orden 24, en lugar de orden 48, dado su parecido a un cubo (tanto en apariencia como en nombre). Sin embargo, al no estar restringidos a movimientos rígidos, tenemos nuevas permutaciones que preservan las aristas. Una en particular es el intercambio de dos "caras opuestas." Localice los dos 4-ciclos opuestos entre sí, listados en el mismo orden: $000, 010, 110, 100$ y $001, 011, 111, 101$. Notemos que cada ciclo se ve muy similar, pero los vértices de uno terminan en 0 y los del otro en 1.

Podemos crear explícitamente la permutación que intercambia estas dos caras opuestas, usando una versión textual de la permutación en notación de ciclos.

```
a = A("('000','001')('010','011')('110','111')('100','101')")
a in A
```

```
True
```

Podemos usar este grupo para ilustrar los comandos de Sage relevantes para la acción de grupos.

```
A.orbits()
```

```
[['000', '001', '010', '100', '011', '101', '110', '111']]
```

Esta acción tiene solo una (gran) órbita. Esto quiere decir que cualquier vértices es "como" cualquier otro. Cuando un grupo de permutaciones se comporta de esta manera, decimos que el grupo es ***transitivo***.

```
A.is_transitive()
```

```
True
```

Si cada vértice es "igual" podemos calcular el estabilizador de cualquier vértice, pues todos serán isomorfos. Como el vértice 000 es el más simple en algún sentido, calcularemos su estabilizador.

```
S = A.stabilizer('000')
S.list()
```

```
[(),
 ('001','100','010')('011','101','110'),
 ('010','100')('011','101'),
 ('001','010','100')('011','110','101'),
 ('001','100')('011','110'),
 ('001','010')('101','110')]
```

Que `S` tenga 6 elementos no es una sorpresa, pues el grupo tiene orden 48 y el tamaño de la única órbita es 8. Pero podemos dar un paso más. Los tres vértices del grafo adyacentes directamente con 000 son 100, 010, 001. Cualquier automorfismo del grafo que fije 000 debe entonces permutar los tres vértices adyacentes. Hay $3! = 6$ posibles maneras de hacer esto, y podemos verificar que cada una aparece en una de los seis elementos del estabilizador. Así podemos entender un grupo transitivo considerando el estabilizador que es más pequeño, y en este caso vemos que cada elemento del estabilizador está determinado por como permuta a los vecinos del vértice estabilizado.

Los grupos transitivos son tan inusuales como importantes. En contraste, acá hay un grupo de automorfismos de un grafo que está lejos de ser transitivo

(sin ser trivial). Un camino es un grafo que tiene todos sus vértices en una línea. Ejecute la primera celda para ver un camino en 11 vértices.

```
P = graphs.PathGraph(11)
P.plot()
```

```
A = P.automorphism_group()
A.list()
```

```
[(), (0,10)(1,9)(2,8)(3,7)(4,6)]
```

El grupo de automorfismos es la identidad (siempre) y una permutación de orden 2 que "da vuelta" el camino de un lado para el otro. El grupo está lejos de ser transitivo y hay muchas órbitas.

```
A.is_transitive()
```

```
False
```

```
A.orbits()
```

```
[[0, 10], [1, 9], [2, 8], [3, 7], [4, 6], [5]]
```

La mayoría de los estabilizadores es trivial, con una excepción. Como subgrupos de un grupo de orden 2, realmente no hay muchas opciones.

```
A.stabilizer(2).list()
```

```
[()]
```

```
A.stabilizer(5).list()
```

```
[(), (0,10)(1,9)(2,8)(3,7)(4,6)]
```

¿Cómo habría sido diferente este ejemplo final de haber usado un camino en 10 vértices?

14.8 Ejercicios en Sage

1. Construya el grafo de Higman-Sims con el comando `graphs.HigmanSimsGraph()`. Luego construya el grupo de automorfismosy determine el orden del subgrupo normal interesante de este grupo. Puede intentar mostrar el grafo, pero el dibujo probablemente no resulte muy informativo.

2. Este ejercicio le pide verificar la ecuación de clase en una situación donde la acción del grupo no es por conjugación. Considere el ejemplo del grupo de automorfismos del camino de 11 vértices. Primero construya la lista de órbitas. De cada órbita, seleccione el primer elemento como su representante. Calcule el tamaño de la órbita como el índice del estabilizador del representante en el grupo por medio del Teorema 14.11. (Sí, podría simplemente calcular el tamaño de la órbita completa, pero la idea del ejercicio es usar resultados de naturaleza grupística.) Luego sume estos tamaños de órbitas, lo que debiese resultar en el tamaño del conjunto de vértices pues las órbitas forman una partición.

3. Construya un grafo simple (sin bucles ni aristas múltiples), con al menos dos vértices y al menos una arista, cuyo grupo de automorfismos sea trivial. Puede comenzar a experimentar con dibujos en un papel antes de construir el grafo. Un comando similar al siguiente le permitirá construir un grafo a partir de sus aristas. El grafo de abajo es un triángulo o 3-ciclo.

```
G = Graph([(1,2), (2,3), (3,1)])
G.plot()
```

4. Para los siguientes dos pares de grupos, obtenga la lista de representantes de clases de conjugación para cada grupo en el par. Para cada parte, compare y contraste los resultados para los dos grupos enel par, con comentarios bien pensados e interesantes.

(a) El grupo símetrico en 5 símbolos, S_5, y el grupo alternante en 5 símbolos, A_5.

(b) Los grupos dihedrales, D_7 y D_8.

5. Use el comando `graphs.CubeGraph(4)` para construir el grafo cúbico de dimensión cuatro, Q_4. Usando el comando `.plot()` debiera obtener un bonito gráfico. Construya el grupo de automorfismos del grafo, lo que dará una acción de grupo en el conjunto de vértices.

(a) Construya las órbitas de esta acción, y comente.

(b) Construya un estabilizador de un vértices (que es un subgrupo del grupo completo de automorfismos) y ocnsidere la acción de *este* grupo en el conjunto de vértices. Construya las órbitas de esta nueva acción, y comente cuidadosamente sobre sus observaciones, especialmente en términos de los vértices del grafo.

6. Construya el grafo dado por el comando de abajo. El resultado debiera ser un grafo de apariencia simétrica con un grupo de automorfismos de orden 16.

```
G = graphs.CycleGraph(8)
G.add_edges([(0,2),(1,3),(4,6),(5,7)])
G.plot()
```

Repita las dos partes del ejercicio anterior, pero note que en la segunda parte ahora hay dos estabilizadores diferentes que crear. construya ambos y compare la diferencias entre los estabilizadores y sus órbitas. Crear un segundo gráfico con `G.plot(layout='planar')` puede proporcionar una mejor visión.

15

The Sylow Theorems

We already know that the converse of Lagrange's Theorem is false. If G is a group of order m and n divides m, then G does not necessarily possess a subgroup of order n. For example, A_4 has order 12 but does not possess a subgroup of order 6. However, the Sylow Theorems do provide a partial converse for Lagrange's Theorem—in certain cases they guarantee us subgroups of specific orders. These theorems yield a powerful set of tools for the classification of all finite nonabelian groups.

15.1 The Sylow Theorems

We will use what we have learned about group actions to prove the Sylow Theorems. Recall for a moment what it means for G to act on itself by conjugation and how conjugacy classes are distributed in the group according to the class equation, discussed in Chapter 14. A group G acts on itself by conjugation via the map $(g, x) \mapsto gxg^{-1}$. Let $x_1, \ldots, x_k$ be representatives from each of the distinct conjugacy classes of G that consist of more than one element. Then the class equation can be written as

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)],$$

where $Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}$ is the center of G and $C(x_i) = \{g \in G : gx_i = x_ig\}$ is the centralizer subgroup of x_i.

We begin our investigation of the Sylow Theorems by examining subgroups of order p, where p is prime. A group G is a ***p-group*** if every element in G has as its order a power of p, where p is a prime number. A subgroup of a group G is a ***p-subgroup*** if it is a p-group.

Teorema 15.1 (Cauchy)**.** *Let G be a finite group and p a prime such that p divides the order of G. Then G contains a subgroup of order p.*

Demostración. We will use induction on the order of G. If $|G| = p$, then clearly G itself is the required subgroup. We now assume that every group of order k, where $p \leq k < n$ and p divides k, has an element of order p. Assume that $|G| = n$ and $p \mid n$ and consider the class equation of G:

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)].$$

We have two cases.

Case 1. The order of one of the centralizer subgroups, $C(x_i)$, is divisible by p for some i, $i = 1, \ldots, k$. In this case, by our induction hypothesis, we are

done. Since $C(x_i)$ is a proper subgroup of G and p divides $|C(x_i)|$, $C(x_i)$ must contain an element of order p. Hence, G must contain an element of order p.

Case 2. The order of no centralizer subgroup is divisible by p. Then p divides $[G : C(x_i)]$, the order of each conjugacy class in the class equation; hence, p must divide the center of G, $Z(G)$. Since $Z(G)$ is abelian, it must have a subgroup of order p by the Fundamental Theorem of Finite Abelian Groups. Therefore, the center of G contains an element of order p. □

Corolario 15.2. *Let G be a finite group. Then G is a p-group if and only if $|G| = p^n$.*

Ejemplo 15.3. Let us consider the group A_5. We know that $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. By Cauchy's Theorem, we are guaranteed that A_5 has subgroups of orders 2, 3 and 5. The Sylow Theorems will give us even more information about the possible subgroups of A_5.

We are now ready to state and prove the first of the Sylow Theorems. The proof is very similar to the proof of Cauchy's Theorem.

Teorema 15.4 (First Sylow Theorem)**.** *Let G be a finite group and p a prime such that p^r divides $|G|$. Then G contains a subgroup of order p^r.*

Demostración. We induct on the order of G once again. If $|G| = p$, then we are done. Now suppose that the order of G is n with $n > p$ and that the theorem is true for all groups of order less than n, where p divides n. We shall apply the class equation once again:

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)].$$

First suppose that p does not divide $[G : C(x_i)]$ for some i. Then $p^r \mid |C(x_i)|$, since p^r divides $|G| = |C(x_i)| \cdot [G : C(x_i)]$. Now we can apply the induction hypothesis to $C(x_i)$.

Hence, we may assume that p divides $[G : C(x_i)]$ for all i. Since p divides $|G|$, the class equation says that p must divide $|Z(G)|$; hence, by Cauchy's Theorem, $Z(G)$ has an element of order p, say g. Let N be the group generated by g. Clearly, N is a normal subgroup of $Z(G)$ since $Z(G)$ is abelian; therefore, N is normal in G since every element in $Z(G)$ commutes with every element in G. Now consider the factor group G/N of order $|G|/p$. By the induction hypothesis, G/N contains a subgroup H of order p^{r-1}. The inverse image of H under the canonical homomorphism $\phi : G \to G/N$ is a subgroup of order p^r in G. □

A ***Sylow p-subgroup*** P of a group G is a maximal p-subgroup of G. To prove the other two Sylow Theorems, we need to consider conjugate subgroups as opposed to conjugate elements in a group. For a group G, let $\mathcal{S}$ be the collection of all subgroups of G. For any subgroup H, $\mathcal{S}$ is a H-set, where H acts on $\mathcal{S}$ by conjugation. That is, we have an action

$$H \times \mathcal{S} \to \mathcal{S}$$

defined by

$$h \cdot K \mapsto hKh^{-1}$$

for K in $\mathcal{S}$.

The set

$$N(H) = \{g \in G : gHg^{-1} = H\}$$

is a subgroup of G called the the ***normalizer*** of H in G. Notice that H is a normal subgroup of $N(H)$. In fact, $N(H)$ is the largest subgroup of G in which H is normal.

Lema 15.5. *Let P be a Sylow p-subgroup of a finite group G and let x have as its order a power of p. If $x^{-1}Px = P$, then $x \in P$.*

DEMOSTRACIÓN. Certainly $x \in N(P)$, and the cyclic subgroup, $\langle xP \rangle \subset N(P)/P$, has as its order a power of p. By the Correspondence Theorem there exists a subgroup H of $N(P)$ containing P such that $H/P = \langle xP \rangle$. Since $|H| = |P| \cdot |\langle xP \rangle|$, the order of H must be a power of p. However, P is a Sylow p-subgroup contained in H. Since the order of P is the largest power of p dividing $|G|$, $H = P$. Therefore, H/P is the trivial subgroup and $xP = P$, or $x \in P$. □

Lema 15.6. *Let H and K be subgroups of G. The number of distinct H-conjugates of K is $[H : N(K) \cap H]$.*

DEMOSTRACIÓN. We define a bijection between the conjugacy classes of K and the right cosets of $N(K) \cap H$ by $h^{-1}Kh \mapsto (N(K) \cap H)h$. To show that this map is a bijection, let $h_1, h_2 \in H$ and suppose that $(N(K) \cap H)h_1 = (N(K) \cap H)h_2$. Then $h_2 h_1^{-1} \in N(K)$. Therefore, $K = h_2 h_1^{-1} K h_1 h_2^{-1}$ or $h_1^{-1} K h_1 = h_2^{-1} K h_2$, and the map is an injection. It is easy to see that this map is surjective; hence, we have a one-to-one and onto map between the H-conjugates of K and the right cosets of $N(K) \cap H$ in H. □

Teorema 15.7 (Second Sylow Theorem)**.** *Let G be a finite group and p a prime dividing $|G|$. Then all Sylow p-subgroups of G are conjugate. That is, if P_1 and P_2 are two Sylow p-subgroups, there exists a $g \in G$ such that $gP_1g^{-1} = P_2$.*

DEMOSTRACIÓN. Let P be a Sylow p-subgroup of G and suppose that $|G| = p^r m$ with $|P| = p^r$. Let

$$\mathcal{S} = \{P = P_1, P_2, \ldots, P_k\}$$

consist of the distinct conjugates of P in G. By Lemma 15.6, $k = [G : N(P)]$. Notice that

$$|G| = p^r m = |N(P)| \cdot [G : N(P)] = |N(P)| \cdot k.$$

Since p^r divides $|N(P)|$, p cannot divide k.

Given any other Sylow p-subgroup Q, we must show that $Q \in \mathcal{S}$. Consider the Q-conjugacy classes of each P_i. Clearly, these conjugacy classes partition $\mathcal{S}$. The size of the partition containing P_i is $[Q : N(P_i) \cap Q]$ by Lemma 15.6, and Lagrange's Theorem tells us that $|Q| = [Q : N(P_i) \cap Q]|N(P_i) \cap Q|$. Thus, $[Q : N(P_i) \cap Q]$ must be a divisor of $|Q| = p^r$. Hence, the number of conjugates in every equivalence class of the partition is a power of p. However, since p does not divide k, one of these equivalence classes must contain only a single Sylow p-subgroup, say P_j. In this case, $x^{-1}P_j x = P_j$ for all $x \in Q$. By Lemma 15.5, $P_j = Q$. □

Teorema 15.8 (Third Sylow Theorem)**.** *Let G be a finite group and let p be a prime dividing the order of G. Then the number of Sylow p-subgroups is congruent to 1 (mod p) and divides $|G|$.*

DEMOSTRACIÓN. Let P be a Sylow p-subgroup acting on the set of Sylow p-subgroups,

$$\mathcal{S} = \{P = P_1, P_2, \ldots, P_k\},$$

by conjugation. From the proof of the Second Sylow Theorem, the only P-conjugate of P is itself and the order of the other P-conjugacy classes is a power of p. Each P-conjugacy class contributes a positive power of p toward

$|\mathcal{S}|$ except the equivalence class $\{P\}$. Since $|\mathcal{S}|$ is the sum of positive powers of p and 1, $|\mathcal{S}| \equiv 1 \pmod{p}$.

Now suppose that G acts on $\mathcal{S}$ by conjugation. Since all Sylow p-subgroups are conjugate, there can be only one orbit under this action. For $P \in \mathcal{S}$,

$$|\mathcal{S}| = |\text{orbit of } P| = [G : N(P)]$$

by Lemma 15.6. But $[G : N(P)]$ is a divisor of $|G|$; consequently, the number of Sylow p-subgroups of a finite group must divide the order of the group. □

Historical Note

Peter Ludvig Mejdell Sylow was born in 1832 in Christiania, Norway (now Oslo). After attending Christiania University, Sylow taught high school. In 1862 he obtained a temporary appointment at Christiania University. Even though his appointment was relatively brief, he influenced students such as Sophus Lie (1842–1899). Sylow had a chance at a permanent chair in 1869, but failed to obtain the appointment. In 1872, he published a 10-page paper presenting the theorems that now bear his name. Later Lie and Sylow collaborated on a new edition of Abel's works. In 1898, a chair at Christiania University was finally created for Sylow through the efforts of his student and colleague Lie. Sylow died in 1918.

15.2 Examples and Applications

Ejemplo 15.9. Using the Sylow Theorems, we can determine that A_5 has subgroups of orders 2, 3, 4, and 5. The Sylow p-subgroups of A_5 have orders 3, 4, and 5. The Third Sylow Theorem tells us exactly how many Sylow p-subgroups A_5 has. Since the number of Sylow 5-subgroups must divide 60 and also be congruent to 1 (mod 5), there are either one or six Sylow 5-subgroups in A_5. All Sylow 5-subgroups are conjugate. If there were only a single Sylow 5-subgroup, it would be conjugate to itself; that is, it would be a normal subgroup of A_5. Since A_5 has no normal subgroups, this is impossible; hence, we have determined that there are exactly six distinct Sylow 5-subgroups of A_5.

The Sylow Theorems allow us to prove many useful results about finite groups. By using them, we can often conclude a great deal about groups of a particular order if certain hypotheses are satisfied.

Teorema 15.10. *If p and q are distinct primes with $p < q$, then every group G of order pq has a single subgroup of order q and this subgroup is normal in G. Hence, G cannot be simple. Furthermore, if $q \not\equiv 1 \pmod{p}$, then G is cyclic.*

Demostración. We know that G contains a subgroup H of order q. The number of conjugates of H divides pq and is equal to $1 + kq$ for $k = 0, 1, \ldots$. However, $1 + q$ is already too large to divide the order of the group; hence, H can only be conjugate to itself. That is, H must be normal in G.

The group G also has a Sylow p-subgroup, say K. The number of conjugates of K must divide q and be equal to $1 + kp$ for $k = 0, 1, \ldots$. Since q is prime, either $1 + kp = q$ or $1 + kp = 1$. If $1 + kp = 1$, then K is normal in G. In this case, we can easily show that G satisfies the criteria, given in Chapter 9, for the internal direct product of H and K. Since H is isomorphic to $\mathbb{Z}_q$ and K is isomorphic to $\mathbb{Z}_p$, $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ by Theorem 9.21. □

Ejemplo 15.11. Every group of order 15 is cyclic. This is true because $15 = 5 \cdot 3$ and $5 \not\equiv 1 \pmod 3$.

Ejemplo 15.12. Let us classify all of the groups of order $99 = 3^2 \cdot 11$ up to isomorphism. First we will show that every group G of order 99 is abelian. By the Third Sylow Theorem, there are $1+3k$ Sylow 3-subgroups, each of order 9, for some $k = 0, 1, 2, \ldots$. Also, $1 + 3k$ must divide 11; hence, there can only be a single normal Sylow 3-subgroup H in G. Similarly, there are $1 + 11k$ Sylow 11-subgroups and $1+11k$ must divide 9. Consequently, there is only one Sylow 11-subgroup K in G. By Corollary 14.16, any group of order p^2 is abelian for p prime; hence, H is isomorphic either to $\mathbb{Z}_3 \times \mathbb{Z}_3$ or to $\mathbb{Z}_9$. Since K has order 11, it must be isomorphic to $\mathbb{Z}_{11}$. Therefore, the only possible groups of order 99 are $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11}$ or $\mathbb{Z}_9 \times \mathbb{Z}_{11}$ up to isomorphism.

To determine all of the groups of order $5 \cdot 7 \cdot 47 = 1645$, we need the following theorem.

Teorema 15.13. *Let $G' = \langle aba^{-1}b^{-1} : a, b \in G \rangle$ be the subgroup consisting of all finite products of elements of the form $aba^{-1}b^{-1}$ in a group G. Then G' is a normal subgroup of G and G/G' is abelian.*

The subgroup G' of G is called the ***commutator subgroup*** of G. We leave the proof of this theorem as an exercise (Exercise 10.3.14 in Chapter 10).

Ejemplo 15.14. We will now show that every group of order $5 \cdot 7 \cdot 47 = 1645$ is abelian, and cyclic by Corollary 9.21. By the Third Sylow Theorem, G has only one subgroup H_1 of order 47. So G/H_1 has order 35 and must be abelian by Theorem 15.10. Hence, the commutator subgroup of G is contained in H which tells us that $|G'|$ is either 1 or 47. If $|G'| = 1$, we are done. Suppose that $|G'| = 47$. The Third Sylow Theorem tells us that G has only one subgroup of order 5 and one subgroup of order 7. So there exist normal subgroups H_2 and H_3 in G, where $|H_2| = 5$ and $|H_3| = 7$. In either case the quotient group is abelian; hence, G' must be a subgroup of H_i, $i = 1, 2$. Therefore, the order of G' is 1, 5, or 7. However, we already have determined that $|G'| = 1$ or 47. So the commutator subgroup of G is trivial, and consequently G is abelian.

Finite Simple Groups

Given a finite group, one can ask whether or not that group has any normal subgroups. Recall that a simple group is one with no proper nontrivial normal subgroups. As in the case of A_5, proving a group to be simple can be a very difficult task; however, the Sylow Theorems are useful tools for proving that a group is not simple. Usually, some sort of counting argument is involved.

Ejemplo 15.15. Let us show that no group G of order 20 can be simple. By the Third Sylow Theorem, G contains one or more Sylow 5-subgroups. The number of such subgroups is congruent to 1 (mod 5) and must also divide 20. The only possible such number is 1. Since there is only a single Sylow 5-subgroup and all Sylow 5-subgroups are conjugate, this subgroup must be normal.

Ejemplo 15.16. Let G be a finite group of order p^n, $n > 1$ and p prime. By Theorem 14.15, G has a nontrivial center. Since the center of any group G is a normal subgroup, G cannot be a simple group. Therefore, groups of orders 4, 8, 9, 16, 25, 27, 32, 49, 64, and 81 are not simple. In fact, the groups of order 4, 9, 25, and 49 are abelian by Corollary 14.16.

Ejemplo 15.17. No group of order $56 = 2^3 \cdot 7$ is simple. We have seen that if we can show that there is only one Sylow p-subgroup for some prime p dividing 56, then this must be a normal subgroup and we are done. By the Third Sylow Theorem, there are either one or eight Sylow 7-subgroups. If there is only a single Sylow 7-subgroup, then it must be normal.

On the other hand, suppose that there are eight Sylow 7-subgroups. Then each of these subgroups must be cyclic; hence, the intersection of any two of these subgroups contains only the identity of the group. This leaves $8 \cdot 6 = 48$ distinct elements in the group, each of order 7. Now let us count Sylow 2-subgroups. There are either one or seven Sylow 2-subgroups. Any element of a Sylow 2-subgroup other than the identity must have as its order a power of 2; and therefore cannot be one of the 48 elements of order 7 in the Sylow 7-subgroups. Since a Sylow 2-subgroup has order 8, there is only enough room for a single Sylow 2-subgroup in a group of order 56. If there is only one Sylow 2-subgroup, it must be normal.

For other groups G, it is more difficult to prove that G is not simple. Suppose G has order 48. In this case the technique that we employed in the last example will not work. We need the following lemma to prove that no group of order 48 is simple.

Lema 15.18. *Let H and K be finite subgroups of a group G. Then*

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Demostración. Recall that

$$HK = \{hk : h \in H, k \in K\}.$$

Certainly, $|HK| \leq |H| \cdot |K|$ since some element in HK could be written as the product of different elements in H and K. It is quite possible that $h_1k_1 = h_2k_2$ for $h_1, h_2 \in H$ and $k_1, k_2 \in K$. If this is the case, let

$$a = (h_1)^{-1}h_2 = k_1(k_2)^{-1}.$$

Notice that $a \in H \cap K$, since $(h_1)^{-1}h_2$ is in H and $k_2(k_1)^{-1}$ is in K; consequently,

$$h_2 = h_1a^{-1}$$
$$k_2 = ak_1.$$

Conversely, let $h = h_1b^{-1}$ and $k = bk_1$ for $b \in H \cap K$. Then $hk = h_1k_1$, where $h \in H$ and $k \in K$. Hence, any element $hk \in HK$ can be written in the form h_ik_i for $h_i \in H$ and $k_i \in K$, as many times as there are elements in $H \cap K$; that is, $|H \cap K|$ times. Therefore, $|HK| = (|H| \cdot |K|)/|H \cap K|$. □

Ejemplo 15.19. To demonstrate that a group G of order 48 is not simple, we will show that G contains either a normal subgroup of order 8 or a normal subgroup of order 16. By the Third Sylow Theorem, G has either one or three Sylow 2-subgroups of order 16. If there is only one subgroup, then it must be a normal subgroup.

Suppose that the other case is true, and two of the three Sylow 2-subgroups are H and K. We claim that $|H \cap K| = 8$. If $|H \cap K| \leq 4$, then by Lemma 15.18,

$$|HK| = \frac{16 \cdot 16}{4} = 64,$$

which is impossible. Notice that $H \cap K$ has index two in both of H and K, so is normal in both, and thus H and K are each in the normalizer of $H \cap K$. Because H is a subgroup of $N(H \cap K)$ and because $N(H \cap K)$ has strictly more than 16 elements, $|N(H \cap K)|$ must be a multiple of 16 greater than 1, as well as dividing 48. The only possibility is that $|N(H \cap K)| = 48$. Hence, $N(H \cap K) = G$.

The following famous conjecture of Burnside was proved in a long and difficult paper by Feit and Thompson [2].

Teorema 15.20 (Odd Order Theorem)**.** *Every finite simple group of nonprime order must be of even order.*

The proof of this theorem laid the groundwork for a program in the 1960s and 1970s that classified all finite simple groups. The success of this program is one of the outstanding achievements of modern mathematics.

Sage Sage will compute a single Sylow p-subgroup for each prime divisor p of the order of the group. Then, with conjugacy, all of the Sylow p-subgroups can be enumerated. It is also possible to compute the normalizer of a subgroup.

15.3 Exercises

1. What are the orders of all Sylow p-subgroups where G has order 18, 24, 54, 72, and 80?

2. Find all the Sylow 3-subgroups of S_4 and show that they are all conjugate.

3. Show that every group of order 45 has a normal subgroup of order 9.

4. Let H be a Sylow p-subgroup of G. Prove that H is the only Sylow p-subgroup of G contained in $N(H)$.

5. Prove that no group of order 96 is simple.

6. Prove that no group of order 160 is simple.

7. If H is a normal subgroup of a finite group G and $|H| = p^k$ for some prime p, show that H is contained in every Sylow p-subgroup of G.

8. Let G be a group of order p^2q^2, where p and q are distinct primes such that $q \nmid p^2 - 1$ and $p \nmid q^2 - 1$. Prove that G must be abelian. Find a pair of primes for which this is true.

9. Show that a group of order 33 has only one Sylow 3-subgroup.

10. Let H be a subgroup of a group G. Prove or disprove that the normalizer of H is normal in G.

11. Let G be a finite group divisible by a prime p. Prove that if there is only one Sylow p-subgroup in G, it must be a normal subgroup of G.

12. Let G be a group of order p^r, p prime. Prove that G contains a normal subgroup of order p^{r-1}.

13. Suppose that G is a finite group of order $p^n k$, where $k < p$. Show that G must contain a normal subgroup.

14. Let H be a subgroup of a finite group G. Prove that $gN(H)g^{-1} = N(gHg^{-1})$ for any $g \in G$.

15. Prove that a group of order 108 must have a normal subgroup.

16. Classify all the groups of order 175 up to isomorphism.

17. Show that every group of order 255 is cyclic.

18. Let G have order $p_1^{e_1} \cdots p_n^{e_n}$ and suppose that G has n Sylow p-subgroups $P_1, \ldots, P_n$ where $|P_i| = p_i^{e_i}$. Prove that G is isomorphic to $P_1 \times \cdots \times P_n$.

19. Let P be a normal Sylow p-subgroup of G. Prove that every inner automorphism of G fixes P.

20. What is the smallest possible order of a group G such that G is nonabelian and $|G|$ is odd? Can you find such a group?

21. (The Frattini Lemma) If H is a normal subgroup of a finite group G and P is a Sylow p-subgroup of H, for each $g \in G$ show that there is an h in H such that $gPg^{-1} = hPh^{-1}$. Also, show that if N is the normalizer of P, then $G = HN$.

22. Show that if the order of G is $p^n q$, where p and q are primes and $p > q$, then G contains a normal subgroup.

23. Prove that the number of distinct conjugates of a subgroup H of a finite group G is $[G : N(H)]$.

24. Prove that a Sylow 2-subgroup of S_5 is isomorphic to D_4.

25. (Another Proof of the Sylow Theorems)

(a) Suppose p is prime and p does not divide m. Show that

$$p \nmid \binom{p^k m}{p^k}.$$

(b) Let $\mathcal{S}$ denote the set of all p^k element subsets of G. Show that p does not divide $|\mathcal{S}|$.

(c) Define an action of G on $\mathcal{S}$ by left multiplication, $aT = \{at : t \in T\}$ for $a \in G$ and $T \in \mathcal{S}$. Prove that this is a group action.

(d) Prove $p \nmid |\mathcal{O}_T|$ for some $T \in \mathcal{S}$.

(e) Let $\{T_1, \ldots, T_u\}$ be an orbit such that $p \nmid u$ and $H = \{g \in G : gT_1 = T_1\}$. Prove that H is a subgroup of G and show that $|G| = u|H|$.

(f) Show that p^k divides $|H|$ and $p^k \leq |H|$.

(g) Show that $|H| = |\mathcal{O}_T| \leq p^k$; conclude that therefore $p^k = |H|$.

26. Let G be a group. Prove that $G' = \langle aba^{-1}b^{-1} : a, b \in G \rangle$ is a normal subgroup of G and G/G' is abelian. Find an example to show that $\{aba^{-1}b^{-1} : a, b \in G\}$ is not necessarily a group.

15.4 A Project

The main objective of finite group theory is to classify all possible finite groups up to isomorphism. This problem is very difficult even if we try to classify the groups of order less than or equal to 60. However, we can break the problem down into several intermediate problems. This is a challenging project that requires a working knowledge of the group theory you have learned up to this

point. Even if you do not complete it, it will teach you a great deal about finite groups. You can use Table 15.21 as a guide.

Order	Number	Order	Number	Order	Number	Order	Number
1	?	16	14	31	1	46	2
2	?	17	1	32	51	47	1
3	?	18	?	33	1	48	52
4	?	19	?	34	?	49	?
5	?	20	5	35	1	50	5
6	?	21	?	36	14	51	?
7	?	22	2	37	1	52	?
8	?	23	1	38	?	53	?
9	?	24	?	39	2	54	15
10	?	25	2	40	14	55	2
11	?	26	2	41	1	56	?
12	5	27	5	42	?	57	2
13	?	28	?	43	1	58	?
14	?	29	1	44	4	59	1
15	1	30	4	45	?	60	13

Cuadro 15.21: Numbers of distinct groups G, $|G| \leq 60$

1. Find all simple groups G ($|G| \leq 60$). *Do not use the Odd Order Theorem unless you are prepared to prove it.*

2. Find the number of distinct groups G, where the order of G is n for $n = 1, \ldots, 60$.

3. Find the actual groups (up to isomorphism) for each n.

15.5 References and Suggested Readings

[1] Edwards, H. "A Short History of the Fields Medal," *Mathematical Intelligencer* **1**(1978), 127–29.

[2] Feit, W. and Thompson, J. G. "Solvability of Groups of Odd Order," *Pacific Journal of Mathematics* **13**(1963), 775–1029.

[3] Gallian, J. A. "The Search for Finite Simple Groups," *Mathematics Magazine* **49**(1976), 163–79.

[4] Gorenstein, D. "Classifying the Finite Simple Groups," *Bulletin of the American Mathematical Society* **14**(1986), 1–98.

[5] Gorenstein, D. *Finite Groups*. AMS Chelsea Publishing, Providence RI, 1968.

[6] Gorenstein, D., Lyons, R., and Solomon, R. *The Classification of Finite Simple Groups*. American Mathematical Society, Providence RI, 1994.

15.6 Sage

Subgrupos de Sylow

El método `.sylow_subgroup(p)`, implementaado para grupos de permutaciones, entregará un p-subgrupo de Sylow. Si el primo no es un divisor propio del orden

del grupo devuelve un subgrupo de orden p^0, en otras palabras, el subgrupo trivial. A veces, solo necesitaremos *un* subgrupo de Sylow, pues cualquiera dos p-subgrupos de Sylow son conjugados, y por ende isomorfos (Teorema 15.7). Esto también quiere decir que podemos crear otros p-subgrupos de Sylow conjugando el que obtuvimos. El método `.conjugate(g)` conjugará el grupo por `g`.

Mediante conjugaciones de un solo p-subgrupo de Sylow p, siempre obtendremos subgrupos repetidos. Necesitamos una construcción un poco más complicada para formar una lista que contenga cada p-subgrupo de Sylow exactamente una vez. La siguiente rutina que calcula todos los p-subgrupos de Sylow será útil para lo que queda de esta sección. Se podría hacer más eficiente conjugando solo por un elemento de cada clase lateral del normalizador, pero es suficiente para nuestros propósitos acá. Asegúrese de ejecutar la próxima celda, para poder usar la función más adelante.

```
def all_sylow(G, p):
    '''Form the set of all distinct Sylow p-subgroups of G'''
    scriptP = []
    P = G.sylow_subgroup(p)
    for x in G:
        H = P.conjugate(x)
        if not(H in scriptP):
            scriptP.append(H)
    return scriptP
```

Investiguemos los subgrupos de Sylow del grupo dihedral D_{18}. Como grupo de orden $36 = 2^2 \cdot 3^2$, sabemos por el Primer Teorema de Sylow que tiene un 2-subgrupo de orden 4 y un 3-subgrupo de Sylow de orden 9. Comenzando con $p = 2$, obtenemos un 2-subgrupo de Sylow, formamos todos sus conjugados, y formamos una lista de los subgrupos sin repeticiones.

```
G = DihedralGroup(18)
S2 = G.sylow_subgroup(2); S2
```

```
Subgroup of (Dihedral group of order 36 as a permutation
    group)
generated by
[(2,18)(3,17)(4,16)(5,15)(6,14)(7,13)(8,12)(9,11),
(1,10)(2,11)(3,12)(4,13)(5,14)(6,15)(7,16)(8,17)(9,18)]
```

```
uniqS2 = all_sylow(G, 2)
uniqS2
```

```
[Permutation Group with generators
 [(2,18)(3,17)(4,16)(5,15)(6,14)(7,13)(8,12)(9,11),
 (1,10)(2,11)(3,12)(4,13)(5,14)(6,15)(7,16)(8,17)(9,18)],
 Permutation Group with generators
 [(1,3)(4,18)(5,17)(6,16)(7,15)(8,14)(9,13)(10,12),
 (1,10)(2,11)(3,12)(4,13)(5,14)(6,15)(7,16)(8,17)(9,18)],
 Permutation Group with generators
 [(1,10)(2,11)(3,12)(4,13)(5,14)(6,15)(7,16)(8,17)(9,18),
 (1,17)(2,16)(3,15)(4,14)(5,13)(6,12)(7,11)(8,10)],
 Permutation Group with generators
 [(1,5)(2,4)(6,18)(7,17)(8,16)(9,15)(10,14)(11,13),
 (1,10)(2,11)(3,12)(4,13)(5,14)(6,15)(7,16)(8,17)(9,18)],
 Permutation Group with generators
 [(1,10)(2,11)(3,12)(4,13)(5,14)(6,15)(7,16)(8,17)(9,18),
 (1,15)(2,14)(3,13)(4,12)(5,11)(6,10)(7,9)(16,18)],
```

```
Permutation Group with generators
[(1,10)(2,11)(3,12)(4,13)(5,14)(6,15)(7,16)(8,17)(9,18),
(1,13)(2,12)(3,11)(4,10)(5,9)(6,8)(14,18)(15,17)],
Permutation Group with generators
[(1,7)(2,6)(3,5)(8,18)(9,17)(10,16)(11,15)(12,14),
(1,10)(2,11)(3,12)(4,13)(5,14)(6,15)(7,16)(8,17)(9,18)],
Permutation Group with generators
[(1,10)(2,11)(3,12)(4,13)(5,14)(6,15)(7,16)(8,17)(9,18),
(1,11)(2,10)(3,9)(4,8)(5,7)(12,18)(13,17)(14,16)],
Permutation Group with generators
[(1,9)(2,8)(3,7)(4,6)(10,18)(11,17)(12,16)(13,15),
(1,10)(2,11)(3,12)(4,13)(5,14)(6,15)(7,16)(8,17)(9,18)]]
```

```
len(uniqS2)
```

```
9
```

El Tercer Teorema de Sylow nos dice que para $p = 2$ podríamos tener $1, 3$ o 9 2-subgrupos de Sylow, de manera que los 9 subgrupos obtenidos son consistentes con lo que predice la teoría. ¿Puede visualizar cada uno de estos subgrupos como simetrías de un polígono regular de 18 lados? Notemos que también tenemos muchos subgrupos de orden 2 dentro de estos subgrupos de orden 4.

Ahora para $p = 3$.

```
G = DihedralGroup(18)
S3 = G.sylow_subgroup(3); S3
```

```
Subgroup of (Dihedral group of order 36 as a permutation
    group)
generated by
[(1,7,13)(2,8,14)(3,9,15)(4,10,16)(5,11,17)(6,12,18),
(1,15,11,7,3,17,13,9,5)(2,16,12,8,4,18,14,10,6)]
```

```
uniqS3 = all_sylow(G, 3)
uniqS3
```

```
[Permutation Group with generators
[(1,7,13)(2,8,14)(3,9,15)(4,10,16)(5,11,17)(6,12,18),
(1,15,11,7,3,17,13,9,5)(2,16,12,8,4,18,14,10,6)]]
```

```
len(uniqS3)
```

```
1
```

¿Qué es lo que predice el Tercer Teorema de Sylow? Habiendo encontrado solo un subgrupo de Sylow computacionalmente, sabemos que todos los conjugados de este único 3-subgrupo de Sylow son iguales. En otras palabras el 3-subgrupo de Sylow es normal en D_{18}. Comprobémoslo de todas formas.

```
S3.is_normal(G)
```

```
True
```

Al menos uno de los subgrupos de orden 3 contenidos en este 3-subgrupo de Sylow debiese ser obvio mirando los órdenes de los generadores, y luego podríamos incluso darnos cuenta que los generadores dados se pueden reducir, y uno es una potencia del otro.

```
S3.is_cyclic()
```

```
True
```

Recuerde que existen muchos otros subgrupos, de otros órdenes. Por ejemplo, ¿puede construir un subgrupo de oreden $6 = 2 \cdot 3$ en D_{18}?

Normalizadores

Un comando nuevo que resulta relevante para esta sección es la construcción del normalizador. El comando `G.normalizer(H)` devolverá el subgrupo de `G` que contiene todos los elementos que normalizan al subgrupo `H`. Ilustraremos su uso con los subgrupos de Sylow de arriba.

```
G = DihedralGroup(18)
S2 = G.sylow_subgroup(2)
S3 = G.sylow_subgroup(3)
N2 = G.normalizer(S2); N2
```

```
Subgroup of (Dihedral group of order 36 as a permutation
    group)
generated by
[(2,18)(3,17)(4,16)(5,15)(6,14)(7,13)(8,12)(9,11),
(1,10)(2,11)(3,12)(4,13)(5,14)(6,15)(7,16)(8,17)(9,18)]
```

```
N2 == S2
```

```
True
```

```
N3 = G.normalizer(S3); N3
```

```
Subgroup of (Dihedral group of order 36 as a permutation
    group)
generated by
[(2,18)(3,17)(4,16)(5,15)(6,14)(7,13)(8,12)(9,11),
(1,2)(3,18)(4,17)(5,16)(6,15)(7,14)(8,13)(9,12)(10,11),
(1,7,13)(2,8,14)(3,9,15)(4,10,16)(5,11,17)(6,12,18),
(1,15,11,7,3,17,13,9,5)(2,16,12,8,4,18,14,10,6)]
```

```
N3 == G
```

```
True
```

El normalizador de n subgrupo siempre contiene al subgrupo, de manera que el normalizador de `S2` este todo lo pequeño que puede ser. Ya sabíamos que `S3` es normal en `G`, así es que no es sorprendente que su normalizador sea todo llo grande que puede ser — todo elemento de `G` normaliza a `S3`. Calculemos un normalizador más "interesante" en D_{18}

```
G = DihedralGroup(18)
a = G("(1,7,13)(2,8,14)(3,9,15)(4,10,16)(5,11,17)(6,12,18)")
b = G("(1,5)(2,4)(6,18)(7,17)(8,16)(9,15)(10,14)(11,13)")
H = G.subgroup([a, b])
H.order()
```

```
6
```

```
N = G.normalizer(H)
N
```

```
Subgroup of (Dihedral group of order 36 as a permutation
    group)
generated by
[(1,2)(3,18)(4,17)(5,16)(6,15)(7,14)(8,13)(9,12)(10,11),
(1,5)(2,4)(6,18)(7,17)(8,16)(9,15)(10,14)(11,13),
(1,13,7)(2,14,8)(3,15,9)(4,16,10)(5,17,11)(6,18,12)]
```

```
N.order()
```

```
12
```

Para este subgrupo de orden 6, el normalizador es estrictamente más grande que el subgrupo, pero estrictamente menor que el grupo completo (y por ende no es normal en el grupo dihedral). Trivialmente, un subgrupo es normal en su normalizador:

```
H.is_normal(G)
```

```
False
```

```
H.is_normal(N)
```

```
True
```

Grupos Finitos Simples

Ya vimos el método `.is_simple()`. En el Ejemplo 15.16 que un grupo de orden 64 nunca es simple. El grupo dicíclico `DiCyclicGroup(16)` es un grupo no-abeliano de orden 64, así es que podemos poner a prueba el método con este grupo. Resulta que este grupo tiene muchos subgrupos normales — la lista siempre contendrá al grupo trivial y al grupo completo, así cualquier número mayor a 2 indica un subgrupo normal no-trivial.

```
DC=DiCyclicGroup(16)
DC.order()
```

```
64
```

```
DC.is_simple()
```

```
False
```

```
ns = DC.normal_subgroups()
len(ns)
```

```
9
```

Acá viene un grupo bastante interesante, uno de los 26 grupos simles esporádicos, conocido como el grupo de Higman-Sims, HS. Los generadores usados abajo vienen de su representación permutacional en 100 puntos en formato GAP, disponible en web.mat.bham.ac.uk/atlas/v2.0/spor/HS/. Dos generadores, uno de orden 2 y otro de orden 5 (como se puede ver fácilmente), generando 44 352 000 elementos, pero ningún subgrupo normal. Impresionante.

```
G = SymmetricGroup(100)
a = G([(1,60),  (2,72),  (3,81),  (4,43),  (5,11),  (6,87),
       (7,34),  (9,63),  (12,46), (13,28), (14,71), (15,42),
```

```
        (16,97), (18,57), (19,52), (21,32), (23,47), (24,54),
        (25,83), (26,78), (29,89), (30,39), (33,61), (35,56),
        (37,67), (44,76), (45,88), (48,59), (49,86), (50,74),
        (51,66), (53,99), (55,75), (62,73), (65,79), (68,82),
        (77,92), (84,90), (85,98), (94,100)])
b = G([(1,86,13,10,47),  (2,53,30,8,38),
        (3,40,48,25,17),  (4,29,92,88,43),   (5,98,66,54,
            65),
        (6,27,51,73,24),  (7,83,16,20,28),   (9,23,89,95,61),
        (11,42,46,91,32), (12,14, 81,55,68),
            (15,90,31,56,37),
        (18,69,45,84,76), (19,59,79,35,93),
            (21,22,64,39,100),
        (26,58,96,85,77), (33,52,94,75,44),
            (34,62,87,78,50),
        (36,82,60,74,72), (41,80,70,49,67),
            (57,63,71,99,97)])
a.order(), b.order()
```

```
(2, 5)
```

```
HS = G.subgroup([a, b])
HS.order()
```

```
44352000
```

```
HS.is_simple()
```

```
True
```

Vimos antes este grupo en los Ejercicios del Capítulo 14 sobre acciones de grupo, donde era el único subgrupo normal no trivial del grupo de automorfismos del grafo de Higman-Sims, de ahí su nombre.

Consola e Interfaz GAP

Acá concluimos el estudio exclusivo de teoría de grupos, aunque seguiremos usando algunos grupos en las secciones que siguientes. Como ya hemos destacado, mucho del lo que hace Sage con grupos es realizado por el programa de código aberto, "Groups, Algorithms, and Programming," más conocido como GAP. Si luego de este curso, sus necesidades superan la capacidad de Sage en relación a grupos, entonces aprender GAP sería el próximo paso como teórico de grupos. Cada copia de Sage incluye una copia de GAP y se puede saber fácilmente cuál es la versión de GAP incluida:

```
gap.version()
```

```
'4.8.6'
```

En Sage se puede interactuar con GAP de diferentes formas. La mñas directa es creando un grupo de permutaciones por medio del comando `gap()` de Sage.

```
G = gap('Group(␣(1,2,3,4,5,6),␣(1,3,5)␣)')
G
```

```
Group( [ (1,2,3,4,5,6), (1,3,5) ] )
```

Ahora podemos usar casi cualquier comando GAP con `G`, via la convención de que la mayoría de los comandos en GAP esperan recibir un grupo como su primer argumento, y en su lugar proveemos el grupo usando la sintaxis orientada al objeto `G.`. Si consulta un manual de GAP verá que `Center` es un comando GAP que toma un grupo como su único argumento, y `Centralizer` es un comando GAP que requiere dos argumentos — un grupo y luego un elemento del grupo.

```
G.Center()
```

```
Group( [ ( 1, 3, 5)( 2, 4, 6) ] )
```

```
G.Centralizer('(1,␣3,␣5)')
```

```
Group( [ (1,3,5), (2,4,6), (1,3,5)(2,4,6) ] )
```

Si usa la interfaz Notebook de Sage puede poner `%gap` en la primera línea de una celda y la celda completa se interpretará como si estuviera interactuando directamente cong GAP. Esto significa que ahora puede (y debe) usar la sintaxis de GAP, que como puede ver arriba, es ligeramente diferente a la Sintaxis de Sage. También se puede usar el menú en el comienzo de la página para seleccionar `gap` en lugar de `sage` y la hoja de trabajo completa será interpretada como GAP. Acá un ejemplo simple, que debiera poder ejecutar en su hoja de trabajo actual. Este ejemplo particular no correrá bien en una celda Sage en la versión web de esta sección.

```
%gap
G := Group( (1,2,3,4,5,6), (1,3,5) );
Centralizer(G, (1,3,5));
```

Notemos que

- No es necesario encerrar las permutaciones individuales con tantas cremillas como haríamos en Sage.
- La asignación es `:=` not `=`. Si olvida los dos puntos, obtendrá un error del tipo `Variable: 'G' must have a value`
- Una línea *debe* terminar en punto y coma (;). Si olvida el punto y coma al final la línea, las líneas se fusionarán como si fuera una sola.

Puede obtener ayuda sobr los comandos en GAP como se muestra más abajo, pero pronto se dará cuenta que GAP supone que usted sabe más álgebra de lo que supone Sage.

```
print(gap.help('SymmetricGroup', pager=False))
```

En la versión de línea de comando de Sage, también es posible usar la "consola" GAP. Nuevamente, será necesario usar la sintaxis de GAP, y no tendrá muchas de las comodidades del Notebook Sage. También es bueno saber de antemano que `quit;` es la forma de salir de la consola GAP y volver a Sage. Si corre Sage en la línea de comando, use el comando `gap_console()` para iniciar GAP.

Es reconfortante saber que con Sage tenemos una copia completa de GAP, instalada y lista para correr. Pero, este no es un tutorial de GAP, así es que si le interesa, puede consultar la página oficial de GAP: www.gap-system.org para aprender más sobre GAP.

15.7 Ejercicios en Sage

1. Este ejercicio ejemplifica el Teorema 15.13. El subgrupo conmutador se puede obtener con el método `.commutator()`. Para el grupo dihedral de orden 40, D_{20} (`DihedralGroup(20)` en Sage), calcule el subgrupo conmutador y forme el cociente del grupo dihedral por este subgrupo. Compruebe que este cocienet es abeliano. ¿Puede identificar a qué grupo conocido es isomorfo este cociente?

2. Para cada primo para el que tenga sentido, encuentre todos los p-subgrupos de Sylow del grupo alternante A_5. Confirme que sus resultados son consistentes con el Terecer Teorema de Sylow Theorem para cada primo. Sabemos que A_5 es un grupo simple. Diga por qué esto podría ayudar a explicar cierto aspecto de sus respuestas.
Cuente el número total de elementos distintos contenidos en la unión de todos los subgrupos de Sylow que acaba de encontrar. ¿Qué le parece interesante de esta cuenta?

3. Para el grupo dihedral D_{36} (simetrías de un polígono regular de 36 lados) y para cada primo, determine los posibles valores para el número de $p$subgrupos de Sylow según lo establecido en el Tercer Teorema de Sylow(15.8). Ahora calcule el número efectivo de $p$subgrupos de Sylow para cada primo y comente sobre el resultado.
Es posible demostrar que *ningún grupo* de orden 72 es un grupo simple, usando técnicas como las usadas en los últimos ejemplos de este capítulo. Discuta este resultado en el contexto de sus cálculos con Sage.

4. Este ejercicio ejemplifica el Lema 15.6. Sea G el grupo dihedral de orden 36, D_{18}. Sea H uno de los 3-subgrupos de Sylow. Sea K el subgrupo de orden 6 generado por las dos permutaciones `a` y `b` dadas abajo. Primero, forme una lista de los distintos conjugados de K por los elementos de H, y cuente el número de subgrupos en esta lista. Compare esto con el índice dado en el eneunciado del lema, empleando un solo comando (largo) que haga uso de los métodos `.order()`, `.normalizer()` y `.intersection()` aplicados a G, H y K, *solamente*.

```
G = DihedralGroup(18)
a = G("(1,7,13)(2,8,14)(3,9,15)(4,10,16)(5,11,17)(6,12,18)")
b = G("(1,5)(2,4)(6,18)(7,17)(8,16)(9,15)(10,14)(11,13)")
```

5. El Ejemplo 15.19 muestra que todo grupo de orden 48 tiene un subgrupo normal. Los grupos dicíclicos forman una familia infinita de grupos no-abelianos de orden $4n$, que incluye al grupo de los cuaterniones (el caso $n = 2$). El grupo `DiCyclicGroup(12)` tiene orden 48. Use Sage para ilustrar la lógica de la demostración en el Ejemplo 15.19 y obtenga un subgrupo normal. (En otras palabras, no pida simplemente la lista de subgrupos normales, sino siga las implicaciones del ejemplo para arribar a un subgrupo normal, y luego compruebe su respuesta.)

6. Las demostraciones del Segundo y Tercer Teorema de Sylow (15.7, 15.8) emplean una acción de grupo en conjuntos de p-subgrupos de Sylow p. Para el Segundo Teorema, la lista se propone como incompleta y luego se demuestra que contiene *todos* los p-subgrupos de Sylow. En este ejercicio veremos como se comportan estas acciones, y como se diferencian cuando usamos distintos grupos actuando en el mismo conjunto.
Construya los seis 5-subgrupos de Sylow del grupo alternante A_5. Este será el conjunto de objetos para nuestras dos acciones. La conjugación de uno de estos 5-subgrupos de Sylow por un elemento de A_5 producirá otro 5-subgrupo

de Sylow, y puede por lo tanto ser usada para definir una acción de grupo. Para una tal acción, para cada elemento del grupo, forme una permutación en Sage numerando los seis subgrupos y usando esos enteros como etiquetas para los subgrupos. El método para listas `.index()` de Python le será muy útil. Ahora use todas estas permutaciones para generar un grupo de permutaciones (un subgrupo de S_6). Finalmente, use métodos de grupos de permutaciones para la obtención de órbitas y estabilizadores, etc. para explorar las acciones.
Para la primera acción, utilice todo A_5 como su grupo. Muestre que la acción resultante es transitiva. En otras palabras, existe una sola órbita.
Para la segunda acción, use uno de los 5-subgrupos de Sylow como su grupo. Escriba la ecuación de clases para esta acción que sugiera la parte "congruencia a 1 mod p" de las conclusiones del Tercer Teorema.

16

Anillos

Hasta ahora hemos estudiado conjuntos con una sola operación binaria que satisface ciertos axiomas, pero muchas veces estamos más interesados en trabajar con conjuntos que tienen dos operaciones binarias. Por ejemplo, una de las estructuras algebraicas más naturales de estudiar es la de los enteros con las operaciones de adición y multiplicación. Estas operaciones están relacionadas por la propiedad distributiva. Al considerar un conjunto con dos operaciones binarias relacionadas así, que satisfacen ciertos axiomas, tenemos una estructura algebraica llamada anillo. En un anillo sumamos y multiplicamos elementos tales como los números reales, los números complejos, matrices y funciones.

16.1 Anillos

Un conjunto no vacío R es un ***anillo*** si tiene dos operaciones binarias, adición y multiplicación, que satisfacen las siguientes condiciones.

1. $a + b = b + a$ for $a, b \in R$.
2. $(a + b) + c = a + (b + c)$ for $a, b, c \in R$.
3. There is an element 0 in R such that $a + 0 = a$ for all $a \in R$.
4. For every element $a \in R$, there exists an element $-a$ in R such that $a + (-a) = 0$.
5. $(ab)c = a(bc)$ for $a, b, c \in R$.
6. For $a, b, c \in R$,

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc.$$

Esta última consición, el axioma de la distributividad, relaciona las operaciones binarias de adición y multiplicación. Note que los primeros cuatro axiomas simplemente requieren que un anillo sea un grupo abeliano con la operación de adición, de manera que podríamos haber definido un anillo como un grupo abeliano $(R, +)$ junto con una operación secundariaque satisface los axiomas quinto y sexto dados arriba.

Si existe un elemento $1 \in R$ tal que $1 \neq 0$ y $1a = a1 = a$ para cada elemento $a \in R$, decimos que tal anillo R es un anillo con ***unidad*** o ***identidad***. Un anillo R para el cual $ab = ba$ para todo a, b en R se llama ***anillo conmutativo***. un anillo conmutativo R con identidad se llama ***dominio integral*** si, para $a, b \in R$ tales que $ab = 0$, se cumple $a = 0$ o $b = 0$. Un ***anillo de división*** es

un anillo R, con identidad, en el que todo elemento distinto de cero en R es una ***unidad***; es decir, para cada $a \in R$ con $a \neq 0$, existe un único elemento a^{-1} tal que $a^{-1}a = aa^{-1} = 1$. Un anillo de división conmutativo se llama ***cuerpo***. La relación entre anillos, dominios integrales, anillos de división y cuerpos se muestra en la Figura 16.1.

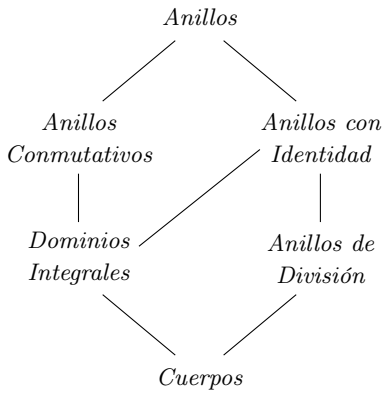


Figura 16.1: Tipos de anillos

Ejemplo 16.2. Como mencionamos antes, los enteros forman un anillo. De hecho, $\mathbb{Z}$ es un dominio integral. De hecho si $ab = 0$ para dos enteros a y b, ya sea $a = 0$ o $b = 0$. Sin embargo, $\mathbb{Z}$ no e sun cuerpo. No hay un entero que sea el inverso multiplicativo de 2, pues $1/2$ no es un entero. Los únicos enteros con inverso multiplicativo son 1 y -1.

Ejemplo 16.3. Bajo las operaciones usuales de adición y multiplicación, todos los sistemas de números familiares son anillos: los racionales, $\mathbb{Q}$; los números reales, $\mathbb{R}$; y los números complejos, $\mathbb{C}$. Cada uno de estos anillos es un cuerpo.

Ejemplo 16.4. Podemos definir el producto de dos elementos a y b en $\mathbb{Z}_n$ como $ab \pmod{n}$. Por ejemplo, en $\mathbb{Z}_{12}$, $5 \cdot 7 \equiv 11 \pmod{12}$. Este producto convierte el grupo abeliano $\mathbb{Z}_n$ en un anillo. De hecho $\mathbb{Z}_n$ es un anillo conmutativo; sin embargo, puede que no se un dominio integral. Si consideramos $3 \cdot 4 \equiv 0 \pmod{12}$ en $\mathbb{Z}_{12}$, es fácil ver que el producto de dos elementos distintos de cero en el anillo puede ser igual a cero.

Un elemento distinto de cero a en un anillo R se dice ***divisor de cero*** si existe un elemento b distinto de cero en R tal que $ab = 0$. En el ejemplo anterior, 3 y 4 son divisores de cero en $\mathbb{Z}_{12}$.

Ejemplo 16.5. El conjunto de funciones reales continuos definidas en un intervalo $[a, b]$ forman un anillo conmutativo. La suma y el producto de dos funciones se definen sumando y multiplicando respectvamente los valores de las funciones. Si $f(x) = x^2$ y $g(x) = \cos x$, entonces $(f+g)(x) = f(x)+g(x) = x^2 + \cos x$ y $(fg)(x) = f(x)g(x) = x^2 \cos x$.

Ejemplo 16.6. Las matrices de 2×2 con coeficientes en $\mathbb{R}$ forman un anillo bajo las operaciones usuales de suma y multiplicacón de matrices. Este anillo es no conmutativo, pues en general $AB \neq BA$. Notemos además, que podemos tener $AB = 0$ sin que A ni B sea cero.

Ejemplo 16.7. Para un ejemplo de un anillo de división no conmutativo, sea

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

con $i^2 = -1$. Estos elementos satisfacen las siguientes relaciones:

$$\begin{aligned}
\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 &= -1 \\
\mathbf{ij} &= \mathbf{k} \\
\mathbf{jk} &= \mathbf{i} \\
\mathbf{ki} &= \mathbf{j} \\
\mathbf{ji} &= -\mathbf{k} \\
\mathbf{kj} &= -\mathbf{i} \\
\mathbf{ik} &= -\mathbf{j}.
\end{aligned}$$

Sea $\mathbb{H}$ el conjunto de todos los elementos de la forma $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, donde a, b, c, d son números reales. Equivalentemente, $\mathbb{H}$ se puede considerar como el conjunto de todas las matrices de 2×2 de la forma

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix},$$

donde $\alpha = a + di$ y $\beta = b + ci$ son números complejos. Podemos definir la suma y la multiplicación en $\mathbb{H}$ en términos de la multiplicación usual de matrices o en términos de sus generadores 1, $\mathbf{i}$, $\mathbf{j}$, y $\mathbf{k}$:

$$\begin{aligned}
&(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) + (a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) \\
&= (a_1 + a_2) + (b_1 + b_2)\mathbf{i} + (c_1 + c_2)\mathbf{j} + (d_1 + d_2)\mathbf{k}
\end{aligned}$$

y

$$(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k})(a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k},$$

donde

$$\begin{aligned}
\alpha &= a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 \\
\beta &= a_1b_2 + a_2b_1 + c_1d_2 - d_1c_2 \\
\gamma &= a_1c_2 - b_1d_2 + c_1a_2 - d_1b_2 \\
\delta &= a_1d_2 + b_1c_2 - c_1b_2 - d_1a_2.
\end{aligned}$$

Aunque la multiplicación se ve complicada, en realidad es un un cálculo directo si recordamos que sumamos y multiplicamos elementos en $\mathbb{H}$ como polinomios teniendo en consideración las relaciones entre los generadores $\mathbf{i}$, $\mathbf{j}$, y $\mathbf{k}$. El anillo $\mathbb{H}$ se llama anillo de ***cuaterniones***.

Para mostrar que los cuaterniones forman un anillo de división, debemos ser capaces de encontrar un inverso para cada elemento distinto de cero. Note que

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) = a^2 + b^2 + c^2 + d^2.$$

Este elemento es cero solo si a, b, c, y d son todos cero. Así si $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \neq 0$,

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \left(\frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2} \right) = 1.$$

Proposición 16.8. *Sea R un anillo con $a, b \in R$. Entonces*

1. $a0 = 0a = 0$;
2. $a(-b) = (-a)b = -ab$;
3. $(-a)(-b) = ab$.

DEMOSTRACIÓN. Para demostra (1), notemos que

$$a0 = a(0+0) = a0 + a0;$$

luego, $a0 = 0$. Similarmente, $0a = 0$. Para (2), tenemos $ab + a(-b) = a(b-b) = a0 = 0$; por lo tanto, $-ab = a(-b)$. Similarmente, $-ab = (-a)b$. La parte (3) sigue directamente de (2) pues $(-a)(-b) = -(a(-b)) = -(-ab) = ab$. □

Así como tenemos subgrupos de grupos, tenemos una clase análoga de subestructuras para anillos. Un ***subanillo*** S de un anillo R es nu subconjunto S de R tal que S también es un anillo con las operaciones heredadas de R.

Ejemplo 16.9. El anillo $n\mathbb{Z}$ es un subanillo de $\mathbb{Z}$. Note que si bien el anillo original pueda tener una identidad, no pedimos que su subanillo tenga una identidad. Tenemos la siguiente cadena de subanillos:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

La siguiente proposición nos entrega criterios sencillos para determinar si un subconjunto de un anillo es o no es un subanillo. (Dejaremos la demostración de esta proposición como ejercicio.)

Proposición 16.10. *Sea R un anillo y S un subconjunto de R. Entonces S es un subanillo de R si y solo si se cumplen las siguientes condiciones.*

1. $S \neq \emptyset$.
2. $rs \in S$ *para todo* $r, s \in S$.
3. $r - s \in S$ *para todo* $r, s \in S$.

Ejemplo 16.11. Sea $R = \mathbb{M}_2(\mathbb{R})$ el anillo de las matrices de 2×2 con coeficientes en $\mathbb{R}$. Si T es el conjunto de las matrices triangulares superiores en R; i.e.,

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\},$$

entonces T es un subanillo de R. Si

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$$

están en T, entonces claramente $A - B$ también está en T. Además,

$$AB = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix}$$

está en T.

16.2 Dominios Integrales y Cuerpos

Recordemos algunas definiciones. Si R es un anillo y r es un elemento distinto de cero en R, entonces r se llama ***divisor de cero*** si existe un elemento distinto de cero $s \in R$ tal que $rs = 0$. Un anillo conmutativo con identidad se llama ***dominio integral*** si no tiene divisores de cero. Si un elemento a en un anillo R con identidad tiene un inverso multiplicativo, decimos que a es una ***unidad***. Si todo elemento distinto de cero en un anillo R es una unidad, entonces R se llama ***anillo de división***. Un anillo de división conmutativo se llama ***cuerpo***.

Ejemplo 16.12. Si $i^2 = -1$, entonces el conjunto $\mathbb{Z}[i] = \{m + ni : m, n \in \mathbb{Z}\}$ forma un anillo conocido como los ***enteros Gaussianos***. Es fácil ver que los enteros Gaussianos forman un subanillo de los números complejos pues están cerrados bajo la suma y la multiplicación. Sea $\alpha = a + bi$ una unidad en $\mathbb{Z}[i]$. Entonces $\overline{\alpha} = a - bi$ también es una unidad pues si $\alpha\beta = 1$, entonces $\overline{\alpha}\overline{\beta} = 1$. Si $\beta = c + di$, entonces

$$1 = \alpha\beta\overline{\alpha}\overline{\beta} = (a^2 + b^2)(c^2 + d^2).$$

Por lo tanto, $a^2 + b^2$ debe ser 1 o -1; y, equivalentemente, $a + bi = \pm 1$ o $a + bi = \pm i$. Por lo tanto, las unidades de este anillo son ± 1 y $\pm i$; luego, los enteros Gaussianos no son un cuerpo. Dejaremos como ejercicio demostrar que los enteros Gaussianos son un dominio integral.

Ejemplo 16.13. El conjunto de las matrices

$$F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

con coeficiente en $\mathbb{Z}_2$ forma un cuerpo.

Ejemplo 16.14. El conjunto $\mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ es un cuerpo. El inverso de un elemento $a + b\sqrt{2}$ en $\mathbb{Q}(\sqrt{2}\,)$ es

$$\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}.$$

Tenemos la siguiente caracterización alternativa de los dominios integrales.

Proposición 16.15 (Ley de Cancelación)**.** *Sea D un anillo conmutativo con identidad. Entonces D es un dominio integral si y solo si para todos los elementos distintos de cero $a \in D$ con $ab = ac$, tenemos $b = c$.*

Demostración. Sea D un dominio integral. Entonces D no tiene divisores de cero. Sea $ab = ac$ con $a \neq 0$. Entonces $a(b - c) = 0$. Luego, $b - c = 0$ y $b = c$.

Recíprocamente, supongamos que la cancelación es posible en D. Es decir, supongamos que $ab = ac$ implica $b = c$. Sea $ab = 0$. Si $a \neq 0$, entonces $ab = a0$ o $b = 0$. Por lo tanto, a no puede ser un divisor de cero. □

El siguiente teorema sorprendente se lo debemos a Wedderburn.

Teorema 16.16. *Todo dominio integral finito es un cuerpo.*

Demostración. Sea D un dominio integral finito y sea D^* el onjunto de los elementos distintos de cero en D. Debemos mostrar que todo elemento en D^* tiene un inverso. Para cada $a \in D^*$ podemos definir una función $\lambda_a : D^* \to D^*$ como $\lambda_a(d) = ad$. Esta función tiene sentid, pues si $a \neq 0$ y $d \neq 0$, entonces $ad \neq 0$. La función λ_a es 1-1, pues para $d_1, d_2 \in D^*$,

$$ad_1 = \lambda_a(d_1) = \lambda_a(d_2) = ad_2$$

implica $d_1 = d_2$ por cancelación a la izquierda. Como D^* es un conjunto finito, la función λ_a también debe ser sobre; luego, para algún $d \in D^*$, $\lambda_a(d) = ad = 1$. Por lo tanto, a tiene inverso a la izquierda. Como D es conmutativo, d también es inverso a la derecha para a. Concluimos que D es un cuerpo. □

Para cualquier entero no negativo n y cualquier elemento r en un anillo R escribimos $r + \cdots + r$ (n times) como nr. Definimos la ***característica*** de un anillo R como el menor entero positivo n tal que $nr = 0$ para todo $r \in R$. Si no existe tal entero, entonces la característica de R se define como 0. Denotaremos la característica de R por $\operatorname{char} R$.

Ejemplo 16.17. Para todo primo p, $\mathbb{Z}_p$ es un cuerpo de característica p. Por la Proposición 3.4, todo elemento distinto de cero en $\mathbb{Z}_p$ tiene un inverso; luego, $\mathbb{Z}_p$ es un cuerpo. Si a es un elemento distinto de cero en el cuerpo, entonces $pa = 0$, pues el orden de cualquier elemento distinto de cero en el grupo abeliano $\mathbb{Z}_p$ es p.

Lema 16.18. *Sea R un anillo con identidad. Si 1 tiene orden n, entonces la característica de R es n.*

Demostración. Si 1 tiene orden n, entonces n es el menor entero positivo tal que $n1 = 0$. Además, para todo $r \in R$,

$$nr = n(1r) = (n1)r = 0r = 0.$$

Por otra parte, si ningún entero positivo n existe tal que $n1 = 0$, entonces la característica de R es cero. □

Teorema 16.19. *La característica de un dominio integral es un número primo o cero.*

Demostración. Sea D un dominio integral y supongamos que la característica de D es n con $n \neq 0$. Si n no es primo, entonces $n = ab$, con $1 < a < n$ y $1 < b < n$. Pr el Lema 16.18, solo necesitamos considerar el caso $n1 = 0$. Como $0 = n1 = (ab)1 = (a1)(b1)$ y no hay divisores de cero en D, ya sea $a1 = 0$ o $b1 = 0$. Luego, la característica de D debe ser menor a n, lo que es una contradicción. Por lo tanto, n debe ser primo. □

16.3 Homomorfismos de Anillos e Ideales

En el estudio de grupos, un homomorfismoes una función que preserva la operación del grupo. Similarmente, un homomorfismo entre anillos preserva las operaciones de adición y multiplicación en el anillo. Más específicamente, si R y S son anillos, entonces un ***homomorfismo de anillos*** es una función $\phi : R \to S$ que satisface

$$\phi(a + b) = \phi(a) + \phi(b)$$
$$\phi(ab) = \phi(a)\phi(b)$$

para todo $a, b \in R$. Si $\phi : R \to S$ es biyectiva, entonces ϕ se llama ***isomorfismo*** de anillos.

El conjunto de los elementos que un homomorfismo de anillo envía en 0 juega un papel fundamental en la teoría de anillos. Para cualquier homomorfismo $\phi : R \to S$, definimos el ***núcleo*** de un homomorfismo de anillos como el conjunto

$$\ker \phi = \{r \in R : \phi(r) = 0\}.$$

Ejemplo 16.20. Para cualquier entero n podemos definir un homomorfismode anillos $\phi : \mathbb{Z} \to \mathbb{Z}_n$ como $a \mapsto a \pmod n$. En efecto es un homomorfismo de anillos, pues

$$\phi(a + b) = (a + b) \pmod n$$

$$\begin{aligned} &= a \pmod n + b \pmod n \\ &= \phi(a) + \phi(b) \end{aligned}$$

y

$$\begin{aligned} \phi(ab) &= ab \pmod n \\ &= a \pmod n \cdot b \pmod n \\ &= \phi(a)\phi(b). \end{aligned}$$

El núcleo del homomorfismo ϕ es $n\mathbb{Z}$.

Ejemplo 16.21. Sea $C[a,b]$ el anillo de funciones reales continuas definidas en un intervalo $[a,b]$ como en el Ejemplo 16.5. Para un $\alpha \in [a,b]$ fijo, podemos definir un homomorfismo de anillos $\phi_\alpha : C[a,b] \to \mathbb{R}$ como $\phi_\alpha(f) = f(\alpha)$. Este es un homomorfismode anillos pues

$$\phi_\alpha(f+g) = (f+g)(\alpha) = f(\alpha) + g(\alpha) = \phi_\alpha(f) + \phi_\alpha(g)$$
$$\phi_\alpha(fg) = (fg)(\alpha) = f(\alpha)g(\alpha) = \phi_\alpha(f)\phi_\alpha(g).$$

Homomorfismos de anillos del tipo ϕ_α se llaman ***isomorfismos de evaluación***.

En la siguiente proposición examinaremos algunas propiedades fundamentales de los homomorfismos de anillos. La demostración de la proposición la dejamos como ejercicio.

Proposición 16.22. *Sea $\phi : R \to S$ un homomorfismo de anillos.*

1. *Si R es un anillos conmutativo, entonces $\phi(R)$ es un anillo conmutativo.*
2. *$\phi(0) = 0$.*
3. *Sean 1_R y 1_S las identidades de R y S, respectivamente. Si ϕ es sobre, entonces $\phi(1_R) = 1_S$.*
4. *Si R es un cuerpo y $\phi(R) \neq \{0\}$, entonces $\phi(R)$ es un cuerpo.*

En teoría de grupos vimos que los subgrupos normales tienen un rol especial. Estos subgrupos tienen buenas características que los hacen más interesantes de estudiar que los subgrupos arbitrarios. En teoría de anillos los objetos que corresponden a los subgrupos normales son una clase especial de subanillos llamados ideales. Un ***ideal*** en un anillo R es un subanillo I de R tal que si a está en I y r está en R, entonces tanto ar como ra están en I; es decir, $rI \subset I$ y $Ir \subset I$ para todo $r \in R$.

Ejemplo 16.23. Todo anillo R tiene al menos dos ideales, $\{0\}$ y R. Estos ideales se llaman ***ideales triviales***.

Sea R un anillo con identidad y supongamos que I es un ideal en R tal que 1 está en I. Como para cualquier $r \in R$, $r1 = r \in I$ por la definición de ideal, $I = R$.

Ejemplo 16.24. Si a es cualquier elemento en un anillo conmutativo R con identidad, entonces el conjunto

$$\langle a \rangle = \{ar : r \in R\}$$

es un ideal en R. De hecho, $\langle a \rangle$ es no vacío pues tanto $0 = a0$ como $a = a1$ están en $\langle a \rangle$. La suma de dos elementos en $\langle a \rangle$ está nuevamoente en $\langle a \rangle$ pues $ar + ar' = a(r+r')$. El inverso aditivo de ar es $-ar = a(-r) \in \langle a \rangle$. Finalmente, si multiplicamos un elemento $ar \in \langle a \rangle$ por un elemento arbitrario $s \in R$, tenemos $s(ar) = a(sr)$. Por lo tanto, $\langle a \rangle$ satisface la definición de un ideal.

Si R s un anillo conmutativo con identidad, entonces un ideal de la forma $\langle a\rangle = \{ar : r \in R\}$ se llama ***ideal principal***.

Teorema 16.25. *Todo ideal en el anillo de los enteros $\mathbb{Z}$ es un ideal principal.*

DEMOSTRACIÓN. El ideal cero $\{0\}$ es un ideal principal pues $\langle 0\rangle = \{0\}$. Si I es un ideal distinto de cero en $\mathbb{Z}$, entonces I debe contener algún entero positivo m. Existe entonces un menor entero positivo n en I por el Principio del Buen Orden. Sea ahora a un elemento en I. Usando el algoritmo de división, sabemos que existee enteros q y r tales que

$$a = nq + r$$

donde $0 \leq r < n$. Esta ecuación nos dice que $r = a - nq \in I$, pero r debe ser 0 pues n es el menor entero positivo en I. Por lo tanto, $a = nq$ e $I = \langle n\rangle$. □

Ejemplo 16.26. El conjunto $n\mathbb{Z}$ es un ideal en el anillo de los enteros. Si na está en $n\mathbb{Z}$ y b está en $\mathbb{Z}$, entonces nab está en $n\mathbb{Z}$ como se pedía. De hecho, por el Teorema 16.25, estos son los únicos ideales de $\mathbb{Z}$.

Proposición 16.27. *El núcleo de cualquier homomorfismo de anillos $\phi : R \to S$ es un ideal en R.*

DEMOSTRACIÓN. Sabemos de teoría de grupos que $\ker\phi$ es un subgrupo aditivo de R. Supongamos que $r \in R$ y $a \in \ker\phi$. Entonces debemos demostrar que ar y ra están en $\ker\phi$. Pero,

$$\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$$

y

$$\phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0.$$ □

Nota 16.28. En nuestra definición de ideal hemos pedido que $rI \subset I$ y $Ir \subset I$ para todo $r \in R$. Tales ideales a veces son denominados ***ideales biláteros***. Podemos también considerar ***ideales por un lado***; es decir, debemos pedir que se cumpla $rI \subset I$ o $Ir \subset I$ para todo $r \in R$ pero no ambos. Tales ideales se llaman ***ideales izquierdos*** e ***ideales derechos***, respectivamente. Por supuesto que en un anillos conmutativo todo ideal es bilátero. En este texto nos concentraremos en los ideales biláteros.

Teorema 16.29. *Sea I un ideal de R. El grupo cociente R/I es un anillo con la multiplicación definida como*

$$(r + I)(s + I) = rs + I.$$

DEMOSTRACIÓN. Ya sabemos que R/I es un grupo abeliano con la adición. Sean $r + I$ y $s + I$ en R/I. Debemos mostrar que el producto $(r + I)(s + I) = rs + I$ es independiente de la elección de representantes de las clases laterales; es decir, si $r' \in r + I$ y $s' \in s + I$, entonces $r's'$ debe estar en $rs + I$. Como $r' \in r + I$, debe existir un elemento a en I tal que $r' = r + a$. Similarmente, existe $b \in I$ tal que $s' = s + b$. Note que

$$r's' = (r + a)(s + b) = rs + as + rb + ab$$

y $as + rb + ab \in I$ pues I es un ideal; por lo tanto, $r's' \in rs + I$. Dejaremos como ejercicio la verificación de la asociatividad del producto y de las reglas de distributividad. □

El anillo R/I en el Teorema 16.29 se llama ***anillo cociente***. Así como con los homomorfismos de grupos y los subgrupos normales, hay una relación entre los homomorfismos de anillos y los ideales.

Teorema 16.30. *Sea I un ideal de R. La función $\phi : R \to R/I$ definida po $\phi(r) = r + I$ es un homomorfismo de anillos de R sobre R/I con núcleo I.*

Demostración. En efecto, $\phi : R \to R/I$ es un homomorfismo epiyectivo de grupo abelianos. Falta demostrar que ϕ funciona correctamente con la multiplicación en el anillo. Sean r y s en R. Entonces

$$\phi(r)\phi(s) = (r + I)(s + I) = rs + I = \phi(rs),$$

lo que completa la demostración del teorema. □

La función $\phi : R \to R/I$ se llama ***homomorfismo natural*** o ***canónico***. En teoría de anillo tenemos teoremas de isomorfía relacionando los ideales y los homomorfismos de anillos similares a los teoremas de isomorfía de grupos que relacionan subgrupos normales y homomorfismos en el Capítulo 11. Demostraremos solo el Primer Teorema de Isomorfía para anillos en este capítulo y dejaremos las demostraciones de los otros dos como ejericios. Todas las demostraciones son similares a las demostraciones de los teoremas de isomorfía para grupos.

Teorema 16.31 (Primer Teorema de Isomorfía)**.** *Sea $\psi : R \to S$ un homomorfismode anillos. Entonces* $\ker \psi$ *es un ideal de R. Si $\phi : R \to R/\ker \psi$ es el homomorfismo canónico, entonces existe un único isomorfismo $\eta : R/\ker \psi \to \psi(R)$ tal que $\psi = \eta\phi$.*

Demostración. Sea $K = \ker \psi$. Por el Primer Teorema de Isomorfía para grupos, existe un homomorfismo de grupos bien definido $\eta : R/K \to \psi(R)$ definido por $\eta(r + K) = \psi(r)$ para los grupos abelianos aditivos R y R/K. Para mostrar que este es un homomorfismo de anillos, solo debemos mostrar que $\eta((r + K)(s + K)) = \eta(r + K)\eta(s + K)$; pero

$$\begin{aligned}\eta((r + K)(s + K)) &= \eta(rs + K)\\ &= \psi(rs)\\ &= \psi(r)\psi(s)\\ &= \eta(r + K)\eta(s + K).\end{aligned}$$

□

Teorema 16.32 (Segundo Teorema de Isomorfía)**.** *Sea I un subanillo de un anillo R y J un ideal de R. Entonces $I \cap J$ es un ideal de I y*

$$I/I \cap J \cong (I + J)/J.$$

Teorema 16.33 (Tercer Teorema de Isomorfía)**.** *Sea R un anillo y sean I y J ideales de R con $J \subset I$. Entonces*

$$R/I \cong \frac{R/J}{I/J}.$$

Teorema 16.34 (Teorema de Correspondencia)**.** *Sea I un idela de un anillo R. Entonces $S \mapsto S/I$ es una correspondencia biunívoca entre el conjunto de subanillos de S que contienen a I y el conjunto de subanillos de R/I. Más aún, los ideales de R que contienen a I corresponden a ideales de R/I.*

16.4 Ideales Maximales e Ideales Primos

En esta sección particular estamos especialmente interesados en ciertos ideales de anillos conmutativos. Estos ideales nos entregan anillos cociente especiales. Más específicamente, queremos caracterizar aquellos ideales I de un anillo conmutativo R tales que R/I es un dominio integral o un cuerpo.

Un ideal propio M de un anillo R es un ***ideal maximal*** de R se el ideal M no es subconjunto propio de ningún ideal de R excepto R msimo. Es decir, M es un ideal maximal si para cualquier ideal I que contenga propiamente a M, $I = R$. El siguiente teorema completamente caracteriza los ideales maximales para anillos conmutativos con identidad en términos de los anillos cociente respectivos.

Teorema 16.35. *Sea R un anillo conmutativo con identidad y sea M un ideal en R. Entonces M es un idela maximal de R si y solo si R/M es un cuerpo.*

Demostración. Sea M un ideal maximal en R. Como R es un anillo conmutativo, R/M también es un anillo conmutativo. Claramente, $1+M$ actúa como identidad para R/M. Debemos mostrar también que cada elemento distinto de cero en R/M tiene un inverso. Si $a+M$ es un elemento distinto de cero en R/M, entonces $a \notin M$. Definamos I como el conjunto $\{ra+m : r \in R \text{ and } m \in M\}$. Mostraremos que I es un ideal en R. El conjunto I es no vacío pues $0a+0 = 0$ está en I. Si $r_1a + m_1$ y $r_2a + m_2$ son dos eleemntos en I, entonces

$$(r_1a + m_1) - (r_2a + m_2) = (r_1 - r_2)a + (m_1 - m_2)$$

está en I. Además, para cualquier $r \in R$ se cumple que $rI \subset I$; luego, I es cerrado bajo multiplicación por elementos del anillo y cumple las condiciones necesarias para ser un ideal. Por lo tanto, por la Proposición 16.10 y la definición de ideal, I es un ideal que contiene propiamente a M. Como M es un ideal maximal, $I = R$; concluimos que, por la definición de I deben existir m en M y b en R tales que $1 = ab + m$. Por lo tanto,

$$1 + M = ab + M = ba + M = (a + M)(b + M).$$

Recíprocamente, supongamos que M es un ideal y que R/M es un cuerpo. Como R/M es un cuerpo, debe contener al menos dos elementos: $0 + M = M$ y $1+M$. Luego, M es un ideal propio de R. Sea I cualquier ideal que contenga propiamente a M. Debemos mostrar que $I = R$. Sea a en I pero no en M. Como $a + M$ es un elemento distinto de cero en un cuerpo, existe $b + M$ en R/M tal que $(a + M)(b + M) = ab + M = 1 + M$. Concluimos que existe un elemento $m \in M$ tal que $ab + m = 1$ y 1 está en I. Por lo tanto, $r1 = r \in I$ para todo $r \in R$. Concluimos que $I = R$. □

Ejemplo 16.36. Sea $p\mathbb{Z}$ un ideal en $\mathbb{Z}$, con p un número primo. Entonces $p\mathbb{Z}$ es un ideal maximal pues $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ es un cuerpo.

Un ideal propio P en un anillo conmutativo R se llama ***ideal primo*** si cada vez que $ab \in P$, tenemos que $a \in P$ o $b \in P$.[1]

Ejemplo 16.37. Es fácil verificar que el conjunto $P = \{0, 2, 4, 6, 8, 10\}$ es un ideal en $\mathbb{Z}_{12}$. Este ideal es primo. De hecho es un ideal maximal.

Proposición 16.38. *Sea R un anillo conmutativo con identidad 1, donde $1 \neq 0$. Entonces P es un ideal primo en R si y solo si R/P es un dominio integral.*

[1] Es posible definir ideales primos en anillos no conmutativos. Vea [1] o [3].

DEMOSTRACIÓN. Primero supongamos que P es un ideal en R y que R/P es un dominio integral. Supongamos que $ab \in P$. Si $a + P$ y $b + P$ son dos elementos de R/P tales que $(a + P)(b + P) = 0 + P = P$, entonces $a + P = P$ o $b + P = P$. Esto quiere decir que a está en P o b está en P, lo que muestra que P debe ser primo.

Recíprocamente, supongamos que P es primo y

$$(a + P)(b + P) = ab + P = 0 + P = P.$$

Entonces $ab \in P$. Si $a \notin P$, entonces b debe estar en P por la definición de ideal primo; luego, $b + P = 0 + P$ y R/P es un dominio integral. □

Ejemplo 16.39. Todo ideal en $\mathbb{Z}$ es de la forma $n\mathbb{Z}$. El anillo cociente $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ es un dominio integral si y solo si n es primo. Es en realidad un cuerpo en tal caso. Luego, los ideales primos distintos de cero en $\mathbb{Z}$ son los ideal $p\mathbb{Z}$, donde p es primo. Este ejemplo realmente justifica el uso de la palabra "primo" en nuestra definición de ideales primos.

Como todo cuerpo es un dominio integral, tenemos el siguiente corolario.

Corolario 16.40. *Todo ideal maximal en un anillo conmutativo con identidad es también un ideal primo.*

Nota Histórica

Amalie Emmy Noether, uno de los matemáticos destacados del siglo XX, nación en Erlangen, Alemania en 1882. Era la hija de Max Noether (1844–1921), un distinguido matemático en la Universidad de Erlangen. Junto a Paul Gordon (1837–1912), el padre de Emmy Noether influyó fuertemente en su educación temprana. Entró a la Universidad de Erlangen a los 18 años de edad. Si bien mujeres ya habían sido admitidas a las universidades en Inglaterra, Francia e Italia por décadas, había gran resistencia a su presencia en la universidades alemanas. Noether era una de las dos únicas mujeres entre los 986 estudiantes de la universidad. Después de obtener su doctorado bajo la dirección de Gordon en 1907, continuó haciendo investigación en Erlangen, dictando cátedras ocasionales cuando su padre estaba enfermo.

Noether fue a estudiar a Göttingen en 1916. David Hilbert y Felix Klein intentaro sin éxito conseguirle un puesto en Göttingen. Algunos de los profesores objetaban la presencia de catedráticas profesoras, diciendo, "¿qué pensarán nuestros soldados cuando vuelvan a la universidad y tengan que aprender bajo una mujer?" Hilbert, exasperado po la pregunta, respondió, "Meine Herren, no veo que el sexo de un candidato sea un argumento contra su contratación como Privatdozent. Después de todo, el senado no es una casa de baños." Al final de la Primera Guerra Mundial, las actitudes cambiaron y las condiciones para las mujeres mejoraron significativamente. Después que pasó su examen de habilitación en 1919, le fue otorgado un título y le comenzaron a pagar una pequeña cantidad por sus clases.

En 1922, Noether fue contratada como Privatdozent en Göttingen. Durante los siguientes 11 años usó métodos axiomáticos para desarrollar una teoría abstracta de anillos e ideales. Si bien no era buena dando cátedra, Noether era una profesora inspiradora. Uno de sus muchos alumnos fue B. L. van der Waerden, autor del primer texto que trató de álgebra abstracta desde un punto de vista moderno. Algunos de los otros matemáticos influenciados por Noether o que trabajaron con ella fueron Alexandroff, Artin, Brauer, Courant, Hasse, Hopf, Pontryagin, von Neumann, y Weyl. Uno de los momentos cúlmines de su carrera fue una invitación a dar una conferencia en el Congrso Internacional

de Matemáticos en Zurich en 1932. A pesar de todo el reconocimiento que recibió de sus colegas, las habilidades de Noether nunca fueron debidamente reconocidas durante su vida. Nunca fue promovida a profesora titular por la burocracia académica Prusiana.

En 1933, a Noether, que era judía, le fue prohibida la participación de todas las actividades académicas en Alemania. Emigró a los Esstados Unidos, tomó una posición en el Bryn Mawr College, y se hizo miembro del Institute for Advanced Study en Princeton. Noether murió repentinamente el 14 de Abril de 1935. Después de su muerte fue eulogiada científicos tan notables como Albert Einstein.

16.5 Una Aplicación al Diseño de Software

El Teorema Chino de los Restos es un resultado de teoría elemental de números sobre las soluciones simultáneas de sistemas de congruencias. El matemático chino Sun-tsï escribió sobre este teorema en el sigo primero D.C. Este teorema tiene interesantes consecuencias en el diseño de software para el uso de procesadores en paralelo.

Lema 16.41. *Sean m y n enteros positivos tales que* $\text{mcd}(m,n) = 1$. *Entonces para $a, b \in \mathbb{Z}$ el sistema*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

tiene solución. Si x_1 y x_2 son dos soluciones del sistema, entonces $x_1 \equiv x_2 \pmod{mn}$.

Demostración. La ecuación $x \equiv a \pmod{m}$ tiene solución pues $a + km$ satisface la ecuación para todo $k \in \mathbb{Z}$. Debemos mostrar que existe un entero k_1 tal que

$$a + k_1 m \equiv b \pmod{n}.$$

Esto es equivalente a mostrar que

$$k_1 m \equiv (b - a) \pmod{n}$$

tiene solución para k_1. Como m y n son relativamente primos, existen enteros s y t tales que $ms + nt = 1$. Concluimos que,

$$(b-a)ms = (b-a) - (b-a)nt,$$

o

$$[(b-a)s]m \equiv (b-a) \pmod{n}.$$

Ahora sea $k_1 = (b-a)s$.

Para mostrar que dos soluciones cualquiera son congruentes módulo mn, sean c_1 y c_2 dos soluciones del sistema. Es decir,

$$\begin{aligned} c_i &\equiv a \pmod{m} \\ c_i &\equiv b \pmod{n} \end{aligned}$$

para $i = 1, 2$. Entonces

$$\begin{aligned} c_2 &\equiv c_1 \pmod{m} \\ c_2 &\equiv c_1 \pmod{n}. \end{aligned}$$

por lo tanto, tanto m como n dividen a $c_1 - c_2$. Concluimos que $c_2 \equiv c_1 \pmod{mn}$. □

Ejemplo 16.42. Resolvamos el sistema

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5. \end{aligned}$$

Usando el algoritmo de Euclides, podemos encontrar enteros s y t tales que $4s + 5t = 1$. Una posibilidad para tales enteros es $s = 4$ y $t = -3$. Concluimos que

$$x = a + k_1 m = 3 + 4k_1 = 3 + 4[(5 - 4)4] = 19.$$

Teorema 16.43 (Teorema Chino de los Restos)**.** *Sean $n_1, n_2, \ldots, n_k$ enteros positivos tales que $\text{mcd}(n_i, n_j) = 1$ para $i \neq j$. Entonces para enteros cualesquiera $a_1, \ldots, a_k$, el sistema*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

tiene solución. Más aún, dos soluciones cualquiera del sistema son congruentes módulo $n_1 n_2 \cdots n_k$.

Demostración. Procederemos por inducción en el número de ecuaciones en el sistema. Si hay $k = 2$ ecuaciones, entonces el teorema es cierto por el Lema 16.41. Ahora supongamos que el resultado es verdadero para un sistema de k o menos ecuaciones y que deseamos encontrar una solución de

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_{k+1} \pmod{n_{k+1}}. \end{aligned}$$

Considerando las primeras k ecuaciones, existe una solución que es única módulo $n_1 \cdots n_k$, digamos a. Como $n_1 \cdots n_k$ y n_{k+1} son relativamente primos, el sistema

$$\begin{aligned} x &\equiv a \pmod{n_1 \cdots n_k} \\ x &\equiv a_{k+1} \pmod{n_{k+1}} \end{aligned}$$

tiene una solución que es única módulo $n_1 \ldots n_{k+1}$ por el lema. □

Ejemplo 16.44. Resolvamos el sistema

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 1 \pmod 9 \\ x &\equiv 5 \pmod 7. \end{aligned}$$

Del Ejemplo 16.42 sabemos que 19 es una solución de las primeras dos congruencias y cualquier otra solución del sistema es congruente a 19 (mod 20). Luego, podemos reducir el sistema a un sistema de tres congruencias:

$$x \equiv 19 \pmod{20}$$

$$x \equiv 1 \pmod 9$$
$$x \equiv 5 \pmod 7.$$

Resolviendo las siguientes dos ecuaciones, podemos reducir el sistema a

$$x \equiv 19 \pmod{180}$$
$$x \equiv 5 \pmod 7.$$

Resolviendo este últimom sistema, encontramos que 19 es una solución para el sistema que es única módulo 1260.

Una aplicación interesante del Teorema Chino de los Restos en el diseño de software computacional es que el teorema nos permite descomponer un cálculo que involucre enteros grandes en varios cálculos menos grandes. Un computador puede trabajar con enteros solamente hasta cierto tamaaños debido al tamaño de su procesador, que usualmente es un procesador de 32 o 64-bit. Por ejemplo, el mayor entero disponible en un computador con un procesador de 64-bit es

$$2^{63} - 1 = 9{,}223{,}372{,}036{,}854{,}775{,}807.$$

Procesadores mayores como 128 o 256-bit han sido propuesto o están en desarrollo. Incluso se habla de un procesador de 512-bit. El mayor entero que un tal procesador ppodría almacenar sería $2^{511} - 1$, que es un número de 154 dígitos. Sin embargo, necesitaríamos trabajar con números mucho más grandes para romper sofisticados métodos de encriptación.

Se requiere Software especial para cálculos con enteros mayores que no pueden ser sumados directamente por la máquina. Usando el Teorema Chino de los Restos podemos descomponer sumas y multiplicaciones de enteros grandes en cálculos que el computador pueda hacer de forma directa. Esto es especialmente útil para el procesamiento paralelo.

La mayor parte de los computadores tiene una única unidad central de proceso (CPU) que contiene un chip procesador que puede sumar solo dos números a la vez. Para sumar una lista de diez números, la CPU debe hacer nueve sumas sucesivamente. Sin embargo un computador de procesamiento paralelo tiene más de una CPU. Un computador con 10 CPUs, por ejemplo, puede hacer 10 operaciones diferentes al mismo tiempo. Si podemos tomar un entero grande y descomponerlo en sus partes, enviando cada una de las partes a una CPU diferente, entonces haciendo sumas y multiplicaciones en paralelo, podemos trabajar con enteros con los que el computador no podría trabajar directamente.

Ejemplo 16.45. Supongamos que deseamos multiplicar 2134 por 1531. Usaremos los enteros 95, 97, 98, y 99 pues estos son relativamente primos. Descompponemos cada uno de los enteros en cuatro partes:

$$2134 \equiv 44 \pmod{95}$$
$$2134 \equiv 0 \pmod{97}$$
$$2134 \equiv 76 \pmod{98}$$
$$2134 \equiv 55 \pmod{99}$$

y

$$1531 \equiv 11 \pmod{95}$$
$$1531 \equiv 76 \pmod{97}$$
$$1531 \equiv 61 \pmod{98}$$

$$1531 \equiv 46 \pmod{99}.$$

Multiplicando las ecuaciones correspondientes, obtenemos

$$\begin{aligned} 2134 \cdot 1531 &\equiv 44 \cdot 11 \equiv 9 \pmod{95} \\ 2134 \cdot 1531 &\equiv 0 \cdot 76 \equiv 0 \pmod{97} \\ 2134 \cdot 1531 &\equiv 76 \cdot 61 \equiv 30 \pmod{98} \\ 2134 \cdot 1531 &\equiv 55 \cdot 46 \equiv 55 \pmod{99}. \end{aligned}$$

Cada uno de estos cálculos puede ser enviado a un procesador diferente si nuestro computador tiene varias CPU. Por el cálculo anterior, sabemos que $2134 \cdot 1531$ es una solución de este sistema

$$\begin{aligned} x &\equiv 9 \pmod{95} \\ x &\equiv 0 \pmod{97} \\ x &\equiv 30 \pmod{98} \\ x &\equiv 55 \pmod{99}. \end{aligned}$$

El Teorema Chino de los Restos que la solución es única módulo $95 \cdot 97 \cdot 98 \cdot 99 = 89{,}403{,}930$. Resolviendo el sistema para x nos dice que $2134 \cdot 1531 = 3{,}267{,}154$.

La conversión del cálculo en sus cuatro componentes tomará cierto tiempo de cálculo. Además, resolver el sistema de congruencias puede tomar un tiempo considerable. A pesar de ello, si tenemos muchos cálculos que realizar en un conjunto particular de números, tiene sentido transformar el problema como hicimos arriba y hacer los cálculos necesarios de forma simultánea.

Sage Rings are at the heart of Sage's design, so you will find a wide range of possibilities for computing with rings and fields. Ideals, quotients, and homomorphisms are all available.

16.6 Exercises

1. Which of the following sets are rings with respect to the usual operations of addition and multiplication? If the set is a ring, is it also a field?

(a) $7\mathbb{Z}$

(b) $\mathbb{Z}_{18}$

(c) $\mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

(d) $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$

(e) $\mathbb{Z}[\sqrt{3}\,] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$

(f) $R = \{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\}$

(g) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\}$

(h) $\mathbb{Q}(\sqrt[3]{3}\,) = \{a + b\sqrt[3]{3} + c\sqrt[3]{9} : a, b, c \in \mathbb{Q}\}$

2. Let R be the ring of 2×2 matrices of the form

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

where $a, b \in \mathbb{R}$. Show that although R is a ring that has no identity, we can find a subring S of R with an identity.

3. List or characterize all of the units in each of the following rings.

(a) $\mathbb{Z}_{10}$

(b) $\mathbb{Z}_{12}$

(c) $\mathbb{Z}_7$

(d) $\mathbb{M}_2(\mathbb{Z})$, the 2×2 matrices with entries in $\mathbb{Z}$

(e) $\mathbb{M}_2(\mathbb{Z}_2)$, the 2×2 matrices with entries in $\mathbb{Z}_2$

4. Find all of the ideals in each of the following rings. Which of these ideals are maximal and which are prime?

(a) $\mathbb{Z}_{18}$

(b) $\mathbb{Z}_{25}$

(c) $\mathbb{M}_2(\mathbb{R})$, the 2×2 matrices with entries in $\mathbb{R}$

(d) $\mathbb{M}_2(\mathbb{Z})$, the 2×2 matrices with entries in $\mathbb{Z}$

(e) $\mathbb{Q}$

5. For each of the following rings R with ideal I, give an addition table and a multiplication table for R/I.

(a) $R = \mathbb{Z}$ and $I = 6\mathbb{Z}$

(b) $R = \mathbb{Z}_{12}$ and $I = \{0, 3, 6, 9\}$

6. Find all homomorphisms $\phi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$.

7. Prove that $\mathbb{R}$ is not isomorphic to $\mathbb{C}$.

8. Prove or disprove: The ring $\mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is isomorphic to the ring $\mathbb{Q}(\sqrt{3}\,) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$.

9. What is the characteristic of the field formed by the set of matrices

$$F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

with entries in $\mathbb{Z}_2$?

10. Define a map $\phi : \mathbb{C} \to \mathbb{M}_2(\mathbb{R})$ by

$$\phi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Show that ϕ is an isomorphism of $\mathbb{C}$ with its image in $\mathbb{M}_2(\mathbb{R})$.

11. Prove that the Gaussian integers, $\mathbb{Z}[i]$, are an integral domain.

12. Prove that $\mathbb{Z}[\sqrt{3}\,i] = \{a + b\sqrt{3}\,i : a, b \in \mathbb{Z}\}$ is an integral domain.

13. Solve each of the following systems of congruences.

(a)
$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 6 \pmod{11} \end{aligned}$$

(b)
$$x \equiv 3 \pmod 7$$

(c)
$$\begin{aligned} x &\equiv 0 \pmod 8 \\ x &\equiv 5 \pmod{15} \end{aligned}$$

(d)
$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

(d)

$$\begin{aligned} x &\equiv 7 \pmod 9 \\ x &\equiv 5 \pmod{11} \\ x &\equiv 3 \pmod 5 \end{aligned} \qquad \begin{aligned} x &\equiv 0 \pmod 8 \\ x &\equiv 1 \pmod{11} \\ x &\equiv 5 \pmod{13} \end{aligned}$$

14. Use the method of parallel computation outlined in the text to calculate $2234 + 4121$ by dividing the calculation into four separate additions modulo 95, 97, 98, and 99.

15. Explain why the method of parallel computation outlined in the text fails for $2134 \cdot 1531$ if we attempt to break the calculation down into two smaller calculations modulo 98 and 99.

16. If R is a field, show that the only two ideals of R are $\{0\}$ and R itself.

17. Let a be any element in a ring R with identity. Show that $(-1)a = -a$.

18. Let $\phi : R \to S$ be a ring homomorphism. Prove each of the following statements.

(a) If R is a commutative ring, then $\phi(R)$ is a commutative ring.

(b) $\phi(0) = 0$.

(c) Let 1_R and 1_S be the identities for R and S, respectively. If ϕ is onto, then $\phi(1_R) = 1_S$.

(d) If R is a field and $\phi(R) \neq 0$, then $\phi(R)$ is a field.

19. Prove that the associative law for multiplication and the distributive laws hold in R/I.

20. Prove the Second Isomorphism Theorem for rings: Let I be a subring of a ring R and J an ideal in R. Then $I \cap J$ is an ideal in I and

$$I/I \cap J \cong I + J/J.$$

21. Prove the Third Isomorphism Theorem for rings: Let R be a ring and I and J be ideals of R, where $J \subset I$. Then

$$R/I \cong \frac{R/J}{I/J}.$$

22. Prove the Correspondence Theorem: Let I be an ideal of a ring R. Then $S \to S/I$ is a one-to-one correspondence between the set of subrings S containing I and the set of subrings of R/I. Furthermore, the ideals of R correspond to ideals of R/I.

23. Let R be a ring and S a subset of R. Show that S is a subring of R if and only if each of the following conditions is satisfied.

(a) $S \neq \emptyset$.

(b) $rs \in S$ for all $r, s \in S$.

(c) $r - s \in S$ for all $r, s \in S$.

24. Let R be a ring with a collection of subrings $\{R_\alpha\}$. Prove that $\bigcap R_\alpha$ is a subring of R. Give an example to show that the union of two subrings is not necessarily a subring.

25. Let $\{I_\alpha\}_{\alpha \in A}$ be a collection of ideals in a ring R. Prove that $\bigcap_{\alpha \in A} I_\alpha$ is also an ideal in R. Give an example to show that if I_1 and I_2 are ideals in R, then $I_1 \cup I_2$ may not be an ideal.

26. Let R be an integral domain. Show that if the only ideals in R are $\{0\}$ and R itself, R must be a field.

27. Let R be a commutative ring. An element a in R is ***nilpotent*** if $a^n = 0$ for some positive integer n. Show that the set of all nilpotent elements forms an ideal in R.

28. A ring R is a ***Boolean ring*** if for every $a \in R$, $a^2 = a$. Show that every Boolean ring is a commutative ring.

29. Let R be a ring, where $a^3 = a$ for all $a \in R$. Prove that R must be a commutative ring.

30. Let R be a ring with identity 1_R and S a subring of R with identity 1_S. Prove or disprove that $1_R = 1_S$.

31. If we do not require the identity of a ring to be distinct from 0, we will not have a very interesting mathematical structure. Let R be a ring such that $1 = 0$. Prove that $R = \{0\}$.

32. Let S be a nonempty subset of a ring R. Prove that there is a subring R' of R that contains S.

33. Let R be a ring. Define the ***center*** of R to be

$$Z(R) = \{a \in R : ar = ra \text{ for all } r \in R\}.$$

Prove that $Z(R)$ is a commutative subring of R.

34. Let p be prime. Prove that

$$\mathbb{Z}_{(p)} = \{a/b : a, b \in \mathbb{Z} \text{ and } \operatorname{mcd}(b, p) = 1\}$$

is a ring. The ring $\mathbb{Z}_{(p)}$ is called the ***ring of integers localized at*** p.

35. Prove or disprove: Every finite integral domain is isomorphic to $\mathbb{Z}_p$.

36. Let R be a ring with identity.

(a) Let u be a unit in R. Define a map $i_u : R \to R$ by $r \mapsto uru^{-1}$. Prove that i_u is an automorphism of R. Such an automorphism of R is called an inner automorphism of R. Denote the set of all inner automorphisms of R by $\operatorname{Inn}(R)$.

(b) Denote the set of all automorphisms of R by $\operatorname{Aut}(R)$. Prove that $\operatorname{Inn}(R)$ is a normal subgroup of $\operatorname{Aut}(R)$.

(c) Let $U(R)$ be the group of units in R. Prove that the map

$$\phi : U(R) \to \operatorname{Inn}(R)$$

defined by $u \mapsto i_u$ is a homomorphism. Determine the kernel of ϕ.

(d) Compute $\operatorname{Aut}(\mathbb{Z})$, $\operatorname{Inn}(\mathbb{Z})$, and $U(\mathbb{Z})$.

37. Let R and S be arbitrary rings. Show that their Cartesian product is a ring if we define addition and multiplication in $R \times S$ by

(a) $(r, s) + (r', s') = (r + r', s + s')$

(b) $(r, s)(r', s') = (rr', ss')$

38. An element x in a ring is called an ***idempotent*** if $x^2 = x$. Prove that the only idempotents in an integral domain are 0 and 1. Find a ring with a idempotent x not equal to 0 or 1.

39. Let $\text{mcd}(a, n) = d$ and $\text{mcd}(b, d) \neq 1$. Prove that $ax \equiv b \pmod{n}$ does not have a solution.

40. (The Chinese Remainder Theorem for Rings) Let R be a ring and I and J be ideals in R such that $I + J = R$.

(a) Show that for any r and s in R, the system of equations

$$\begin{aligned} x &\equiv r \pmod{I} \\ x &\equiv s \pmod{J} \end{aligned}$$

has a solution.

(b) In addition, prove that any two solutions of the system are congruent modulo $I \cap J$.

(c) Let I and J be ideals in a ring R such that $I + J = R$. Show that there exists a ring isomorphism

$$R/(I \cap J) \cong R/I \times R/J.$$

16.7 Ejercicio de programación

1. Escriba un programa de computadora implementando la suma y el producto usando el Teorema Chino de los Restos y el método delineado en el texto.

16.8 Referencias y Lecturas Recomendadas

[1] Anderson, F. W. and Fuller, K. R. *Rings and Categories of Modules*. 2nd ed. Springer, New York, 1992.

[2] Atiyah, M. F. and MacDonald, I. G. *Introduction to Commutative Algebra*. Westview Press, Boulder, CO, 1994.

[3] Herstein, I. N. *Noncommutative Rings*. Mathematical Association of America, Washington, DC, 1994.

[4] Kaplansky, I. *Commutative Rings*. Revised edition. University of Chicago Press, Chicago, 1974.

[5] Knuth, D. E. *The Art of Computer Programming: Semi-Numerical Algorithms*, vol. 2. 3rd ed. Addison-Wesley Professional, Boston, 1997.

[6] Lidl, R. and Pilz, G. *Applied Abstract Algebra*. 2nd ed. Springer, New York, 1998. A good source for applications.

[7] Mackiw, G. *Applications of Abstract Algebra*. Wiley, New York, 1985.

[8] McCoy, N. H. *Rings and Ideals*. Carus Monograph Series, No. 8. Mathematical Association of America, Washington, DC, 1968.

[9] McCoy, N. H. *The Theory of Rings*. Chelsea, New York, 1972.

[10] Zariski, O. and Samuel, P. *Commutative Algebra*, vols. I and II. Springer, New York, 1975, 1960.

16.9 Sage

Los anillos son muy importantes en el estudio del álgebra abstracta, y de igual forma, son muy importantes en el diseño y el uso de Sage. Este capítulo contiene mucho material, y hay muchos comandos correspondientes en Sage.

Creando Anillos

Acá hay una lista de varios anillos, dominio y cuerpos que se pueden construir de forma sencilla.

1. `Integers()`, `ZZ`: el dominio integral de los números enteros positivos y negativos, $\mathbb{Z}$.
2. `Integers(n)`: los enteros mód n, $\mathbb{Z}_n$. Un cuerpop cuando n es primo, pero solo un anillo cuando n es compuesto.
3. `QQ`: el cuerpo de los números racionales, $\mathbb{Q}$.
4. `RR`, `CC`: el cuerpos de los números reales y el cuerpo de los números complejos, $\mathbb{R}$, $\mathbb{C}$. Es imposible crear *todo* número real en un computador, así es que técnicamenteso estos conjuntos no se comportan como cuerpos, sino solo ofrecen una buena imitación del objeto real. Decimos que son anillos ***inexactos*** para enfatizar este punto.
5. `QuadraticField(n)`: el cuerpo obtenido de adjuntar una solución de la ecuación $x^2 - n = 0$ a los números racionales. La notación en el texto es $\mathbb{Q}[\sqrt{n}]$. Una forma equivalente funcionalmente de construirlos es con la sintaxis `QQ[sqrt(n)]`. Notemos que `n` puede ser negativo.
6. `CyclotomicField(n)`: el cuerpo formado de adjuntar las soluciones de la ecuación polinomial $x^n - 1 = 0$ a los números racionales.
7. `QQbar`: el cuerpo formado de adjuntar soluciones de *toda* ecuación polinomial con coeficientes enteros al cuerpo de los números racionales. Este se conoce como el cuerpo de los números algebraicos, y se denota como $\overline{\mathbb{Q}}$.
8. `FiniteField(p)`: para un primo p, es el cuerpo $\mathbb{Z}_p$.

Cuando se muestra una descripción de algunos de los anillos anteriores, se puede ver la introducción de nuevos símbolos. Considere el siguiente ejemplo:

```
F = QuadraticField(7)
F
```

```
Number Field in a with defining polynomial x^2 - 7
```

```
root = F.gen(0)
root^2
```

```
7
```

```
root
```

```
a
```

```
(2*root)^3
```

```
56*a
```

Acá `Number Field` describe un objecto generalmente formado combinando los racionales con otro número (en este caso $\sqrt{7}$). "a" es un nunevo símbolo que se comporta como una raíz del polinomio $x^2 - 7$. No especificamos cuál raíz, $\sqrt{7}$ o $-\sqrt{7}$, y en la medida que comprendamos mejor la teoría, veremos que esta distinción no importa realmente.

Podemos obtener esta raíz como un generador del cuerpo de números, y luego manipularla. Elevando `root` al cuadrado, nos da 7. Notemos que `root` se muestra como `a`. Notemos, además, que los cálculos que involucran a `root` se comportan como si fuera *cualquier* raíz de $x^2 - 7$, y los resultados se muestran usando `a`.

Esto puede ser un poco confuso, ingresar los cálculos usando `root` y obtener respuestas en términos de `a`. Afortunadamente, hay una mejor forma. Considere el siguiente ejemplo:

```
F.<b> = QuadraticField(7)
F
```

```
Number Field in b with defining polynomial x^2 - 7
```

```
b^2
```

```
7
```

```
(2*b)^3
```

```
56*b
```

Con la sintaxis `F.<b>` podemos crear el cuerpo `F` especificando al mismo tiempo un generador `b` con un nombre de nuestra elección. Luego los cálculos podrán usar `b` tanto en la entrada como en la salida como una raíz de $x^2 - 7$.

Acá hay tres nuevos anillos que se crean mejor con esta nueva sintaxis.

1. `F.<a> = FiniteField(p^n)`: Más adelante tendremos un teorema que diga que los cuerpos finitos existen solo de orden igual a una potencia de un primo. Si la potencia es mayor a 1, entonces necesitamos un generador, en este caso dado como `a`.

2. `P.<x>=R[]`: el anillo de todos los polinomios en la variable `x`, con coeficientes en el anillo `R`. Notemos que `R` puede ser *cualquier* anillo, de manera que esta es una construcción muy general que usa un anillo para formar otro. Vea el ejemplo abajo.

3. `Q.<r,s,t> = QuaternionAlgebra(n, m)`: los racionales combinados con indeterminadas `r`, `s` y `t` tales que $r^2 = n$, $s^2 = m$ y $t = rs = -sr$. Esta es na generalización de los cuaterniones descritos en este capítulo, pero sobre lo racionales en lugar de los reales, de manera que es un anillo exacto. Notemos que este es uno de los pocos anillos no-conmutativos en Sage. Los cuaterniones "usuales" se construyen como `Q.<I,J,K> = QuaternionAlgebra(-1, -1)`. (Notemo que usar `I` en esta construcción no es la mejor idea, pues estaríamos redefiniendo el símbolo `I` usado para el número complejo i.)

La sintaxis que especifica los nombres de los generadores puede también ser usada para muchos de los anillos de más arriba, como se ha demostrado para los cuerpos cuadráticos y se demuestra más abajo para los cuerpos ciclotómicos.

```
C.<t> = CyclotomicField(8)
C.random_element()
```

```
-2/11*t^2 + t - 1
```

Propiedades de los Anillos

Los ejemplos abajo muestran como preguntar por ciertas propiedades de los anillos. Asegúrese de ejecutar la primera celda, pues allí se definen los distintos anillos involucrados en los ejemplos posteriores.

```
Z7 = Integers(7)
Z9 = Integers(9)
Q = QuadraticField(-11)
F.<a> = FiniteField(3^2)
P.<x> = Z7[]
S.<f,g,h> = QuaternionAlgebra(-7, 3)
```

Exacto versus inexacto.

```
QQ.is_exact()
```

```
True
```

```
RR.is_exact()
```

```
False
```

Finito versus infinito.

```
Z7.is_finite()
```

```
True
```

```
Z7.is_finite()
```

```
True
```

¿Dominio integral?

```
Z7.is_integral_domain()
```

```
True
```

```
Z9.is_integral_domain()
```

```
False
```

¿Cuerpo?

```
Z9.is_field()
```

```
False
```

```
F.is_field()
```

```
True
```

```
Q.is_field()
```

```
True
```

¿Conmutativo?

```
Q.is_commutative()
```

```
True
```

```
S.is_commutative()
```

```
False
```

Característica.

```
Z7.characteristic()
```

```
7
```

```
Z9.characteristic()
```

```
9
```

```
Q.characteristic()
```

```
0
```

```
F.characteristic()
```

```
3
```

```
P.characteristic()
```

```
7
```

```
S.characteristic()
```

```
0
```

Neutros aditivo y multiplicativo se *muestran* como uno esperaría, pero notemos que si bien se puedan *mostrar* idénticos, podrían ser *diferentes* debido al anillo en el que están.

```
b = Z9.zero(); b
```

```
0
```

```
b.parent()
```

```
Ring of integers modulo 9
```

```
c = Q.zero(); c
```

```
0
```

```
c.parent()
```

```
Number Field in a with defining polynomial x^2 + 11
```

```
b == c
```

```
False
```

```
d = Z9.one(); d
```

```
1
```

```
d.parent()
```

```
Ring of integers modulo 9
```

```
e = Q.one(); e
```

```
1
```

```
e.parent()
```

```
Number Field in a with defining polynomial x^2 + 11
```

```
d == e
```

```
False
```

Existe cierta implementación de subanillos. Por ejemplo, `Q` y `S` son extensiones de los racionales, mientras `F` es totalmente distinto de los racionales.

```
QQ.is_subring(Q)
```

```
True
```

```
QQ.is_subring(S)
```

```
True
```

```
QQ.is_subring(F)
```

```
False
```

No todo elemento de un anillo tiene inverso multiplicativo. Puede ser una buena práctica verificar si un elemento es una unidad antes de intentar calcular su inverso.

```
three = Z9(3)
three.is_unit()
```

```
False
```

```
three*three
```

```
0
```

```
four = Z9(4)
four.is_unit()
```

```
True
```

```
g = four^-1; g
```

```
7
```

```
four*g
```

```
1
```

Estructuras Cociente

Ideales corresponden a los subgrupos normales en el caso de anillos y nos permiten contruir "cocientes" — básicamente anillos nuevos definidos sobre clases de equivalencia de elementos del anillo original. La implementación de ideales en Sage es dispar. Cuando pueden ser creados, no siempre es mucho lo que se puede hacer con ellos. Pero funcionan bien en algunos casos muy importantes.

El anillo de los enteros, $\mathbb{Z}$, tiene ideales que son simplemente los múltiplos de un solo entero. Los podemos crear con el método `.ideal()` o escribiendo un múltiplo escalar de `ZZ`. Luego el cociente es isomorfo a un anillo que entendemos bien. (Note que `I` es un mal nombre para un ideal si queremos trabajar con números complejos más adelante.)

```
I1 = ZZ.ideal(4)
I2 = 4*ZZ
I3 = (-4)*ZZ
I1 == I2
```

```
True
```

```
I2 == I3
```

```
True
```

```
Q = ZZ.quotient(I1); Q
```

```
Ring of integers modulo 4
```

```
Q == Integers(4)
```

```
True
```

Usualmente seremos más cuidadosos con la última instrucción. El cociente es un conjunto de clases de equivalencia, cada una infinita, ciertamente no es un solo entero. Pero el cociente es *isomorfo* a $\mathbb{Z}_4$, de manera que Sage simplemente hace esa identificación.

```
Z7 = Integers(7)
P.<y> = Z7[]
M = P.ideal(y^2+4)
Q = P.quotient(M)
Q
```

```
Univariate Quotient Polynomial Ring in ybar over
Ring of integers modulo 7 with modulus y^2 + 4
```

```
Q.random_element()
```

```
2*ybar + 6
```

```
Q.order()
```

```
49
```

```
Q.is_field()
```

```
True
```

Notemos que la construcción del anillo cociente a creado un nuevo generador, convirtiendo `y` (y) en `ybar` ($\overline{y}$). Podemos modificar este comportamiento con la sintaxis mostrada abajo.

```
Q.<t> = P.quotient(M); Q
```

```
Univariate Quotient Polynomial Ring in t over
Ring of integers modulo 7 with modulus y^2 + 4
```

```
Q.random_element()
```

```
4*t + 6
```

Así del cociente de una anillo infinito por un ideal (que también es un anillo), creamos un cuerpo, que es finito. Entender esta construcción será un tópico importante en los próximos capítulos. Para ver lo notable que es, considere lo que pasa con un pequeño cambio.

```
Z7 = Integers(7)
P.<y> = Z7[]
M = P.ideal(y^2+3)
Q.<t> = P.quotient(M)
Q
```

```
Univariate Quotient Polynomial Ring in t over
Ring of integers modulo 7 with modulus y^2 + 3
```

```
Q.random_element()
```

```
3*t + 1
```

```
Q.order()
```

```
49
```

```
Q.is_field()
```

```
False
```

Hay unos pocos métodos disponibles que nos darán propiedades de los ideales. En particular, podemos preguntar si un ideal en un anillo de polinomios es primo o maximal. Examine los resultados de arriba y de abajo en el contexto del Teorema 16.35.

```
Z7 = Integers(7)
P.<y> = Z7[]
M = P.ideal(y^2+4)
N = P.ideal(y^2+3)
M.is_maximal()
```

```
True
```

```
N.is_maximal()
```

```
False
```

El hecho de que `M` sea un ideal primo es una verificación del Corolario 16.40.

```
M.is_prime()
```

```
True
```

```
N.is_prime()
```

```
False
```

Homomorfismo de Anillos

Cuando Sage recibe la entrada `3 + 4/3`, ¿cómo sabe que se supone que 3 es un número entero? Y depués al sumarlo con un racional, ¿cómo sabe que lo que queremos es la suma de racionales, $3/1 + 4/3$? Esto es muy fácil para una persona como usted o como yo, pero extremadamente complejo para un programa, y usted se podrá imaginar que se vuelve cada vez más difícil con los muchos posible anillos, subanillos, matrices, etc en Sage. Una parte de la respuesta es que Sage usa homomorfismos de anillos para "traducir" objectos (números) entre anillos.

Daremos un ejemplo abajo, pero no insistiremos mucho con el tema. Si tiene curiosidad, leer la documentación de Sage y experimentar un poco pueden ser ejercicios interesantes.

```
H = Hom(ZZ, QQ)
phi = H([1])
phi
```

```
Ring morphism:
  From: Integer Ring
  To:   Rational Field
  Defn: 1 |--> 1
```

```
phi.parent()
```

```
Set of Homomorphisms from Integer Ring to Rational Field
```

```
a = 3; a
```

```
3
```

```
a.parent()
```

```
Integer Ring
```

```
b = phi(3); b
```

```
3
```

```
b.parent()
```

```
Rational Field
```

Así `phi` es un homomorfismo ("morfismo") que convierte números enteros (el dominio es `ZZ`) en racionales (el codominio es `QQ`), cuyo parent es un conjunto de homomorfismos que Sage denomina "homset." Si bien tanto `a` como `b` se muestran como `3`, de forma indistinguible a la vista, los parents de `a` y `b` son diferentes.

16.10 Ejercicios en Sage

1. Defina los dos anillos $\mathbb{Z}_{11}$ y $\mathbb{Z}_{12}$ usando los comandos `R = Integers(11)` y `S = Integers(12)`. Para cada anillo, use los comandos relevantes para determinar: si el anillo es finito, si es conmutativo, si es un dominio integral y si es un cuerpo. Luego use comandos Sage para encontrar el orden del anillo, listar sus elementos, y mostrar su neutro multiplicativo (i.e. 1, si es que existe).

2. Defina `R` como el anillo de los números enteros, $\mathbb{Z}$, ejecutando `R = ZZ` o `R = Integers()`. Un comando como `R.ideal(4)` creará el ideal principal $\langle 4 \rangle$. El mismo comando puede recibir mñas de un generador, por ejemplo, `R.ideal(3, 5)` creará el ideal $\{a \cdot 3 + b \cdot 5 \mid a, b \in \mathbb{Z}\}$. Cree varios ideales de $\mathbb{Z}$ con dos generadores y pídale a Sage que los muestre al crearlos. Explique lo que observa y escriba comandos que le permitan comprobar su observación para miles de ejemplos diferentes.

3. Cree un cuerpo finito F de orden 81 por medio de `F.<t>=FiniteField(3^4)`.

(a) Liste los elementos de F.

(b) Obtenga los generadores de F con `F.gens()`.

(c) Obtenga el primer generador de F y guárdelo como `u` con `u = F.0` (alternativamente, `u = F.gen(0)`).

(d) Calcule las primeras 80 potencias de `u` y comente.

(e) El generador con el que trabajó arriba es una raíz de un polinomio sobre $\mathbb{Z}_3$. Obtenga este polinomio con `F.modulus()` y use esta observación para explicar la entrada correspondiente a la cuarta potencia en su lista de potencias del generador.

4. Construya y analice un anillo cociente como sigue:

(a) Use `P.<z>=Integers(7)[]` para construir un anillo P de polinomios en z con coeficientes en $\mathbb{Z}_7$.

(b) Use `K = P.ideal(z^2+z+3)` para contruir el ideal principal K generado por el polinomio $z^2 + z + 3$.

(c) Use `H = P.quotient(K)` para contruir H, el anillo cociente de P por K.

(d) Use Sage para comprobar que H es un cuerpo.

(e) Como en el ejercicio anterior, obtenga un generador y examine la colección de potencias de ese generador.

17

Polinomios

La mayoría de las personas está razonablemente familiarizada con los polinomios cuando comienza a estudiar álgebra abstracta. Cuando examinamos expresiones polinomiales como

$$p(x) = x^3 - 3x + 2$$
$$q(x) = 3x^2 - 6x + 5,$$

tenemos una idea bastante clara de lo que significan $p(x) + q(x)$ y $p(x)q(x)$. Simplemente sumamos y multiplicamos polinomios como funciones; es decir,

$$\begin{aligned}(p+q)(x) &= p(x) + q(x) \\ &= (x^3 - 3x + 2) + (3x^2 - 6x + 5) \\ &= x^3 + 3x^2 - 9x + 7\end{aligned}$$

y

$$\begin{aligned}(pq)(x) &= p(x)q(x) \\ &= (x^3 - 3x + 2)(3x^2 - 6x + 5) \\ &= 3x^5 - 6x^4 - 4x^3 + 24x^2 - 27x + 10.\end{aligned}$$

Probablemente no es una sorpresa que los polinomios forman un anillo. En este capítulo enfatizaremos la estructura algebraica de los polinomios estudiando anillos de polinomios. Podemos demostrar muchos resultados para anillos de polinomio que son similares a los teoremas que demostramos para los enteros. Existen análogos de los números primos, el algoritmo de división y el algoritmo de Euclides para polinomios.

17.1 Anillos de Polinomios

En todo este capítulo supondremos que R es un anillo conmutativo con uno. Una expresión de la forma

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

donde $a_i \in R$ y $a_n \neq 0$, se llama ***polinomio sobre*** R con ***indeterminada*** x. Los elementos $a_0, a_1, \ldots, a_n$ se llaman ***coeficientes*** de f. El coeficiente a_n se llama ***coeficiente líder***. Un polinomio se llama ***mónico*** si su coeficiente líder es 1. Si n es el mayor entero no negativo para el que $a_n \neq 0$, decimos que el ***grado*** de f es n y escribimos $\operatorname{gr} f(x) = n$. Si no existe tal n—es decir,

si $f = 0$ es el polinomio cero—entonces el grado de f se define como $-\infty$. Denotaremos por $R[x]$ al conjunto de todos los polinomios con coeficientes en un anillo R. Dos polinomios son iguales exactamente cuando sus coeficientes correspondientes son iguales; es decir, si

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$
$$q(x) = b_0 + b_1x + \cdots + b_mx^m,$$

entonces $p(x) = q(x)$ si y solo si $a_i = b_i$ para todo $i \geq 0$.

Para mostrar que el conjunto de todos los polinomios forma un anillo, debemos primero definir adición y multiplicación. Definimos la suma de dos polinomios como sigue. Sean

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$
$$q(x) = b_0 + b_1x + \cdots + b_mx^m.$$

Entonces la suma de $p(x)$ y $q(x)$ es

$$p(x) + q(x) = c_0 + c_1x + \cdots + c_kx^k,$$

donde $c_i = a_i + b_i$ for each i. Definimos el producto de $p(x)$ y $q(x)$ como

$$p(x)q(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n},$$

donde

$$c_i = \sum_{k=0}^{i} a_kb_{i-k} = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0$$

para cada i. Notemos que en cada caso algunos de los coeficientes pueden ser cero.

Ejemplo 17.1. Supongamos que

$$p(x) = 3 + 0x + 0x^2 + 2x^3 + 0x^4$$

y

$$q(x) = 2 + 0x - x^2 + 0x^3 + 4x^4$$

son polinomios en $\mathbb{Z}[x]$. Si el coeficiente de algún término en un polinomio es cero, entonces simplemente omitiremos ese término. En este caso escribiremos $p(x) = 3 + 2x^3$ y $q(x) = 2 - x^2 + 4x^4$. La suma de estos dos polinomios es

$$p(x) + q(x) = 5 - x^2 + 2x^3 + 4x^4.$$

El producto,

$$p(x)q(x) = (3 + 2x^3)(2 - x^2 + 4x^4) = 6 - 3x^2 + 4x^3 + 12x^4 - 2x^5 + 8x^7,$$

puede ser calculado ya sea determinando los c_i en la definición o simplemente multiplicando los polinomios de la misma forma en que lo hemos hecho siempre.

Ejemplo 17.2. Sean

$$p(x) = 3 + 3x^3 \qquad \text{and} \qquad q(x) = 4 + 4x^2 + 4x^4$$

polinomios en $\mathbb{Z}_{12}[x]$. La suma de $p(x)$ y $q(x)$ es $7 + 4x^2 + 3x^3 + 4x^4$. El producto de los dos polinomios es el polinomio cero. Este ejemplo nos muestra que no podemos esperar que $R[x]$ sea un dominio integral si R no es un dominio integral.

Teorema 17.3. *Sea R un anillo conmutativo con identidad. Entonces $R[x]$ es un anillo conmutativo con identidad.*

Demostración. Nuestra primera tarea es mostrar que $R[x]$ es un grupo abeliano con la operación de suma de polinomios. El polinomio cero, $f(x) = 0$, es el neutro aditivo. Dado un polinomio $p(x) = \sum_{i=0}^{n} a_i x^i$, el inverso aditivo de $p(x)$ es $-p(x) = \sum_{i=0}^{n} (-a_i) x^i = -\sum_{i=0}^{n} a_i x^i$. La conmutatividad y la asociatividad son consecuencia inmediata de la definición de la suma de polinomios y del hecho que la adición en R es tanto conmutativa como asociativa.

Para mostrar que la multiplicación de polinomios es asociativa, sean

$$\begin{aligned} p(x) &= \sum_{i=0}^{m} a_i x^i, \\ q(x) &= \sum_{i=0}^{n} b_i x^i, \\ r(x) &= \sum_{i=0}^{p} c_i x^i. \end{aligned}$$

Entonces

$$\begin{aligned} [p(x)q(x)]r(x) &= \left[\left(\sum_{i=0}^{m} a_i x^i \right) \left(\sum_{i=0}^{n} b_i x^i \right) \right] \left(\sum_{i=0}^{p} c_i x^i \right) \\ &= \left[\sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i \right] \left(\sum_{i=0}^{p} c_i x^i \right) \\ &= \sum_{i=0}^{m+n+p} \left[\sum_{j=0}^{i} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) c_{i-j} \right] x^i \\ &= \sum_{i=0}^{m+n+p} \left(\sum_{j+k+l=i} a_j b_k c_l \right) x^i \\ &= \sum_{i=0}^{m+n+p} \left[\sum_{j=0}^{i} a_j \left(\sum_{k=0}^{i-j} b_k c_{i-j-k} \right) \right] x^i \\ &= \left(\sum_{i=0}^{m} a_i x^i \right) \left[\sum_{i=0}^{n+p} \left(\sum_{j=0}^{i} b_j c_{i-j} \right) x^i \right] \\ &= \left(\sum_{i=0}^{m} a_i x^i \right) \left[\left(\sum_{i=0}^{n} b_i x^i \right) \left(\sum_{i=0}^{p} c_i x^i \right) \right] \\ &= p(x)[q(x)r(x)] \end{aligned}$$

La conmutatividad y la distributividad se demuestran de forma similar. Dejaremos estas demostraciones como ejercicios. □

Proposición 17.4. *Sean $p(x)$ y $q(x)$ polinomios en $R[x]$, donde R es un dominio integral. Entonces* $\operatorname{gr} p(x) + \operatorname{gr} q(x) = \operatorname{gr}(p(x)q(x))$. *Además, $R[x]$ es un dominio integral.*

Demostración. Supongamos que tenemos dos polinomios distintos de cero

$$p(x) = a_m x^m + \cdots + a_1 x + a_0$$

y

$$q(x) = b_n x^n + \cdots + b_1 x + b_0$$

con $a_m \neq 0$ y $b_n \neq 0$. Los grados de $p(x)$ y $q(x)$ son m y n, respectivamente. El término líder de $p(x)q(x)$ es $a_m b_n x^{m+n}$, que no puede ser cero pues R es un dominio integral; Vemos que el grado de $p(x)q(x)$ es $m+n$, y $p(x)q(x) \neq 0$. Como $p(x) \neq 0$ y $q(x) \neq 0$ implica que $p(x)q(x) \neq 0$, concluimos que $R[x]$ también es un dominio integral. □

También queremos considerar polynomios en dos o más variables, tales cómo $x^2 - 3xy + 2y^3$. Sea R un anillo y supongamos que tenemos dos indeterminadas x e y. Ciertamente podemos formar el anillo $(R[x])[y]$. Es directo, aunque quizás tedioso, demostrar que $(R[x])[y] \cong R([y])[x]$. Identificaremos estos dos anillos por medio de este isomorfismo y simplemente escribiremos $R[x, y]$. El anillo $R[x, y]$ se llama ***anillo de polinomios en dos indeterminadas*** x ***e*** y ***con coeficientes en*** R. Podemos definir similarmente el ***anillo de polinomios en*** n ***indeterminadas con coeficientes en*** R. Denotaremos este anillo por $R[x_1, x_2, \ldots, x_n]$.

Teorema 17.5. *Sea R un anillo conmutativo con identidad y sea $\alpha \in R$. Entonces tenemos un homomorfismo de anillos $\phi_\alpha : R[x] \to R$ definido por*

$$\phi_\alpha(p(x)) = p(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0,$$

donde $p(x) = a_n x^n + \cdots + a_1 x + a_0$.

Demostración. Sean $p(x) = \sum_{i=0}^{n} a_i x^i$ y $q(x) = \sum_{i=0}^{m} b_i x^i$. Es fácil mostrar que $\phi_\alpha(p(x)+q(x)) = \phi_\alpha(p(x)) + \phi_\alpha(q(x))$. Para mostrar que la multiplicación es preservada por la función ϕ_α, observemos que

$$\begin{aligned}
\phi_\alpha(p(x))\phi_\alpha(q(x)) &= p(\alpha)q(\alpha) \\
&= \left(\sum_{i=0}^{n} a_i \alpha^i\right)\left(\sum_{i=0}^{m} b_i \alpha^i\right) \\
&= \sum_{i=0}^{m+n} \left(\sum_{k=0}^{i} a_k b_{i-k}\right) \alpha^i \\
&= \phi_\alpha(p(x)q(x)).
\end{aligned}$$

□

La función $\phi_\alpha : R[x] \to R$ se llama ***homomorfismo de evaluación*** en α.

17.2 El Algoritmo de División

Recuerde que el algoritmo de división para enteros (Teorema 2.9) dice que si a y b son enteros con $b > 0$, entonces existen únicos enteros q y r tales que $a = bq + r$, con $0 \leq r < b$. Un teorema similar existe para polinomios. El algoritmo de división para polinomios tiene varias consecuencias importantes. Como su demostración es muy similar a la demostración correspondiente para los enteros, resulta conveniente revisar el Teorema 2.9 antes de seguir.

Teorema 17.6 (Algoritmo de División)**.** *Sean $f(x)$ y $g(x)$ polinomios en $F[x]$, donde F es un cuerpo y $g(x)$ es un polinomio distinto de cero. Entonces existen polinomios únicos $q(x), r(x) \in F[x]$ tales que*

$$f(x) = g(x)q(x) + r(x),$$

con $\operatorname{gr} r(x) < \operatorname{gr} g(x)$ o $r(x) = 0$.

DEMOSTRACIÓN. Primero demostraremos la existencia de $q(x)$ y $r(x)$. Si $f(x)$ es el polinomio cero, entonces

$$0 = 0 \cdot g(x) + 0;$$

luego, tanto q como r también son el polinomio cero. Ahora supongamos que $f(x)$ no es polinomio cero y que $\operatorname{gr} f(x) = n$ y $\operatorname{gr} g(x) = m$. Si $m > n$, entonces $q(x) = 0$ y $r(x) = f(x)$. Podemos ahora suponer que $m \leq n$ y proceder por inducción en n. Si

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

entonces el polinomio

$$f'(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$

tiene grado menor a n o es el polinomio cero. Por la hipótesis de inducción, existens polinomios $q'(x)$ y $r(x)$ tales que

$$f'(x) = q'(x)g(x) + r(x),$$

donde $r(x) = 0$ o el grado de $r(x)$ es menor al grado de $g(x)$. Ahora, sea

$$q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}.$$

Entonces

$$f(x) = g(x)q(x) + r(x),$$

con $r(x)$ el polinomio cero o $\operatorname{gr} r(x) < \operatorname{gr} g(x)$.

Para mostrar que $q(x)$ y $r(x)$ son únicos, supongamos que además existen $q_1(x)$ y $r_1(x)$ tales que $f(x) = g(x)q_1(x) + r_1(x)$ con $\operatorname{gr} r_1(x) < \operatorname{gr} g(x)$ o $r_1(x) = 0$, de manera que

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x),$$

y

$$g(x)[q(x) - q_1(x)] = r_1(x) - r(x).$$

Si $g(x)$ no es el polinomio cero, entonces

$$\operatorname{gr}(g(x)[q(x) - q_1(x)]) = \operatorname{gr}(r_1(x) - r(x)) \geq \operatorname{gr} g(x).$$

Pero, los grados tanto de $r(x)$ como de $r_1(x)$ son estrictamente menores que el grado de $g(x)$; por lo tanto, $r(x) = r_1(x)$ y $q(x) = q_1(x)$. □

Ejemplo 17.7. El algoritmo de división meramente formaliza la división larga de polinomios, una tarea con la que probablemente estamos familiarizados desde el colegio. Por ejemplo, supongamos que dividimos $x^3 - x^2 + 2x - 3$ por $x - 2$.

$$\begin{array}{rcl|rcrcrcr}
 & & & x^2 & + & x & + & 4 & & \\
\cline{4-10}
x & - & 2 & x^3 & - & x^2 & + & 2x & - & 3 \\
 & & & x^3 & - & 2x^2 & & & & \\
\cline{4-10}
 & & & & & x^2 & + & 2x & - & 3 \\
 & & & & & x^2 & - & 2x & & \\
\cline{4-10}
 & & & & & & & 4x & - & 3 \\
 & & & & & & & 4x & - & 8 \\
\cline{4-10}
 & & & & & & & & & 5
\end{array}$$

Luego, $x^3 - x^2 + 2x - 3 = (x - 2)(x^2 + x + 4) + 5$.

Sea $p(x)$ un polinomio en $F[x]$ y $\alpha \in F$. Decimos que α es un ***cero*** o ***raíz*** de $p(x)$ si $p(x)$ está en el núcleo del homomorfismo de evaluación ϕ_α. Lo único que estamos dicendo realmente es que α es un cero de $p(x)$ si $p(\alpha) = 0$.

Corolario 17.8. *Sea F un cuerpo. Un elemento $\alpha \in F$ es un cero de $p(x) \in F[x]$ si y solo si $x - \alpha$ divide a $p(x)$ en $F[x]$.*

Demostración. Supongamos que $\alpha \in F$ y $p(\alpha) = 0$. Por el algoritmo de la división, existen polinomios $q(x)$ y $r(x)$ tales que

$$p(x) = (x - \alpha)q(x) + r(x)$$

y el grado de $r(x)$ es menor que el grado de $x - \alpha$. Como el grado de $r(x)$ es menor a 1, $r(x) = a$ para algún $a \in F$; por lo tanto,

$$p(x) = (x - \alpha)q(x) + a.$$

Pero

$$0 = p(\alpha) = 0 \cdot q(\alpha) + a = a;$$

Por ende, $p(x) = (x - \alpha)q(x)$, y $x - \alpha$ es un factor de $p(x)$.

Recíprocamente, supongamos que $x - \alpha$ es un factor de $p(x)$; digamos $p(x) = (x - \alpha)q(x)$. Entonces $p(\alpha) = 0 \cdot q(\alpha) = 0$. □

Corolario 17.9. *Sea F un cuerpo. Un polinomio $p(x)$ distinto de cero y de grado n en $F[x]$ puede tener a lo sumo n ceros distintos en F.*

Demostración. Procederemos por inducción sobre el grado de $p(x)$. Si $\operatorname{gr} p(x) = 0$, entonces $p(x)$ es un polinomio constante y no tiene ceros. Si $\operatorname{gr} p(x) = 1$, entonces $p(x) = ax + b$ para ciertos a y b en F. Si α_1 y α_2 so ceros de $p(x)$, entonces $a\alpha_1 + b = a\alpha_2 + b$ y $\alpha_1 = \alpha_2$.

Ahora supongamos que $\operatorname{gr} p(x) > 1$. Si $p(x)$ no tiene ceros en F, estamos listos. Por otra parte, si α es un cero de $p(x)$, entonces $p(x) = (x - \alpha)q(x)$ para cierto $q(x) \in F[x]$ por el Corolario 17.8. El grado de $q(x)$ es $n - 1$ por la Proposición 17.4. Sea β algún otro cero de $p(x)$ distinto de α. Entonces $p(\beta) = (\beta - \alpha)q(\beta) = 0$. Como $\alpha \neq \beta$ y F es un cuerpo, $q(\beta) = 0$. Por la hipótesis de inducción, $q(x)$ puede tener a lo sumo $n - 1$ ceros distintos en F. Por lo tanto, $p(x)$ tiene a lo sumo n ceros distintos en F. □

Sea F un cuerpo. Un polinomio mónico $d(x)$ es un ***máximo común divisor*** de los polinomios $p(x), q(x) \in F[x]$ si $d(x)$ divide tanto a $p(x)$ como a $q(x)$; y, si para cualquier otro polinomio $d'(x)$ que divida tanto a $p(x)$ como a $q(x)$, $d'(x) \mid d(x)$. Escribiremos $d(x) = \operatorname{mcd}(p(x), q(x))$. Dos polinomios $p(x)$ y $q(x)$ son ***relativamente primos*** si $\operatorname{mcd}(p(x), q(x)) = 1$.

Proposición 17.10. *Sea F un cuerpo y supongamos que $d(x)$ es un máximo común divisor de dos polinomios $p(x)$ y $q(x)$ en $F[x]$. Entonces existen polinomios $r(x)$ y $s(x)$ tales que*

$$d(x) = r(x)p(x) + s(x)q(x).$$

Además, el máximo común divisor de dos polinomios es único.

Demostración. Sea $d(x)$ el polinomio mónico de menor grado en el conjunto

$$S = \{f(x)p(x) + g(x)q(x) : f(x), g(x) \in F[x]\}.$$

Podemos escribir $d(x) = r(x)p(x) + s(x)q(x)$ para dos polinomios $r(x)$ y $s(x)$ en $F[x]$. Debemos demostrar que $d(x)$ divide a $p(x)$ y a $q(x)$. Primero

mostraremos que $d(x)$ divide a $p(x)$. Por el algoritmo de división, existen polinomios $a(x)$ y $b(x)$ tales que $p(x) = a(x)d(x) + b(x)$, donde $b(x)$ es el polinomio cero o $\operatorname{gr} b(x) < \operatorname{gr} d(x)$. Por lo tanto,

$$\begin{aligned} b(x) &= p(x) - a(x)d(x) \\ &= p(x) - a(x)(r(x)p(x) + s(x)q(x)) \\ &= p(x) - a(x)r(x)p(x) - a(x)s(x)q(x) \\ &= p(x)(1 - a(x)r(x)) + q(x)(-a(x)s(x)) \end{aligned}$$

es una combinación lineal de $p(x)$ y $q(x)$ y por lo tanto está en S. Entonces, $b(x)$ debe ser el polinomio cero pues $d(x)$ fue elegido de grado minimal; Concluimos que $d(x)$ divide a $p(x)$. Un argumento simétrico muestra que $d(x)$ también divide a $q(x)$; luego, $d(x)$ es un divisor común de $p(x)$ y $q(x)$.

Para mostrar que $d(x)$ es un máximo común divisor de $p(x)$ y $q(x)$, supongamos que $d'(x)$ es otro divisor común de $p(x)$ y $q(x)$. Mostraremos que $d'(x) \mid d(x)$. Como $d'(x)$ es un divisor común de $p(x)$ y $q(x)$, existen polinomios $u(x)$ y $v(x)$ tales que $p(x) = u(x)d'(x)$ y $q(x) = v(x)d'(x)$. Por lo tanto,

$$\begin{aligned} d(x) &= r(x)p(x) + s(x)q(x) \\ &= r(x)u(x)d'(x) + s(x)v(x)d'(x) \\ &= d'(x)[r(x)u(x) + s(x)v(x)]. \end{aligned}$$

Como $d'(x) \mid d(x)$, $d(x)$ es un máximo común divisor de $p(x)$ y $q(x)$.

Finalmente, debemos mostrar que el máximo común divisor de $p(x)$ y $q(x)$ es único. Supongamos que $d'(x)$ también es un máximo común divisor de $p(x)$ y $q(x)$. Acabamos de mostrar que existen polinomios $u(x)$ y $v(x)$ en $F[x]$ tales que $d(x) = d'(x)[r(x)u(x) + s(x)v(x)]$. Como

$$\operatorname{gr} d(x) = \operatorname{gr} d'(x) + \operatorname{gr}[r(x)u(x) + s(x)v(x)]$$

y $d(x)$ y $d'(x)$ son ambos máximo común divisor, $\operatorname{gr} d(x) = \operatorname{gr} d'(x)$. Como $d(x)$ y $d'(x)$ son ambos polinomios mónicos del mismo grado, se debe tener que $d(x) = d'(x)$. □

Notemos la similaridad entre la demostración de la Proposición 17.10 y la demostración del Teorema 2.10.

17.3 Polinomios Irreducibles

Un polinomio no constante $f(x) \in F[x]$ es ***irreducible*** sobre un cuerpo F si $f(x)$ no puede ser expresado como producto de dos polinomios $g(x)$ y $h(x)$ en $F[x]$, donde los grados de $g(x)$ y $h(x)$ son ambos menores que el grado de $f(x)$. Los polinomios irreducibles funcionan como los "números primos" de los anillos de polinomios.

Ejemplo 17.11. El polinomio $x^2 - 2 \in \mathbb{Q}[x]$ es irreducible pues no puede ser factorizado sobre los números racionales. Similarmente, $x^2 + 1$ es irreducible sobre los números reales.

Ejemplo 17.12. El polinomio $p(x) = x^3 + x^2 + 2$ es irreducible sobre $\mathbb{Z}_3[x]$. Supongamos que este polinomio fuera reducible sobre $\mathbb{Z}_3[x]$. Por el algoritmo de división tendría que haber un factor de la forma $x - a$, donde a es algún elemento en $\mathbb{Z}_3[x]$. Es decir, tendríamos que tener $p(a) = 0$. Pero,

$$p(0) = 2$$

$$p(1) = 1$$
$$p(2) = 2.$$

Por lo tanto, $p(x)$ no tiene ceros en $\mathbb{Z}_3$ y es irreducible.

Lema 17.13. *Sea $p(x) \in \mathbb{Q}[x]$. Entonces*

$$p(x) = \frac{r}{s}(a_0 + a_1 x + \cdots + a_n x^n),$$

donde $r, s, a_0, \ldots, a_n$ son enteros, los a_i son relativamente primos, y r y s son relativamente primos.

DEMOSTRACIÓN. Supongamos que

$$p(x) = \frac{b_0}{c_0} + \frac{b_1}{c_1}x + \cdots + \frac{b_n}{c_n}x^n,$$

donde los b_i y los c_i son enteros. Podemos reescribir $p(x)$ como

$$p(x) = \frac{1}{c_0 \cdots c_n}(d_0 + d_1 x + \cdots + d_n x^n),$$

donde $d_0, \ldots, d_n$ son enteros. Sea d el máximo común divisor de $d_0, \ldots, d_n$. Entonces

$$p(x) = \frac{d}{c_0 \cdots c_n}(a_0 + a_1 x + \cdots + a_n x^n),$$

donde $d_i = da_i$ y los a_i son relativamente primos. Reduciendo $d/(c_0 \cdots c_n)$ to its lowest terms, podemos escribir

$$p(x) = \frac{r}{s}(a_0 + a_1 x + \cdots + a_n x^n),$$

donde $\operatorname{mcd}(r, s) = 1$. □

Teorema 17.14 (Lema de Gauss)**.** *Sea $p(x) \in \mathbb{Z}[x]$ un polinomio mónico tal que $p(x)$ se factoriza como producto de dos polinomios $\alpha(x)$ y $\beta(x)$ en $\mathbb{Q}[x]$, donde los grados de $\alpha(x)$ y de $\beta(x)$ son menores que el grado de $p(x)$. Entonces $p(x) = a(x)b(x)$, donde $a(x)$ y $b(x)$ son polinomios mónicos en $\mathbb{Z}[x]$ con $\operatorname{gr}\alpha(x) = \operatorname{gr} a(x)$ y $\operatorname{gr}\beta(x) = \operatorname{gr} b(x)$.*

DEMOSTRACIÓN. Por el Lema 17.13, podemos suponer que

$$\alpha(x) = \frac{c_1}{d_1}(a_0 + a_1 x + \cdots + a_m x^m) = \frac{c_1}{d_1}\alpha_1(x)$$
$$\beta(x) = \frac{c_2}{d_2}(b_0 + b_1 x + \cdots + b_n x^n) = \frac{c_2}{d_2}\beta_1(x),$$

donde los a_i son relativamente primos y los b_i son relativamente primos. En consecuencia,

$$p(x) = \alpha(x)\beta(x) = \frac{c_1 c_2}{d_1 d_2}\alpha_1(x)\beta_1(x) = \frac{c}{d}\alpha_1(x)\beta_1(x),$$

donde c/d es el producto de c_1/d_1 y c_2/d_2 expresado de forma reducida. Luego, $dp(x) = c\alpha_1(x)\beta_1(x)$.

Si $d = 1$, entonces $ca_m b_n = 1$ pues $p(x)$ es un polinomio mónico. Luego, ya sea $c = 1$ o $c = -1$. Si $c = 1$, entonces ya sea $a_m = b_n = 1$ o $a_m = b_n = -1$. En el primer caso $p(x) = \alpha_1(x)\beta_1(x)$, donde $\alpha_1(x)$ y $\beta_1(x)$ son polinomios mónicos con $\operatorname{gr}\alpha(x) = \operatorname{gr}\alpha_1(x)$ y $\operatorname{gr}\beta(x) = \operatorname{gr}\beta_1(x)$. En el segundo caso $a(x) = -\alpha_1(x)$ y $b(x) = -\beta_1(x)$ son los polinomios mónicos correctos pues

$p(x) = (-\alpha_1(x))(-\beta_1(x)) = a(x)b(x)$. El caso cuando $c = -1$ se resuelve de forma similar.

Ahora supongamos que $d \neq 1$. Como $\text{mcd}(c, d) = 1$, existe un primo p tal que $p \mid d$ y $p \not| c$. Además, como los coeficientes de $\alpha_1(x)$ son relativamente primos, existe un coeficiente a_i tal que $p \not| a_i$. Similarmente, existe un coeficiente b_j de $\beta_1(x)$ tal que $p \not| b_j$. Sean $\alpha_1'(x)$ y $\beta_1'(x)$ los polinomios en $\mathbb{Z}_p[x]$ obtenidos de reducir los coeficientes de $\alpha_1(x)$ y $\beta_1(x)$ módulo p. Como $p \mid d$, $\alpha_1'(x)\beta_1'(x) = 0$ en $\mathbb{Z}_p[x]$. Pero esto es imposible, pues ni $\alpha_1'(x)$ ni $\beta_1'(x)$ es el polinomio cero y $\mathbb{Z}_p[x]$ es un dominio integral. Por lo tanto, $d = 1$ y el teorema está demostrado. □

Corolario 17.15. *Sea $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ un polinomio con coeficientes en $\mathbb{Z}$ y $a_0 \neq 0$. Si $p(x)$ tiene un cero en $\mathbb{Q}$, entonces $p(x)$ también tiene un cero α en $\mathbb{Z}$. Más aún, α divide a a_0.*

Demostración. Supongamos que $p(x)$ tiene un cero $a \in \mathbb{Q}$. Entonces $p(x)$ debe tener un factor lineal $x - a$. Por el Lema de Gauss, $p(x)$ tiene una factorización con un factor lineal en $\mathbb{Z}[x]$. Luego, para algún $\alpha \in \mathbb{Z}$

$$p(x) = (x - \alpha)(x^{n-1} + \cdots - a_0/\alpha).$$

Por lo tanto $a_0/\alpha \in \mathbb{Z}$ y $\alpha \mid a_0$. □

Ejemplo 17.16. Sea $p(x) = x^4 - 2x^3 + x + 1$. Demostraremos que $p(x)$ es irreducible sobre $\mathbb{Q}[x]$. Supongamos que $p(x)$ es reducible. Entonces ya sea $p(x)$ tiene un factor lineal, digamos $p(x) = (x - \alpha)q(x)$, donde $q(x)$ es un polinomio d egrado tres, o $p(x)$ tiene dos factores cuadráticos.

Si $p(x)$ tiene un factor lineal en $\mathbb{Q}[x]$, entonces tiene un cero en $\mathbb{Z}$. Por el Corolario 17.15, cualquier cero debe dividir a 1 y por lo tanto debe ser ± 1; pero, $p(1) = 1$ y $p(-1) = 3$. Así hemos descartado la posibilidad de que $p(x)$ tenga un factor lineal.

Por lo tanto, si $p(x)$ es reducible debe ser como producto de dos factores cuadráticos, digamos

$$\begin{aligned} p(x) &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd, \end{aligned}$$

donde cada factor está en $\mathbb{Z}[x]$ por el Lema de Gauss. Luego,

$$\begin{aligned} a + c &= -2 \\ ac + b + d &= 0 \\ ad + bc &= 1 \\ bd &= 1. \end{aligned}$$

Como $bd = 1$, ya sea $b = d = 1$ o $b = d = -1$. En cualquier caso $b = d$ y así

$$ad + bc = b(a + c) = 1.$$

Como $a + c = -2$, sabemos que $-2b = 1$. Esto es imposible pues b es un entero. Por lo tanto, $p(x)$ es irreducible sobre $\mathbb{Q}$.

Teorema 17.17 (Criterio de Eisenstein)**.** *Sea p un número primo y supongamos que*

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x].$$

Si $p \mid a_i$ for $i = 0, 1, \ldots, n-1$, pero $p \not| a_n$ y $p^2 \not| a_0$, entonces $f(x)$ es irreducible sobre $\mathbb{Q}$.

DEMOSTRACIÓN. Por el Lema de Gauss, solo necesitamos demostrar que $f(x)$ no se factoriza como producto de polinomios de grado menor en $\mathbb{Z}[x]$. Supongamos que

$$f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$$

es una factorización en $\mathbb{Z}[x]$, con b_r y c_s ndistinto de cero y $r, s < n$. Como p^2 no divide a $a_0 = b_0 c_0$, ya sea b_0 o c_0 no es divisible por p. Supongamos que $p \not| b_0$ y $p \mid c_0$. Como $p \not| a_n$ y $a_n = b_r c_s$, ni b_r ni c_s es divisible por p. Sea m el menor valor de k tal que $p \not| c_k$. Entonces

$$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + b_m c_0$$

no es divisible por p, como cada término del lado derecho de la ecuación es divisible por p excepto $b_0 c_m$. Por lo tanto, $m = n$ pues a_i es divisible por p para $m < n$. Luego, $f(x)$ no puede ser factorizado como producto de polinomios de grado menor y por lo tanto es irreducible. □

Ejemplo 17.18. El polinomio

$$f(x) = 16x^5 - 9x^4 + 3x^2 + 6x - 21$$

es irreducible sobre $\mathbb{Q}$ por el Criterio de Eisenstein con $p = 3$.

El Criterio de Eisenstein es más útil para construir polinomios irreducibles de cierto grado sobre $\mathbb{Q}$ que para determinar la irreducibilidad de un polinomio arbitrario en $\mathbb{Q}[x]$: dado cualquier polinomio, no es muy probable que podamos aplicar el Criterio de Eisenstein. La importancia del Teorema 17.17 es que ahora tenemos una herramienta sencilla para generar polinomios irreducibles de cualquier grado.

Ideales en $F[x]$

Sea F un cuerpo. Recuerde que un ideal principal en $F[x]$ es un ideal $\langle p(x) \rangle$ generado por algún polinomio $p(x)$; es decir,

$$\langle p(x) \rangle = \{p(x)q(x) : q(x) \in F[x]\}.$$

Ejemplo 17.19. El polinomio x^2 en $F[x]$ genera el ideal $\langle x^2 \rangle$ que consiste de todos los polinomios que no tienen término constante ni de grado 1.

Teorema 17.20. *Si F es un cuerpo, entonces todo ideal en $F[x]$ es un ideal principal.*

DEMOSTRACIÓN. Sea I un ideal de $F[x]$. Si I es el ideal cero, no hay nada que demostrar. Supongamos que I es un ideal no trivial en $F[x]$, y sea $p(x) \in I$ un elemento distinto de cero de grado minimal. Si $\operatorname{gr} p(x) = 0$, entonces $p(x)$ es una constante no nula y 1 está en I. Como 1 genera todo $F[x]$, $\langle 1 \rangle = I = F[x]$ y I es un ideal principal.

Ahora supongamos que $\operatorname{gr} p(x) \geq 1$ y sea $f(x)$ cualquier elemento en I. Por el algoritmo de división existen $q(x)$ y $r(x)$ en $F[x]$ tales que $f(x) = p(x)q(x) + r(x)$ y $\operatorname{gr} r(x) < \operatorname{gr} p(x)$. Como $f(x), p(x) \in I$ eI es un ideal, $r(x) = f(x) - p(x)q(x)$ también está en I. Pero, como escogimos $p(x)$ de grado minimal, $r(x)$ debe ser el polinomio cero. Como podemos escribir cualquier elemento $f(x)$ en I como $p(x)q(x)$ para algún $q(x) \in F[x]$, tenemos que $I = \langle p(x) \rangle$. □

Ejemplo 17.21. No todo ideal en el anillo $F[x, y]$ es un ideal principal. Consideremos el ideal de $F[x, y]$ generado por los polinomios x e y. Este es el ideal de $F[x, y]$ que consiste de todos los polinomios que no tienen término constante. Como tanto x como y están en el ideal, ningún polinomio puede pos si solo generar todo el ideal.

Teorema 17.22. *Let F be a field and suppose that $p(x) \in F[x]$. Then the ideal generated by $p(x)$ is maximal if and only if $p(x)$ is irreducible.*

Demostración. Supongamos que $p(x)$ genera un ideal maximal de $F[x]$. Entonces $\langle p(x)\rangle$ es también un ideal primo de $F[x]$. Como un ideal maximal debe estar propiamente contenido en $F[x]$, $p(x)$ no puede ser un polinoio constante. Supongamos que $p(x)$ se factoriza en dos polinomios de grado menor, digamos $p(x) = f(x)g(x)$. Como $\langle p(x)\rangle$ es un ideal primo uno de estos factores, digamos $f(x)$, está en $\langle p(x)\rangle$ y por lo tanto es un múltiplo de $p(x)$. Pero esto implicaría que $\langle p(x)\rangle \subset \langle f(x)\rangle$, lo que es imposible pues $\langle p(x)\rangle$ es maximal.

Recíprocamente, supongamos que $p(x)$ es irreducible sobre $F[x]$. Sea I un ideal en $F[x]$ que contenga $\langle p(x)\rangle$. Por el Teorema 17.20, I es un ideal principal; luego, $I = \langle f(x)\rangle$ para algún $f(x) \in F[x]$. Como $p(x) \in I$, debe ser que $p(x) = f(x)g(x)$ para algún $g(x) \in F[x]$. Pero, $p(x)$ es irreducible; luego, ya sea $f(x)$ o $g(x)$ es un polinomio constante. Si $f(x)$ es constante, entonces $I = F[x]$ y estamos listos. Si $f(x)$ no es constante, entonces $f(x)$ es un múltiplo constante de $p(x)$ e $I = \langle p(x)\rangle$. Por lo tanto, no existen ideales propios de $F[x]$ que contengan propiamente a $\langle p(x)\rangle$. □

Sage Polynomial rings are very important for computational approaches to algebra, and so Sage makes it very easy to compute with polynomials, over rings, or over fields. And it is trivial to check if a polynomial is irreducible.

Nota Histórica

A lo largo de la historia, resolver ecuaciones polinomiales ha sido un problema desafiante. Los Babilonios sabían cómo resolver la ecuación $ax^2 + bx + c = 0$. Omar Khayyam (1048–1131) ideó métodos para resolver ecuaciones cúbicasmediante el uso de cnonstrucciones geométricas y secciones cónicas. La solución algebraica de la ecuación cúbica general $ax^3+bx^2+cx+d = 0$ no fue descubierta hasta el siglo XVI. Un matemático italiano, Luca Pacioli (ca. 1445–1509), escribió en *Summa de Arithmetica* que la solución a la cúbica era imposible. Esto fue tomado como un desafío por el resto de la comunidad matemática.

Scipione del Ferro (1465–1526), de la Universidad de Bologna, resolvió la "cúbica reducida,"

$$ax^3 + cx + d = 0.$$

Mantuvo en absoluto secreto esta solución. Esto puede parecer sorprendente hoy en día, cuando los matemáticos suelen estar muy interesados en publicar sus resultados, pero en durante el Renacimiento Italiano el secretismo era costumbre. Los cargos académicos no eran fáciles de mantener y dependían de ganar competencias públicas. Estos desafíos podían ser declarados en cualquier momento. En consecuencia cualquier nuevo descubrimiento de importancia era un arma valiosa en una competencia de ese tipo. Si un oponente presentaba una lista de problemas a resolver, del Ferro podía a su vez presentar una lista de cúbicas reducidas. Mantuvo el secreto de su descubrimiento durante toda su vida, comunicándoselo en el lecho de muerte a su estudiante Antonio Fior (ca. 1506–?).

Si bien Fior no era igual a su tutor, de inmediato lanzó un desafío a Niccolo Fontana (1499–1557). Fontana era conocido como Tartaglia (el Tartamudo).

Cuando joven había recibido un golpe de espada por parte de un soldado francés durante un ataque a su aldea. Sobrevivió la feroz herida, pero mantuvo el defecto de la dicción por el resto de su vida. Tartaglia envió a Fior una lista de 30 problemas matemáticos variados; Fior respondió enviando a Tartaglia una lista de 30 cúbicas reducidas. Tartaglia ya sea podría resolver todos los problemas de la lista o fallar absolutamente. Luego de un gran esfuerzo Tartaglia finalmente tovo éxito en resolver la cúbica reducida y venció a Fior, quien pasó al olvido.

En este momento otro matemático, Gerolamo Cardano (1501–1576), entra en el relato. Cardano le escribió a Tartaglia, rogándole que le diera la solución de la cúbica reducida. Tartaglia se rehusó a varias de sus súplicas, pero finalmente reveló la solución a Cardano después que este último jurara que no publicaría el secreto ni se lo transmitiría a nadie más. Usando lo que había aprendido de Tartaglia, Cardano finalmente resolvió la ecuación cúbica general

$$ax^3 + bx^2 + cx + d = 0.$$

Cardano compartió el secreto con su pupilo, Ludovico Ferrari (1522–1565), quien resolvió la ecuación general de cuarto grado,

$$ax^4 + bx^3 + cx^2 + dx + e = 0.$$

En 1543, Cardano y Ferrari esxaminaronlos trabajos de del Ferro y descubrieron que él también había resuelto la cúbica reducida. Cardano sintió que esto le absolvía de su compromiso con Tartaglia, de manera que publicó las soluciones en *Ars Magna* (1545), dándole crédito a del Ferro por resolver el caso especial de la cúbica. Esto resultó en una amarga disputa entre Cardano y Tartaglia, quien publicó la historia del juramento un año después.

17.4 Exercises

1. List all of the polynomials of degree 3 or less in $\mathbb{Z}_2[x]$.

2. Compute each of the following.

(a) $(5x^2 + 3x - 4) + (4x^2 - x + 9)$ in $\mathbb{Z}_{12}$

(b) $(5x^2 + 3x - 4)(4x^2 - x + 9)$ in $\mathbb{Z}_{12}$

(c) $(7x^3 + 3x^2 - x) + (6x^2 - 8x + 4)$ in $\mathbb{Z}_9$

(d) $(3x^2 + 2x - 4) + (4x^2 + 2)$ in $\mathbb{Z}_5$

(e) $(3x^2 + 2x - 4)(4x^2 + 2)$ in $\mathbb{Z}_5$

(f) $(5x^2 + 3x - 2)^2$ in $\mathbb{Z}_{12}$

3. Use the division algorithm to find $q(x)$ and $r(x)$ such that $a(x) = q(x)b(x) + r(x)$ with $\operatorname{gr} r(x) < \operatorname{gr} b(x)$ for each of the following pairs of polynomials.

(a) $a(x) = 5x^3 + 6x^2 - 3x + 4$ and $b(x) = x - 2$ in $\mathbb{Z}_7[x]$

(b) $a(x) = 6x^4 - 2x^3 + x^2 - 3x + 1$ and $b(x) = x^2 + x - 2$ in $\mathbb{Z}_7[x]$

(c) $a(x) = 4x^5 - x^3 + x^2 + 4$ and $b(x) = x^3 - 2$ in $\mathbb{Z}_5[x]$

(d) $a(x) = x^5 + x^3 - x^2 - x$ and $b(x) = x^3 + x$ in $\mathbb{Z}_2[x]$

4. Find the greatest common divisor of each of the following pairs $p(x)$ and $q(x)$ of polynomials. If $d(x) = \operatorname{mcd}(p(x), q(x))$, find two polynomials $a(x)$ and $b(x)$ such that $a(x)p(x) + b(x)q(x) = d(x)$.

(a) $p(x) = x^3 - 6x^2 + 14x - 15$ and $q(x) = x^3 - 8x^2 + 21x - 18$, where $p(x), q(x) \in \mathbb{Q}[x]$

(b) $p(x) = x^3 + x^2 - x + 1$ and $q(x) = x^3 + x - 1$, where $p(x), q(x) \in \mathbb{Z}_2[x]$

(c) $p(x) = x^3 + x^2 - 4x + 4$ and $q(x) = x^3 + 3x - 2$, where $p(x), q(x) \in \mathbb{Z}_5[x]$

(d) $p(x) = x^3 - 2x + 4$ and $q(x) = 4x^3 + x + 3$, where $p(x), q(x) \in \mathbb{Q}[x]$

5. Find all of the zeros for each of the following polynomials.

(a) $5x^3 + 4x^2 - x + 9$ in $\mathbb{Z}_{12}$

(b) $3x^3 - 4x^2 - x + 4$ in $\mathbb{Z}_5$

(c) $5x^4 + 2x^2 - 3$ in $\mathbb{Z}_7$

(d) $x^3 + x + 1$ in $\mathbb{Z}_2$

6. Find all of the units in $\mathbb{Z}[x]$.

7. Find a unit $p(x)$ in $\mathbb{Z}_4[x]$ such that $\operatorname{gr} p(x) > 1$.

8. Which of the following polynomials are irreducible over $\mathbb{Q}[x]$?

(a) $x^4 - 2x^3 + 2x^2 + x + 4$

(b) $x^4 - 5x^3 + 3x - 2$

(c) $3x^5 - 4x^3 - 6x^2 + 6$

(d) $5x^5 - 6x^4 - 3x^2 + 9x - 15$

9. Find all of the irreducible polynomials of degrees 2 and 3 in $\mathbb{Z}_2[x]$.

10. Give two different factorizations of $x^2 + x + 8$ in $\mathbb{Z}_{10}[x]$.

11. Prove or disprove: There exists a polynomial $p(x)$ in $\mathbb{Z}_6[x]$ of degree n with more than n distinct zeros.

12. If F is a field, show that $F[x_1, \ldots, x_n]$ is an integral domain.

13. Show that the division algorithm does not hold for $\mathbb{Z}[x]$. Why does it fail?

14. Prove or disprove: $x^p + a$ is irreducible for any $a \in \mathbb{Z}_p$, where p is prime.

15. Let $f(x)$ be irreducible in $F[x]$, where F is a field. If $f(x) \mid p(x)q(x)$, prove that either $f(x) \mid p(x)$ or $f(x) \mid q(x)$.

16. Suppose that R and S are isomorphic rings. Prove that $R[x] \cong S[x]$.

17. Let F be a field and $a \in F$. If $p(x) \in F[x]$, show that $p(a)$ is the remainder obtained when $p(x)$ is divided by $x - a$.

18. (The Rational Root Theorem) Let

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x],$$

where $a_n \neq 0$. Prove that if $p(r/s) = 0$, where $\operatorname{mcd}(r, s) = 1$, then $r \mid a_0$ and $s \mid a_n$.

19. Let $\mathbb{Q}^*$ be the multiplicative group of positive rational numbers. Prove that $\mathbb{Q}^*$ is isomorphic to $(\mathbb{Z}[x], +)$.

20. (Cyclotomic Polynomials) The polynomial

$$\Phi_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1$$

is called the ***cyclotomic polynomial.*** Show that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$ for any prime p.

21. If F is a field, show that there are infinitely many irreducible polynomials in $F[x]$.

22. Let R be a commutative ring with identity. Prove that multiplication is commutative in $R[x]$.

23. Let R be a commutative ring with identity. Prove that multiplication is distributive in $R[x]$.

24. Show that $x^p - x$ has p distinct zeros in $\mathbb{Z}_p$, for any prime p. Conclude that

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$

25. Let F be a field and $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be in $F[x]$. Define $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$ to be the ***derivative*** of $f(x)$.

(a) Prove that

$$(f+g)'(x) = f'(x) + g'(x).$$

Conclude that we can define a homomorphism of abelian groups $D : F[x] \to F[x]$ by $D(f(x)) = f'(x)$.

(b) Calculate the kernel of D if $\operatorname{char} F = 0$.

(c) Calculate the kernel of D if $\operatorname{char} F = p$.

(d) Prove that

$$(fg)'(x) = f'(x)g(x) + f(x)g'(x).$$

(e) Suppose that we can factor a polynomial $f(x) \in F[x]$ into linear factors, say

$$f(x) = a(x-a_1)(x-a_2)\cdots(x-a_n).$$

Prove that $f(x)$ has no repeated factors if and only if $f(x)$ and $f'(x)$ are relatively prime.

26. Let F be a field. Show that $F[x]$ is never a field.

27. Let R be an integral domain. Prove that $R[x_1, \ldots, x_n]$ is an integral domain.

28. Let R be a commutative ring with identity. Show that $R[x]$ has a subring R' isomorphic to R.

29. Let $p(x)$ and $q(x)$ be polynomials in $R[x]$, where R is a commutative ring with identity. Prove that $\operatorname{gr}(p(x) + q(x)) \leq \max(\operatorname{gr} p(x), \operatorname{gr} q(x))$.

17.5 Ejercicios Adicionales: Resolviendo las Ecuaciones Cúbica y Cuártica

1. Resuelva la ecuación cuadrática general

$$ax^2 + bx + c = 0$$

obteniendo

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

El ***discriminante*** de la ecuación cuadrática $\Delta = b^2 - 4ac$ determina la naturaleza de las soluciones de la ecuación. Si $\Delta > 0$, la ecuación tiene dos soluciones reales diferentes. Si $\Delta = 0$, la ecuación tiene una única solución real repetida. Si $\Delta < 0$, existen dos soluciones imaginarias diferentes.

2. Muestre que cualquier ecuación cúbica de la forma

$$x^3 + bx^2 + cx + d = 0$$

puede ser reducida a la forma $y^3+py+q = 0$ haciendo la sustitución $x = y-b/3$.

3. Demuestre que las raíces cúbicas de 1 están dadas por

$$\omega = \frac{-1 + i\sqrt{3}}{2}$$
$$\omega^2 = \frac{-1 - i\sqrt{3}}{2}$$
$$\omega^3 = 1.$$

4. Haga la sustitución

$$y = z - \frac{p}{3z}$$

para y en la ecuación $y^3 + py + q = 0$ ay obtenga dos soluciones A y B para z^3.

5. Muestre que el producto de las soluciones obtenidas en (4) es $-p^3/27$, deduciendo que $\sqrt[3]{AB} = -p/3$.

6. Demuestre que las posibles soluciones para z en (4) están dadas por

$$\sqrt[3]{A}, \quad \omega\sqrt[3]{A}, \quad \omega^2\sqrt[3]{A}, \quad \sqrt[3]{B}, \quad \omega\sqrt[3]{B}, \quad \omega^2\sqrt[3]{B}$$

y use este resultado para mostrar que las tres posibles soluciones para y son

$$\omega^i \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \omega^{2i} \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}},$$

donde $i = 0, 1, 2$.

7. El ***discriminante*** de la ecuación cúbica es

$$\Delta = \frac{p^3}{27} + \frac{q^2}{4}.$$

Muestre que $y^3 + py + q = 0$

(a) tiene tres raíces reales, de las que al menos dos son iguales, si $\Delta = 0$.

(b) tiene una raíz real y dos raíces complejas no reales conjugadas si $\Delta > 0$.

(c) tiene tres raíces reales distintas si $\Delta < 0$.

8. Resueva las siguientes ecuaciones cúbicas.

(a) $x^3 - 4x^2 + 11x + 30 = 0$

(b) $x^3 - 3x + 5 = 0$

(c) $x^3 - 3x + 2 = 0$

(d) $x^3 + x + 3 = 0$

9. Muestre que la ecuación cuártica general

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

se reduce a

$$y^4 + py^2 + qy + r = 0$$

busando la sustitución $x = y - a/4$.

10. Muestre que

$$\left(y^2 + \frac{1}{2}z\right)^2 = (z-p)y^2 - qy + \left(\frac{1}{4}z^2 - r\right).$$

11. Muestre que el lado derecho del Ejercicio 17.5.10 puede ser puesto en la forma $(my+k)^2$ si y solo si

$$q^2 - 4(z-p)\left(\frac{1}{4}z^2 - r\right) = 0.$$

12. Del Ejercicio 17.5.11 obtenga la ***ecuación cúbica resolvente***

$$z^3 - pz^2 - 4rz + (4pr - q^2) = 0.$$

Resolviendo la resolvente cúbica, ponga la ecuación encontrada en el Ejercicio 17.5.10 en la forma

$$\left(y^2 + \frac{1}{2}z\right)^2 = (my+k)^2$$

para obtener la solución de la ecuación cuártica.

13. Use este método para resolver las siguientes ecuaciones cuárticas.

(a) $x^4 - x^2 - 3x + 2 = 0$

(b) $x^4 + x^3 - 7x^2 - x + 6 = 0$

(c) $x^4 - 2x^2 + 4x - 3 = 0$

(d) $x^4 - 4x^3 + 3x^2 - 5x + 2 = 0$

17.6 Sage

Sage es particularmente bueno para construir, analizar y manipular anillos de polinomios. Hemos visto algo de esto en el capítulo anterior. Comencemos creando tres anillo de polinomios y comprobemos algunas de sus propiedades básicas. Existen difierentes formas de construir anillos de polinomios, pero la sintaxis usada acá es la más directa.

Anillos de Polinomios y sus Elementos

```
R.<x> = Integers(8)[]; R
```

```
Univariate Polynomial Ring in x over Ring of integers modulo 8
```

```
S.<y> = ZZ[]; S
```

```
Univariate Polynomial Ring in y over Integer Ring
```

```
T.<z> = QQ[]; T
```

```
Univariate Polynomial Ring in z over Rational Field
```

Las propiedades básicas de los anillos se pueden usar en estos ejemplos.

```
R.is_finite()
```

```
False
```

```
R.is_integral_domain()
```

```
False
```

```
S.is_integral_domain()
```

```
True
```

```
T.is_field()
```

```
False
```

```
R.characteristic()
```

```
8
```

```
T.characteristic()
```

```
0
```

Con la construcción y la sintaxis de arriba, las variables se pueden usar para crear elementos del anillo de polinomios sin coercionarlos explícitamente (aunque tenemos que tener cuidado con los polinomios constantes).

```
y in S
```

```
True
```

```
x in S
```

```
False
```

```
q = (3/2) + (5/4)*z^2
q in T
```

```
True
```

```
3 in S
```

```
True
```

```
r = 3
r.parent()
```

```
Integer Ring
```

```
s = 3*y^0
s.parent()
```

```
Univariate Polynomial Ring in y over Integer Ring
```

Los polinomios pueden ser evaluados como si fueran funciones, de manera que podemos imitar el homomorfismo de evaluación.

```
p = 3 + 5*x + 2*x^2
p.parent()
```

```
Univariate Polynomial Ring in x over Ring of integers modulo 8
```

```
p(1)
```

```
2
```

```
[p(t) for t in Integers(8)]
```

```
[3, 2, 5, 4, 7, 6, 1, 0]
```

Notemos que `p` es un polinomio de grado dos, sin embargo podemos verificar a fuerza-bruta que solo tiene una raíz, contrario a nuestra expectativa usual. Puede ser incluso más inusual.

```
q = 4*x^2+4*x
[q(t) for t in Integers(8)]
```

```
[0, 0, 0, 0, 0, 0, 0, 0]
```

Sage puede crear y manipular anillos de polinomios en más de una variable, pero no tendremos mayores oportunidades de analizar esa funcionalidad en este curso.

```
M.<s, t> = QQ[]; M
```

```
Multivariate Polynomial Ring in s, t over Rational Field
```

Polinomios Irreducibles

Si un polinomio se factoriza o no, tomando en consideración el anillo usado para sus coeficientes, es una pregunta importante en este capítulo y en muchos de los que siguen. Sage es capaz de factorizar, y de determinar irreducibilidad, sobre los enteros, los racionales, y los cuerpos finitos.

Primero, sobre los racionales.

```
R.<x> = QQ[]
p = 1/4*x^4 - x^3 + x^2 - x - 1/2
p.is_irreducible()
```

```
True
```

```
p.factor()
```

```
(1/4) * (x^4 - 4*x^3 + 4*x^2 - 4*x - 2)
```

```
q = 2*x^5 + 5/2*x^4 + 3/4*x^3 - 25/24*x^2 - x - 1/2
q.is_irreducible()
```

```
False
```

```
q.factor()
```

```
(2) * (x^2 + 3/2*x + 3/4) * (x^3 - 1/4*x^2 - 1/3)
```

Factorizar sobre los enteros no es realmente diferente a hacerlo sobre los racionales. Esto es lo que nos dice el Teorema 17.14 — encontrar una factorización sobre los enteros puede ser convertido en encontrar una factorización sobre los racionales. Así es en Sage, hay poca diferencia entre trabajar sobre los racionales y sobre los enteros. Es un poco diferente cuando trabajamos sobre un cuerpo finito. Un comentario viene más adelante.

```
F.<a> = FiniteField(5^2)
S.<y> = F[]
p = 2*y^5 + 2*y^4 + 4*y^3 + 2*y^2 + 3*y + 1
p.is_irreducible()
```

```
True
```

```
p.factor()
```

```
(2) * (y^5 + y^4 + 2*y^3 + y^2 + 4*y + 3)
```

```
q = 3*y^4+2*y^3-y+4; q.factor()
```

```
(3) * (y^2 + (a + 4)*y + 2*a + 3) * (y^2 + 4*a*y + 3*a)
```

```
r = y^4+2*y^3+3*y^2+4; r.factor()
```

```
(y + 4) * (y^3 + 3*y^2 + y + 1)
```

```
s = 3*y^4+2*y^3-y+3; s.factor()
```

```
(3) * (y + 1) * (y + 3) * (y + 2*a + 4) * (y + 3*a + 1)
```

Para verificar estas factorizaciones, debemos calcular en el cuerpo finito, `F`, por lo que necesitamos saber como se comporta el símbolo `a` behaves. Este símbolo corresponde a una raíz de un polinomio de grado 2 sobre los enteros mód 5, que podemos obtener con el método `.modulus()`.

```
F.modulus()
```

```
x^2 + 4*x + 2
```

Así $a^2+4a+2=0$, o $a^2=-4a-3=a+2$. Así, al verificar las factorizaciones, cada vez que aparezca a^2 lo podemos reemplazar por $a+2$. Notemos que por el Corolario 17.8 podríamos encontrar el factor lineal de `r`, y los cuatro factores lineales de `s`, mediante una búsqueda a la bruta de sus raíces. Esto es realizable dado que el cuerpo es finito.

```
[t for t in F if r(t)==0]
```

```
[1]
```

```
[t for t in F if s(t)==0]
```

```
[2, 3*a + 1, 4, 2*a + 4]
```

Pero, `q` se factoriza en dos polinomios de grado 2, de manera que ninguna búsque de raíces nos permitirá descubrir estos factores.

Por el criterio de Eisenstein, podemos crear polinomios irreducibles, como en el Ejemplo 17.18.

```
W.<w> = QQ[]
p = 16*w^5 - 9*w^4 +3*w^2 + 6*w -21
p.is_irreducible()
```

```
True
```

Sobre el cuerpo $\mathbb{Z}_p$, los polinomios de Conway son elecciones canónicas para un polinomio de grado $n$irreducible sobre $\mathbb{Z}_p$. Vea los ejercicios para aprender más sobre estos polinomios.

Polinomios sobre Cuerpos

Si F es un cuerpo, entonces todo ideal de $F[x]$ es principal (Teorema 17.20). Nada nos impide darle a Sage dos (o más) generadores para construir un ideal, pero Sage determinará un elemento para usarlo en la descripción del ideal como ideal principal.

```
W.<w> = QQ[]
r = -w^5 + 5*w^4 - 4*w^3 + 14*w^2 - 67*w + 17
s = 3*w^5 - 14*w^4 + 12*w^3 - 6*w^2 + w
S = W.ideal(r, s)
S
```

```
Principal ideal (w^2 - 4*w + 1) of
Univariate Polynomial Ring in w over Rational Field
```

```
(w^2)*r + (3*w-6)*s in S
```

```
True
```

El Teorema 17.22 es el hecho clave que nos permite construir cuerpos finitos fácilmente. Acá hay una construcción de un cuero finito de orden $7^5 = 16\,807$. Todo lo que necesitamos es un polinomio de grado 5 que sea irreducible sobre $\mathbb{Z}_7$.

```
F = Integers(7)
R.<x> = F[]
p = x^5+ x + 4
p.is_irreducible()
```

```
True
```

```
id = R.ideal(p)
Q = R.quotient(id); Q
```

```
Univariate Quotient Polynomial Ring in xbar over
Ring of integers modulo 7 with modulus x^5 + x + 4
```

```
Q.is_field()
```

```
True
```

```
Q.order() == 7^5
```

```
True
```

El símbolo `xbar` es un generador del cuerpo, pero en este momento no es accesible. `xbar` es la clase $x + \langle x^5 + x + 4\rangle$. Una mejor construcción incluiría la especificación de este generador.

```
Q.gen(0)
```

```
xbar
```

```
Q.<t> = R.quotient(id); Q
```

```
Univariate Quotient Polynomial Ring in t over
Ring of integers modulo 7 with modulus x^5 + x + 4
```

```
t^5 + t + 4
```

```
0
```

```
t^5 == -(t+4)
```

```
True
```

```
t^5
```

```
6*t + 3
```

```
(3*t^3 + t + 5)*(t^2 + 4*t + 2)
```

```
5*t^4 + 2*t^2 + 5*t + 5
```

```
a = 3*t^4 - 6*t^3 + 3*t^2 + 5*t + 2
ainv = a^-1; ainv
```

```
6*t^4 + 5*t^2 + 4
```

```
a*ainv
```

```
1
```

17.7 Ejercicios en Sage

1. Consideremos el polinomio $x^3 - 3x + 4$. Calcule la máxima factorización de este polinomio sobre cada uno de los siguientes cuerpos: (a) el cuerpo finito $\mathbb{Z}_5$, (b) el cuerpo finito de orden 125, (c) $\mathbb{Q}$, (d) $\mathbb{R}$ y (e) $\mathbb{C}$. Para hacer esto, construya el anillo de polinomio apropiado, construya el polinomio en este anillo y use el método `.factor()`.

2. "Los polinomios de Conway" son polinomios irreducibles sobre $\mathbb{Z}_p$ que Sage (y otros programas) usa para construir ideales maximales en anillos de polinomio, y por ende anillos cociente que son cuerpos. A grosso modo, son elecciones canónicaspara cada grado y para cada primo. El comando `conway_polynomial(p, n)` entrega un polinomio irreducible de grado n sobre $\mathbb{Z}_p$.
Ejecute el comando `conway_polynomial(5, 4)` para obtener un polinomio presuntamente irreducible de grado 4 sobre $\mathbb{Z}_5$: $p = x^4 + 4x^2 + 4x + 2$. Construya el anillo de polinomios apropiado (i.e., en la indeterminada x) y verifique que `p` realmente es un elemento de ese anillo de polinomios.
Primero verifique que p no tiene factores lineales. La única posibilidad que queda es que `p` se factorice como producto de dos polinomios cuadráticos sobre

$\mathbb{Z}_5$. Use una lista con *tres* `for` para crear *todos* los posibles polinomios cuadráticos sobre $\mathbb{Z}_5$. Ahora use esta lista para crear todos los posibles productos de dos polinomios cuadráticos y compruebe si `p` está en esta lista.
Puede encontrar más información sobre los polinomios de Conway en el sitio de Frank Lübeck.

3. Construya un cuerpo finito de orden 729 como cociente de un anillo de polinomios por un ideal principal generado con un polinomio de Conway.

4. Defina los polinomios $p = x^3 + 2x^2 + 2x + 4$ y $q = x^4 + 2x^2$ como polinomios con coeficientes enteros. Calcule `gcd(p, q)` y verifique que el resultado divide tanto a `p` como a `q` (simlemente forme la fracción en Sage y vea que se simplifica completamente, o use el método `.quo_rem()`).
La Proposición 17.10 dice que existen polinomio $r(x)$ y $s(x)$ tales que el máximo común divisor es $r(x)p(x) + s(x)q(x)$, *si los coeficientes están en un cuerpo*. Como acá tenemos dos polinomios sobre los enteros, investigue los resultados entregados por Sage para el mcd extendido, `xgcd(p, q)`. En particular, muestre que la primera componente del resultado es un múltiplo del mcd. Después verifique la propiedad de "combinación lineal".

5. Para un anillo de polinomios sobre un cuerpo, todo ideal es principal. Comience con el anillo de polinomios sobre los racionales. Experimente construyendo ideales con dos generadores y vea que Sage los convierte en ideales principales con un solo generador. (Puede obtener este generador con el método `.gen()` del ideal.) ¿Puede explicar como se calcula este generador?

18

Dominios Integrales

Uno de los anillos más importantes que estudiamos es el de los enteros. Fue nuestro primer ejemplo de una estructura algebraica: el primer anillo de polinomio que examinamos fue $\mathbb{Z}[x]$. También sabemos que los enteros están contenidos naturalmente en el cuerpo de los números racionales, $\mathbb{Q}$. El anillo de los enteros es el modelo para todos los dominios integrales (también se llaman dominios enteros). En este capítulo estudiaremos dominios integrales en general, contestando preguntas sobre su estructura de ideales, anillos de polinomios sobre dominios integrales y si es posible incrustar un dominio integral en un cuerpo.

18.1 Cuerpos de Fracciones

Todo cuerpo es un dominio integral; pero, existen muchos dominios integrales que no son cuerpos. Por ejemplo, los enteros $\mathbb{Z}$ forman un dominio integral pero no un cuerpo. Una pregunta que surge naturalmente es como asociar un dominio integral con un cuerpo. Existe una forma natural de construir los racionales $\mathbb{Q}$ a partir de los enteros: los racionales pueden ser representados como cocientes de dos enteros. Los números racionales por cierto forman un cuerpo. De hecho, se puede demostrar que los racionales forman el cuerpo más pequeño que contiene a los enteros. Dado un dominio integral D, nuestra pregunta ahora es cómo construir un menor cuerpo F que contenga a D. Haremos esto de la misma forma en que construimos los racionales a partir de los enteros.

Un elemento $p/q \in \mathbb{Q}$ es el cociente de dos enteros p y q; sin embargo, diferentes pares de enteros pueden representar el mismo número racional. Por ejemplo, $1/2 = 2/4 = 3/6$. Sabemos que

$$\frac{a}{b} = \frac{c}{d}$$

si y solo si $ad = bc$. Una manera más formal de considerar este problema es examinando las fracciones en términos de relaciones de equivalencia. Podemos pensar los elementos en $\mathbb{Q}$ como pares ordenados en $\mathbb{Z} \times \mathbb{Z}$. Un cociente p/q puede ser escrito como (p, q). Por ejemplo, $(3, 7)$ representaría la fracción $3/7$. Pero, surgen problemas si consideramos todos los pares posibles en $\mathbb{Z} \times \mathbb{Z}$. No existe la fracción $5/0$ que corresponda al par $(5, 0)$. Además, los pares $(3, 6)$ y $(2, 4)$ ambos representan la fracción $1/2$. El primer problema lo resolvemos de forma sencilla si exigimos que la segunda coordenada sea dstinta de cero. El segundo problema se resuelve considerando dos pares (a, b) y (c, d) como equivalentes si y solo si $ad = bc$.

Si usamos la idea de pares ordenados en lugar de fracciones, entonces podemos estudiar dominios integrales en general. Sea D un dominio integral

cualquiera y sea

$$S = \{(a, b) : a, b \in D \text{ and } b \neq 0\}.$$

Definimos una relación en S por $(a, b) \sim (c, d)$ si y solo si $ad = bc$.

Lema 18.1. *La relación $\sim$ entre elementos de S es una relación de equivalencia.*

DEMOSTRACIÓN. Como D es conmutativo, $ab = ba$; luego, $\sim$ es refleja en D. Ahora supongamos que $(a, b) \sim (c, d)$. Entonces $ad = bc$ y $cb = da$. Por lo tanto, $(c, d) \sim (a, b)$ y la relación es simétrica. Finalmente, para mostrar que la relación es transitiva, sean $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$. En este caso $ad = bc$ y $cf = de$. Multiplicando ambos lados de $ad = bc$ por f resulta

$$afd = adf = bcf = bde = bed.$$

Como D es un dominio integral, podemos deducir que $af = be$ y $(a, b) \sim (e, f)$. □

Denotaremos el conjunto de clases de equivalencia en S por F_D. Ahora debemos definir las operaciones de adición y multiplicación en F_D. Recuerde cómo se suman y multiplican las fracciones en $\mathbb{Q}$:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd};$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Parece razonable definir las operaciones de adición y multiplicación en F_D de manera similar. Si denotamos la clase de equivalencia de $(a, b) \in S$ por $[a, b]$, esto nos lleva a definir las operaciones de adición y multiplicación en F_D como

$$[a, b] + [c, d] = [ad + bc, bd]$$

y

$$[a, b] \cdot [c, d] = [ac, bd],$$

respectivamente. El próximos lema demuestra que estas operaciones son independientes de la elección de representantes para cada clase de equivalencia.

Lema 18.2. *Las operaciones de adición y multiplicación en F_D están bien-definidas.*

DEMOSTRACIÓN. Demostraremos que la operación de adición está bien-definida. La demostración de que la multiplicación está bien-definida la dejaremos como ejercicio. Sean $[a_1, b_1] = [a_2, b_2]$ y $[c_1, d_1] = [c_2, d_2]$. Debemos mostrar que

$$[a_1d_1 + b_1c_1, b_1d_1] = [a_2d_2 + b_2c_2, b_2d_2]$$

o, equivalentemente, que

$$(a_1d_1 + b_1c_1)(b_2d_2) = (b_1d_1)(a_2d_2 + b_2c_2).$$

Como $[a_1, b_1] = [a_2, b_2]$ and $[c_1, d_1] = [c_2, d_2]$, sabemos que $a_1b_2 = b_1a_2$ y $c_1d_2 = d_1c_2$. Por lo tanto,

$$\begin{aligned}(a_1d_1 + b_1c_1)(b_2d_2) &= a_1d_1b_2d_2 + b_1c_1b_2d_2 \\ &= a_1b_2d_1d_2 + b_1b_2c_1d_2 \\ &= b_1a_2d_1d_2 + b_1b_2d_1c_2 \\ &= (b_1d_1)(a_2d_2 + b_2c_2).\end{aligned}$$

□

Lema 18.3. *El conjunto F_D de clases de equivalencia de S, bajo la relación de equivalencia $\sim$, junto a las operaciones de adición y multiplicación definidas por*

$$[a,b]+[c,d]=[ad+bc,bd]$$
$$[a,b]\cdot[c,d]=[ac,bd],$$

es un cuerpo.

Demostración. Las identidades aditiva y multiplicativa son $[0,1]$ y $[1,1]$, respectivamente. Para mostrar que $[0,1]$ es la identidad aditiva (o neutro aditivo), observemos que

$$[a,b]+[0,1]=[a1+b0,b1]=[a,b].$$

Es fácil mostrar que $[1,1]$ es la identidad multiplicativa. Sea $[a,b]\in F_D$ tal que $a\neq 0$. Entonces $[b,a]$ también está en F_D y $[a,b]\cdot[b,a]=[1,1]$; luego, $[b,a]$ es el inverso multiplicativo para $[a,b]$. Similarmente, $[-a,b]$ es el inverso aditivo de $[a,b]$. Dejamos como ejercicios la verificación de la asociatividad y la conmutatividad en F_D. También dejamos al lector la demostración de que F_D es un grupo abeliano con la operación de adición.

Falta demostrar que se cumple la propiedad distributiva en F_D; pero,

$$\begin{aligned}[a,b][e,f]+[c,d][e,f]&=[ae,bf]+[ce,df]\\&=[aedf+bfce,bdf^2]\\&=[aed+bce,bdf]\\&=[ade+bce,bdf]\\&=([a,b]+[c,d])[e,f]\end{aligned}$$

y el lema está demostrado. □

El cuerpo F_D en el Lema 18.3 se llama ***cuerpo de fracciones*** o ***cuerpo de cocientes*** del dominio integral D.

Teorema 18.4. *Sea D un dominio integral. Entonces D puede ser incrustado en un cuerpo de fracciones F_D, donde cualquier elemento en F_D se puede expresar como el cociente de dos elementos en D. Además, el cuerpo de fracciones F_D es único en el sentido de que si E es cualquier cuerpo que contiene D, entonces existe una función $\psi: F_D\to E$ que da lugar a un somorfismo con un subcuerpo de E tal que $\psi(a)=a$ para todos los elementos $a\in D$, donde identificamos a cn su imagen en F_D.*

Demostración. Primero demostraremos que D puede ser incrustado en el cuerpo F_D. Definamos una función $\phi: D\to F_D$ como $\phi(a)=[a,1]$. Entonces para a y b en D,

$$\phi(a+b)=[a+b,1]=[a,1]+[b,1]=\phi(a)+\phi(b)$$

y

$$\phi(ab)=[ab,1]=[a,1][b,1]=\phi(a)\phi(b);$$

es decir, ϕ es un homomorfismo. Para mostrar que ϕ es 1-1, supongamos que $\phi(a)=\phi(b)$. Entonces $[a,1]=[b,1]$, y $a=a1=1b=b$. Finalmente, cualquier elemento de F_D puede ser expresadocomo el cociente de dos elementos en D, pues

$$\phi(a)[\phi(b)]^{-1}=[a,1][b,1]^{-1}=[a,1]\cdot[1,b]=[a,b].$$

Ahora sea E un cuerpo que contenga a D y definamos na función $\psi : F_D \to E$ por $\psi([a,b]) = ab^{-1}$. Para mostrar que ψ está bien-definida, sean $[a_1,b_1] = [a_2,b_2]$. Entonces $a_1b_2 = b_1a_2$. Por lo tanto, $a_1b_1^{-1} = a_2b_2^{-1}$ y $\psi([a_1,b_1]) = \psi([a_2,b_2])$.

Si $[a,b]$ y $[c,d]$ están en F_D, entonces

$$\begin{aligned}\psi([a,b]+[c,d]) &= \psi([ad+bc,bd]) \\ &= (ad+bc)(bd)^{-1} \\ &= ab^{-1}+cd^{-1} \\ &= \psi([a,b])+\psi([c,d])\end{aligned}$$

y

$$\begin{aligned}\psi([a,b]\cdot[c,d]) &= \psi([ac,bd]) \\ &= (ac)(bd)^{-1} \\ &= ab^{-1}cd^{-1} \\ &= \psi([a,b])\psi([c,d]).\end{aligned}$$

Por lo tanto, ψ es un homomorfismo.

Para completar la demostración, debemos mostrar que ψ es 1-1. Supongamos que $\psi([a,b]) = ab^{-1} = 0$. Entonces $a = 0b = 0$ y $[a,b] = [0,b]$. Por lo tanto, el núcleo de ψ contiene solo el elemento cero $[0,b]$ en F_D, y ψ es inyectiva. □

Ejemplo 18.5. Como $\mathbb{Q}$ es un cuerpo, $\mathbb{Q}[x]$ es un dominio integral. El cuerpo de fracciones de $\mathbb{Q}[x]$ es el conjunto de todas las expresiones racionales $p(x)/q(x)$, donde $p(x)$ y $q(x)$ son polinomios sobre los racionales y $q(x)$ no es el polinomio cero. Denotaremos este cuerpo por $\mathbb{Q}(x)$.

Dejaremos como ejercicios las demostraciones de los siguientes corolarios al Teorema 18.4.

Corolario 18.6. *Sea F un cuerpo de característica cero. Entonces F contiene un subcuerpo isomorfo a $\mathbb{Q}$.*

Corolario 18.7. *Sea F un cuerpo de característica p. Entonces F contiene un subcuerpo isomorfo a $\mathbb{Z}_p$.*

18.2 Factorización en un Dominio Integral

Los componentes esenciales para la factorización de enteros son los números primos. Si F es un cuerpo, los polinomios irreducibles en $F[x]$ tienen un rol muy similar al que tienen los números primos en el anillo de los enteros. Dado un dominio integral arbitrario, esto nos lleva a las siguientes definiciones.

Sea R un anillo conmutativo con identidad, y sean a y b elementos en R. Decimos que a ***divide a*** b, y escribimos $a \mid b$, si existe un elemento $c \in R$ tal que $b = ac$. Una ***unidad*** en R es un elemento que tiene inverso multiplicativo. Dos elementos a y b en R se dicen ***asociados*** si existe una unidad u en R tal que $a = ub$.

Sea D un dominio integral. Un elemento distinto de cero $p \in D$ que no sea una unidad se dice ***irreducible*** si cada vez que $p = ab$, ya sea a o b es una unidad. Además, p es ***primo*** si cada vez que $p \mid ab$ ya sea $p \mid a$ o $p \mid b$.

Ejemplo 18.8. Es importante notar que los elementos primos y los elementos irreducibles no siempre coinciden. Sea R el subanillo (con identidad) de $\mathbb{Q}[x, y]$ generado por x^2, y^2, y xy. Cada uno de estos elementos es irreducible en R; pero, xy no es primo, pues xy divide a x^2y^2 pero no divide a x^2 ni a y^2.

El Teorema Fundamental de la Aritméticas establece que cada entero $n > 1$ puede ser factorizado como pruducto de números primos $p_1 \cdots p_k$, donde los p_i no son cecesariamente distintos. También sabemos que tal factorización es única salvo el orden en que aparecen los p_i. Podemos fácilmente extender este resultado a todos los enteros. La pregunta surge sobre si tales factorizaciones son posibles en otros anillos. Generalizando esta definición, diremos que un dominio integral D es un ***dominio de factorización única***, o **DFU**, si D satisface los siguientes criterios.

1. Sea $a \in D$ tal que $a \neq 0$ y a no es una unidad. Entonces a puede ser escrito como producto de elementos irreducibles en D.

2. Sea $a = p_1 \cdots p_r = q_1 \cdots q_s$, donde los p_i y los q_i son irreducibles. Entonces $r = s$ y existe $\pi \in S_r$ tal que p_i y $q_{\pi(j)}$ son asociados para $j = 1, \ldots, r$.

Ejemplo 18.9. El anillo de los enteros es un dominio de factorización única por el Teorema Fundamental de la Aritmética.

Ejemplo 18.10. No todo dominio integral es un dominio de factorización única. El subanillo $\mathbb{Z}[\sqrt{3}\,i] = \{a + b\sqrt{3}\,i\}$ de los números complejos es un dominio integral (Ejercicio 16.6.12, Capítulo 16). Sea $z = a + b\sqrt{3}\,i$ y defina $\nu : \mathbb{Z}[\sqrt{3}\,i] \to \mathbb{N} \cup \{0\}$ por $\nu(z) = |z|^2 = a^2 + 3b^2$. Es claro que $\nu(z) \geq 0$ con igualdad cuando $z = 0$. Además, de nuestro conocimiento de números complejos sabemos que $\nu(zw) = \nu(z)\nu(w)$. Es fácil mostrar que si $\nu(z) = 1$, entonces z es una unidad, y que las únicas unidades de $\mathbb{Z}[\sqrt{3}\,i]$ son 1 y -1.

Afirmamos que 4 tiene dos factorizaciones distintas en elementos irreducibles:

$$4 = 2 \cdot 2 = (1 - \sqrt{3}\,i)(1 + \sqrt{3}\,i).$$

Debemos demostrar que cada uno de estos factores es un elemento irreducible en $\mathbb{Z}[\sqrt{3}\,i]$. Si 2 no fuera irreducible, entonces $2 = zw$ para ciertos z, w en $\mathbb{Z}[\sqrt{3}\,i]$ con $\nu(z) = \nu(w) = 2$. Pero, no existe ningún elemento z en $\mathbb{Z}[\sqrt{3}\,i]$ tal que $\nu(z) = 2$ pues la ecuación $a^2 + 3b^2 = 2$ no tiene solución entera. Por lo tanto, 2 es irreducible. Un argumento similar muestra que tanto $1 - \sqrt{3}\,i$ como $1 + \sqrt{3}\,i$ son irreducibles. Como 2 no es un múltiplo de una unidad por $1 - \sqrt{3}\,i$ o $1 + \sqrt{3}\,i$, vemos que 4 tiene al menos dos factorizaciones diferentes en elementos irreducibless.

Dominios de Ideales Principales

Sea R un anillo conmutativo con identidad. Recordemos que un ideal principal generado por $a \in R$ es un ideal de la forma $\langle a \rangle = \{ra : r \in R\}$. Un dominio integral en el que todos los ideales son principales se llama ***dominio de ideales principales***, o **DIP**.

Lema 18.11. *Sea D un dominio integral y sean $a, b \in D$. Entonces*

1. *$a \mid b$ si y solo si $\langle b \rangle \subset \langle a \rangle$.*

2. *a y b son asociados si y solo si $\langle b \rangle = \langle a \rangle$.*

3. *a es una unidad en D si y solo si $\langle a \rangle = D$.*

DEMOSTRACIÓN. (1) Supongamos que $a \mid b$. Entonces $b = ax$ para algún $x \in D$. Luego, para cada r en D, $br = (ax)r = a(xr)$ y $\langle b\rangle \subset \langle a\rangle$. Recíprocamente, supongamos que $\langle b\rangle \subset \langle a\rangle$. Entonces $b \in \langle a\rangle$. Concluimos que, $b = ax$ para algún $x \in D$. Es decir, $a \mid b$.

(2) Como a y b son asociados, existe una unidad u tal que $a = ub$. Por lo tanto, $b \mid a$ y $\langle a\rangle \subset \langle b\rangle$. Similarmente, $\langle b\rangle \subset \langle a\rangle$. En consecuencia $\langle a\rangle = \langle b\rangle$. Recíprocamente, supongamos que $\langle a\rangle = \langle b\rangle$. Por la parte (1), $a \mid b$ y $b \mid a$. Entonces $a = bx$ y $b = ay$ para ciertos $x, y \in D$. Por lo tanto, $a = bx = ayx$. Como D es un dominio integral, $xy = 1$; es decir, x e y son unidades y a y b son asociados.

(3) Un elemento $a \in D$ es una unidad si y solo si a es un asociado de 1. Pero, a es un asociado de 1 si y solo si $\langle a\rangle = \langle 1\rangle = D$. □

Teorema 18.12. *Sea D un* DIP *y $\langle p\rangle$ un ideal distinto de cero en D. Entonces $\langle p\rangle$ es un ideal maximal si y solo si p es irreducible.*

DEMOSTRACIÓN. Supongamos que $\langle p\rangle$ es un ideal maximal. Si algún elemento a en D divide a p, entonces $\langle p\rangle \subset \langle a\rangle$. Como $\langle p\rangle$ es maximal, ya sea $D = \langle a\rangle$ o $\langle p\rangle = \langle a\rangle$. En otras palabras, ya sea a y p son asociados o a es una unidad. Por lo tanto, p es irreducible.

Recíprocamente, sea p irreducible. Si $\langle a\rangle$ es un ideal en D tal que $\langle p\rangle \subset \langle a\rangle \subset D$, entonces $a \mid p$. Como p es irreducible, ya sea a es una unidad o a y p son asociados. Por lo tanto, ya sea $D = \langle a\rangle$ o $\langle p\rangle = \langle a\rangle$. Concluioms que $\langle p\rangle$ es un ideal maximal. □

Corolario 18.13. *Sea D un* DIP*. Si p es irreducible, entonces p es primo.*

DEMOSTRACIÓN. Sea p un irreducible y supongamos que $p \mid ab$. Entonces $\langle ab\rangle \subset \langle p\rangle$. Por el Corolario 16.40, como $\langle p\rangle$ es un ideal maximal, $\langle p\rangle$ también es un ideal primo. Luego, ya sea $a \in \langle p\rangle$ o $b \in \langle p\rangle$. En otras palabras, ya sea $p \mid a$ o $p \mid b$. □

Lema 18.14. *Sea D un* DIP*. Sean $I_1, I_2, \ldots$ ideales tales que $I_1 \subset I_2 \subset \cdots$. Entonces existe un entero N tal que $I_n = I_N$ para todo $n \geq N$.*

DEMOSTRACIÓN. Afirmamos que $I = \bigcup_{i=1}^{\infty} I_i$ es un ideal de D. Ciertamente I no es vacío, pues $I_1 \subset I$ y $0 \in I$. Si $a, b \in I$, entonces $a \in I_i$ y $b \in I_j$ para ciertos i y j en $\mathbb{N}$. Sin pérdida de generalidad podemos suponer que $i \leq j$. Entonces, a y b están ambos en I_j de manera que $a - b$ también está en I_j. Ahora sea $r \in D$ y $a \in I$. Nuevamente, notemos que $a \in I_i$ para algún entero positivo i. Como I_i es un ideal, $ra \in I_i$ y $ra \in I$. Por lo tanto, hemos demostrado que I es un ideal en D.

Como D es un dominio de ideales principales, existe un elemento $\overline{a} \in D$ que genera a I. Como $\overline{a}$ está en I_N para algún $N \in \mathbb{N}$, sabemos que $I_N = I = \langle \overline{a}\rangle$. Consecuentemente, $I_n = I_N$ para $n \geq N$. □

Cualquier anillo conmutativo que satisfaga la condición en el Lema 18.14 se dice que satisface la ***condición de cadenas ascendentes***, o ***CCA***. Tales anillo se llaman ***anillos Noetherianos***, en honor a Emmy Noether.

Teorema 18.15. *Todo* DIP *es un* DFU.

DEMOSTRACIÓN. *Existencia de una factorización.* Sea D un DIP y sea a un elemento distinto de cero en D que no sea una unidad. Si a es irreducible, no hay más que probar. Si no, entonces existe una factorización $a = a_1 b_1$, donde ni a_1 ni b_1 son unidades. Por ende, $\langle a\rangle \subset \langle a_1\rangle$. Por el Lema 18.11, sabemos que $\langle a\rangle \neq \langle a_1\rangle$; de lo contrario, a y a_1 serían asociados y b_1 sería una unidad,

lo que sería una contradicción. Ahora supongamos que $a_1 = a_2 b_2$, donde ni a_2 ni b_2 son unidades. Por el mismo argumento de antes, $\langle a_1 \rangle \subset \langle a_2 \rangle$. Podemos continuar esta construcción para obtener una cadena ascendente de ideales

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots .$$

Por el Lema 18.14, existe un entero positivo N tal que $\langle a_n \rangle = \langle a_N \rangle$ para todo $n \geq N$. En consecuencia, a_N debe ser irreducible. Hemos mostrado que a es producto de dos elementos, uno de los cuáles tiene que ser irreducible.

Ahora supongamos que $a = c_1 p_1$, donde p_1 es irreducible. Si c_1 no es una unidad, podemos repetir el argumento anterior para concluir que $\langle a \rangle \subset \langle c_1 \rangle$. Ya sea c_1 es irreducible o $c_1 = c_2 p_2$, donde p_2 es irreducible y c_2 no es una unidad. Continuando de esta manera, obtenemos otra cadena de ideales

$$\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \cdots .$$

Esta cadena debe satisfacer la condición de cadenas ascendentes; por lo tanto,

$$a = p_1 p_2 \cdots p_r$$

para elementos irreducibles $p_1, \ldots, p_r$.

Unicidad de la factorización. Para mostrar la unicidad, sea

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

donde cada p_i y cada q_i es irreducible. Sin pérdida de generalidad, podemos suponer que $r < s$. Como p_1 divide a $q_1 q_2 \cdots q_s$, por el Corolario 18.13 debe dividir a algún q_i. Reordenando los q_i, podemos suponer que $p_1 \mid q_1$; así, $q_1 = u_1 p_1$ para alguna unidad u_1 en D. Por lo tanto,

$$a = p_1 p_2 \cdots p_r = u_1 p_1 q_2 \cdots q_s$$

o

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s.$$

Continuando de esta manera, podemos reordenar los q_i tal que $p_2 = u_2 q_2, p_3 = u_3 q_3, \ldots, p_r = u_r q_r$, y obtener

$$u_1 u_2 \cdots u_r q_{r+1} \cdots q_s = 1.$$

En este caso $q_{r+1} \cdots q_s$ es una unidad, lo que contradice el hecho de que $q_{r+1}, \ldots, q_s$ son irreducibles. Por lo tanto, $r = s$ y la factorización de a es única. □

Corolario 18.16. *Sea F un cuerpo. Entonces $F[x]$ es un* DFU.

Ejemplo 18.17. Todo DIP es un DFU, pero no todo DFU es un DIP. En el Corolario 18.31, demostraremos que $\mathbb{Z}[x]$ es un DFU. Pero, $\mathbb{Z}[x]$ no es un DIP. Sea $I = \{5f(x) + xg(x) : f(x), g(x) \in \mathbb{Z}[x]\}$. Podemos mostrar fácilmente que I es un ideal de $\mathbb{Z}[x]$. Supongamos que $I = \langle p(x) \rangle$. Como $5 \in I$, $5 = f(x)p(x)$. En este caso $p(x) = p$ debe ser una constante. Como $x \in I$, $x = pg(x)$; luego, $p = \pm 1$. Pero, de esto conluimos que $\langle p(x) \rangle = \mathbb{Z}[x]$. Pero esto diría que 3 está en I. Por lo tanto, podemos escribir $3 = 5f(x) + xg(x)$ para ciertos $f(x)$ y $g(x)$ en $\mathbb{Z}[x]$. Examinando el términio constante de este polinomio, vemos que $3 = 5f(x)$, lo que es imposible.

Dominios Euclideanos

Hemos usado de forma repetida el algoritmo de la división para probar resultados tanto sobre $\mathbb{Z}$ como sobre $F[x]$, donde F es un cuerpo. Nos preguntamos ahora cuándo es que existe un algoritmo de la división para un dominio integral.

Sea D un dominio integral tal que para cada $a \in D$ existe un entero no negativo $\nu(a)$ que satisface las siguientes condiciones.

1. Si a y b son elementos distintos de cero en D, entonces $\nu(a) \leq \nu(ab)$.

2. Sean $a, b \in D$ y supongamos que $b \neq 0$. Entonces existen elementos $q, r \in D$ tales que $a = bq + r$ y ya sea $r = 0$ o $\nu(r) < \nu(b)$.

Entonces D se llama ***dominio Euclideano*** y ν se llama ***valuación Euclideana***.

Ejemplo 18.18. El valor absoluto en $\mathbb{Z}$ es una valuación Euclideana.

Ejemplo 18.19. Sea F un cuerpo. Entonces el grado de un polinomio en $F[x]$ es una valuación Euclideana.

Ejemplo 18.20. Reclos enteros Gaussianos en el Ejemplo 16.12 del Capítulo 16 están definidos como

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Usualmente medimos el tamaño de un número complejo $a + bi$ por su valor absoluto, $|a + bi| = \sqrt{a^2 + b^2}$; pero, $\sqrt{a^2 + b^2}$ podría no ser un entero. Como valuación elegiremos $\nu(a + bi) = a^2 + b^2$ para asegurarnos de tener un entero.

Afirmamos que $\nu(a+bi) = a^2+b^2$ es una valuación Euclideana en $\mathbb{Z}[i]$. Sean $z, w \in \mathbb{Z}[i]$. Entonces $\nu(zw) = |zw|^2 = |z|^2|w|^2 = \nu(z)\nu(w)$. Como $\nu(z) \geq 1$ para todo $z \in \mathbb{Z}[i]$ distinto de cero, $\nu(z) \leq \nu(z)\nu(w)$.

A continuación, debemos mostrar que para cualquiera $z = a+bi$ y $w = c+di$ en $\mathbb{Z}[i]$ con $w \neq 0$, existen elementos q y r en $\mathbb{Z}[i]$ tales que $z = qw + r$ con ya sea $r = 0$ o $\nu(r) < \nu(w)$. Podemos considerar z y w como elementos en $\mathbb{Q}(i) = \{p + qi : p, q \in \mathbb{Q}\}$, el cuerpo de fracciones de $\mathbb{Z}[i]$. Observemos que

$$\begin{aligned}
zw^{-1} &= (a + bi)\frac{c - di}{c^2 + d^2} \\
&= \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i \\
&= \left(m_1 + \frac{n_1}{c^2 + d^2}\right) + \left(m_2 + \frac{n_2}{c^2 + d^2}\right)i \\
&= (m_1 + m_2 i) + \left(\frac{n_1}{c^2 + d^2} + \frac{n_2}{c^2 + d^2}i\right) \\
&= (m_1 + m_2 i) + (s + ti)
\end{aligned}$$

en $\mathbb{Q}(i)$. En los últimos pasos escribimos las partes real e imaginaria como un entero más una fracción propia. Es decir, tomamos el entero más cercano m_i tal que la parte fraccionaria satisface $|n_i/(a^2 + b^2)| \leq 1/2$. Por ejemplo, escribimos

$$\begin{aligned}
\frac{9}{8} &= 1 + \frac{1}{8} \\
\frac{15}{8} &= 2 - \frac{1}{8}.
\end{aligned}$$

Así, s y t son las "partes fraccionarias" de $zw^{-1} = (m_1+m_2i)+(s+ti)$. También sabemos que $s^2 + t^2 \leq 1/4 + 1/4 = 1/2$. Multiplicando por w, tenemos

$$z = zw^{-1}w = w(m_1 + m_2i) + w(s + ti) = qw + r,$$

donde $q = m_1 + m_2i$ y $r = w(s + ti)$. Como z y qw están en $\mathbb{Z}[i]$, r también está en $\mathbb{Z}[i]$. Finalmente, dedemos mostrar que ya sea $r = 0$ o $\nu(r) < \nu(w)$. Pero,

$$\nu(r) = \nu(w)\nu(s + ti) \leq \frac{1}{2}\nu(w) < \nu(w).$$

Teorema 18.21. *Todo dominio Euclideano es un dominio de ideales principales.*

DEMOSTRACIÓN. Sea D un dominio Euclideano y sea ν una valuación Euclideana en D. Supongamos que I es un ideal no trivial en D y escojamos un elemento $b \in I$ distinto de cero tal que $\nu(b)$ es minimal entre todos los $a \in I$ distintos de cero. Para cualquier $a \in I$ distinto de cero, como D es un dominio Euclideano, existen elementos q y r en D tales que $a = bq + r$ y ya sea $r = 0$ o $\nu(r) < \nu(b)$. Pero $r = a - bq$ está en I pues I es un ideal; por lo tanto, $r = 0$ por la minimalidad de b. Concluioms que $a = bq$ y que $I = \langle b \rangle$. □

Corolario 18.22. *Todo dominio Euclideano es un dominio de factorización única.*

Factorización en $D[x]$

Uno de los anillos de polinomios más importantes es $\mathbb{Z}[x]$. Una de las primeras preguntas que surgen es si $\mathbb{Z}[x]$ es o no un DFU. Demostraremos un resultado más general. Primero obtendremos una generalización del Lema de Gauss (Teorema 17.14).

Sea D un dominio de factorización única y supongamos que

$$p(x) = a_n x^n + \cdots + a_1 x + a_0$$

en $D[x]$. Entonces, el ***contenido*** de $p(x)$ es el máximo común divisor de $a_0, \ldots, a_n$. Decimos que $p(x)$ es ***primitivo*** si $\text{mcd}(a_0, \ldots, a_n) = 1$.

Ejemplo 18.23. En $\mathbb{Z}[x]$ el polinomio $p(x) = 5x^4 - 3x^3 + x - 4$ es un polinomio primitivo pues el máximo común divisor de sus coeficientes es 1; pero, el polinomio $q(x) = 4x^2 - 6x + 8$ no es primitivo pues el contenido de $q(x)$ es 2.

Teorema 18.24 (Lema de Gauss)**.** *Sea D un* DFU *y sean $f(x)$ y $g(x)$ polinomios primitivos en $D[x]$. Entonces $f(x)g(x)$ es primitivo.*

DEMOSTRACIÓN. Sean $f(x) = \sum_{i=0}^{m} a_i x^i$ y $g(x) = \sum_{i=0}^{n} b_i x^i$. Supongamos que p es un primo que divide a todos los coeficientes de $f(x)g(x)$. Sea r el menor entero tal que $p \not| a_r$ y s el menor entero tal que $p \not| b_s$. El coeficiente de x^{r+s} en $f(x)g(x)$ es

$$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r+s-1} b_1 + a_{r+s} b_0.$$

Como p divide a $a_0, \ldots, a_{r-1}$ y $b_0, \ldots, b_{s-1}$, p divide a cada término de c_{r+s} excepto por el término $a_r b_s$. Pero, como $p \mid c_{r+s}$, ya sea p divide a a_r o p divide a b_s lo que es imposible. □

Lema 18.25. *Sea D un* DFU*, y sean $p(x)$ y $q(x)$ polinomios en $D[x]$. Entonecs el contenido de $p(x)q(x)$ es igual al producto de los contenidos de $p(x)$ y $q(x)$.*

DEMOSTRACIÓN. Sean $p(x) = cp_1(x)$ y $q(x) = dq_1(x)$, donde c y d son los contenidos de $p(x)$ y $q(x)$, respectivamente. Entonces $p_1(x)$ y $q_1(x)$ son primitivos. Podemos ahora escribir $p(x)q(x) = cdp_1(x)q_1(x)$. Como $p_1(x)q_1(x)$ es primitivo, el contenido de $p(x)q(x)$ es cd. □

Lema 18.26. *Sea D un* DFU *y sea F su cuerpo de fracciones. Supongamos que $p(x) \in D[x]$ y $p(x) = f(x)g(x)$, donde $f(x)$ y $g(x)$ están en $F[x]$. Entonces $p(x) = f_1(x)g_1(x)$, donde $f_1(x)$ y $g_1(x)$ están en $D[x]$. Además,* $\operatorname{gr} f(x) = \operatorname{gr} f_1(x)$ *y* $\operatorname{gr} g(x) = \operatorname{gr} g_1(x)$.

DEMOSTRACIÓN. Sean a y b elementos distintos de cero en D tales que $af(x), bg(x)$ están en $D[x]$. Podemos encontrar $a_1, b_2 \in D$ tales que $af(x) = a_1f_1(x)$ y $bg(x) = b_1g_1(x)$, donde $f_1(x)$ y $g_1(x)$ son polinomios primitivos en $D[x]$. Por lo tanto, $abp(x) = (a_1f_1(x))(b_1g_1(x))$. Como $f_1(x)$ y $g_1(x)$ son polinomios primitivos, debemos tener que $ab \mid a_1b_1$ por el Lema de Gauss. Así, existe un $c \in D$ tal que $p(x) = cf_1(x)g_1(x)$. Claramente, $\operatorname{gr} f(x) = \operatorname{gr} f_1(x)$ y $\operatorname{gr} g(x) = \operatorname{gr} g_1(x)$. □

Los siguientes corolarios son consecuencia directa del Lema 18.26.

Corolario 18.27. *Sea D un* DFU *y F su cuerpo de fracciones. Un polinomio primitiv $p(x)$ en $D[x]$ es irreducible en $F[x]$ si y solo si es irreducible en $D[x]$.*

Corolario 18.28. *Sea D un* DFU *y F su cuerpo de fracciones. Si $p(x)$ es un polinomio mónico en $D[x]$ con $p(x) = f(x)g(x)$ en $F[x]$, entonces $p(x) = f_1(x)g_1(x)$, donde $f_1(x)$ y $g_1(x)$ están en $D[x]$. Además,* $\operatorname{gr} f(x) = \operatorname{gr} f_1(x)$ *y* $\operatorname{gr} g(x) = \operatorname{gr} g_1(x)$.

Teorema 18.29. *Si D es un* DFU*, entonces $D[x]$ es un* DFU.

DEMOSTRACIÓN. Sea $p(x)$ un polinomio distinto de cero en $D[x]$. Si $p(x)$ es un polinomio constante, entonces tiene una factorización única pues D es un DFU. Ahora supongamos que $p(x)$ es un polinomio de grado positivo en $D[x]$. Sea F el cuerpo de fracciones de D, y sea $p(x) = f_1(x)f_2(x)\cdots f_n(x)$ una factorización de $p(x)$, donde cada $f_i(x)$ es irreducible. Escojamos $a_i \in D$ tales que $a_if_i(x)$ esté en $D[x]$. Existen $b_1, \ldots, b_n \in D$ tales que $a_if_i(x) = b_ig_i(x)$, donde $g_i(x)$ es un polinomio primitivo en $D[x]$. Por el Corolario 18.27, cada $g_i(x)$ es irreducible en $D[x]$. Así, podemos escribir

$$a_1 \cdots a_n p(x) = b_1 \cdots b_n g_1(x) \cdots g_n(x).$$

Sea $b = b_1 \cdots b_n$. Como $g_1(x) \cdots g_n(x)$ es primitive, $a_1 \cdots a_n$ divide a b. Por lo tanto, $p(x) = ag_1(x) \cdots g_n(x)$, donde $a \in D$. Como D es un DFU, podemos factorizar a como $uc_1 \cdots c_k$, donde u es una unidad y cada uno de los c_i es irreducible en D.

Ahora mostraremos la unicidad de esta factorización. Sean

$$p(x) = a_1 \cdots a_m f_1(x) \cdots f_n(x) = b_1 \cdots b_r g_1(x) \cdots g_s(x)$$

dos factorizaciones de $p(x)$, donde todos los factores son irreducibles en $D[x]$. Por el Corolario 18.27, cada uno de los f_i y de los g_i es irreducible en $F[x]$. Los a_i y los b_i son unidades en F. Como $F[x]$ es un DIP, es un DFU; por lo tanto, $n = s$. Reordenamos los $g_i(x)$ de manera que $f_i(x)$ y $g_i(x)$ sean asociados para $i = 1, \ldots, n$. Entonces existen $c_1, \ldots, c_n$ y $d_1, \ldots, d_n$ en D tales que $(c_i/d_i)f_i(x) = g_i(x)$ o $c_if_i(x) = d_ig_i(x)$. Los polinomios $f_i(x)$ y $g_i(x)$ son primitivos; luego, c_i y d_i son asociados en D. Así, $a_1 \cdots a_m = ub_1 \cdots b_r$ en D, donde u es una unidad en D. Como D es un dominio de factorización única, $m = s$. Finalmente, podemos reordenar los b_i de manera que a_i y b_i sean asociados para cada i. Esto completa la parte de unicidad de la demostración. □

El teorema que acabamos de demostrar tiene varios corolarios obvios pero importantes.

Corolario 18.30. *Sea F un cuerpo. Entonces $F[x]$ es un* DFU.

Corolario 18.31. *El anillo de polinomios sobre los enteros, $\mathbb{Z}[x]$, es un* DFU.

Corolario 18.32. *Sea D un* DFU. *Entonces $D[x_1, \ldots, x_n]$ es un* DFU.

Nota 18.33. Es importante destacar que todo dominio Euclideano es un DIP y que todo DIP es un DFU. Sinembargo, como hemos demostrado con ejemplos, los recíprocos de cada una de estas aseveraciones son falsos. Existen dominios de ideales principales que no son dominios Euclideanos, y existen dominios de factorización única que no son dominios de ideales principales ($\mathbb{Z}[x]$).

Sage Sage supports distinctions between "plain" rings, domains, principal ideal domains and fields. Support is often very good for constructions and computations with PID's, but sometimes problems get significantly harder (computationally) when a ring has less structure that that of a PID. So be aware when using Sage that some questions may go unanswered for rings with less structure.

Nota Histórica

Karl Friedrich Gauss, nació en Brunswick, Alemania el 30 de Abril de 1777 y es considerado uno de los matemáticos más importantes de la historia. Gauss fue realmente un niño prodigio. A los tres años pudo detectar errores en los libros de contabilidad del negocio de su padre. Gauss entró a la universidad a los 15 años. Antes de los 20, Gauss fue capaz de cosntruir un heptadecágono regular con regla y compás. Esta fue la primera construcción nueva de un n-ágono regular desde el tiempo de la Grecia Antigua. Gauss pudo demostrar que si $N = 2^{2^n} + 1$ es primo, entonces es posible construir un polígono regular de N lados usando regla y compás.

Gauss obtuvo su doctorado en 1799 bajo la dirección de Pfaff en la Universidad de Helmstedt. En su tesis fue el primero en dar una demostración completa del Teorema Fundamental del Álgebra, que establece que todo polinomio con coeficientes complejos puede ser factorizado completamente sobre los números complejos. La aceptación de los números complejos fue liderada por Gauss, quien fue el primero en usar la notación i para $\sqrt{-1}$.

A continuación Gauss se dedicó a la teoría de números; en 1801, publicó su famoso libro de teoría de números, *Disquisitiones Arithmeticae*. Durante toda su vida estuvo interesado por esta rama de las matemáticas. Alguna vez escribió que, "la Matemática es la reina de las Ciencias, y la teoría de números es la reina de las matemáticas."

En 1807, Gauss fue nombrado director del Observatorio en la Universidad de Göttingen, cargo que mantuvo hasta su muerte. En este cargo tuvo que estudiar aplicaciones de las matemáticas a las ciencias. Realizó contribuciones a campos como astronomía, mecánica, óptica, geodesia y magnetismo. Junto a Wilhelm Weber, fue coinventor del primer telégrafo eléctrico prácticoalgunos años anes de que una versión mejor fuera inventada por Samuel F. B. Morse.

Gauss fue claramente el matemático más prominente de comienzos del siglo XIX. Su estatus lo sometió naturalmente a un intenso escrutinio. La personalidad fría y distante de Gauss lo llevó muchas veces a ignorar el trabajo de su contemporáneos, creándole muchos enemigos. No le gustaba mucho hacer clases, y jóvenes que buscaban su apoyo, eran rechazados con frecuencia. Sin

embargo, tuvo muchos discípulos sobresalientes, incluyendo a Eisenstein, Riemann, Kummer, Dirichlet, y Dedekind. Gauss también apoyó decididamente a Sophie Germain (1776–1831), que tuvo que sobrepasar los muchos obstáculos que existían en su tiempo en el camino de una mujer para convertirse en una prestigiosa matemática. Gauss murió a los 78 años en Göttingen el 23 de February 23 de 1855.

18.3 Exercises

1. Let $z = a + b\sqrt{3}\,i$ be in $\mathbb{Z}[\sqrt{3}\,i]$. If $a^2 + 3b^2 = 1$, show that z must be a unit. Show that the only units of $\mathbb{Z}[\sqrt{3}\,i]$ are 1 and -1.

2. The Gaussian integers, $\mathbb{Z}[i]$, are a UFD. Factor each of the following elements in $\mathbb{Z}[i]$ into a product of irreducibles.

(a) 5
(b) $1 + 3i$
(c) $6 + 8i$
(d) 2

3. Let D be an integral domain.

(a) Prove that F_D is an abelian group under the operation of addition.
(b) Show that the operation of multiplication is well-defined in the field of fractions, F_D.
(c) Verify the associative and commutative properties for multiplication in F_D.

4. Prove or disprove: Any subring of a field F containing 1 is an integral domain.

5. Prove or disprove: If D is an integral domain, then every prime element in D is also irreducible in D.

6. Let F be a field of characteristic zero. Prove that F contains a subfield isomorphic to $\mathbb{Q}$.

7. Let F be a field.

(a) Prove that the field of fractions of $F[x]$, denoted by $F(x)$, is isomorphic to the set all rational expressions $p(x)/q(x)$, where $q(x)$ is not the zero polynomial.
(b) Let $p(x_1, \ldots, x_n)$ and $q(x_1, \ldots, x_n)$ be polynomials in $F[x_1, \ldots, x_n]$. Show that the set of all rational expressions $p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n)$ is isomorphic to the field of fractions of $F[x_1, \ldots, x_n]$. We denote the field of fractions of $F[x_1, \ldots, x_n]$ by $F(x_1, \ldots, x_n)$.

8. Let p be prime and denote the field of fractions of $\mathbb{Z}_p[x]$ by $\mathbb{Z}_p(x)$. Prove that $\mathbb{Z}_p(x)$ is an infinite field of characteristic p.

9. Prove that the field of fractions of the Gaussian integers, $\mathbb{Z}[i]$, is

$$\mathbb{Q}(i) = \{p + qi : p, q \in \mathbb{Q}\}.$$

10. A field F is called a ***prime field*** if it has no proper subfields. If E is a subfield of F and E is a prime field, then E is a ***prime subfield*** of F.

(a) Prove that every field contains a unique prime subfield.

(b) If F is a field of characteristic 0, prove that the prime subfield of F is isomorphic to the field of rational numbers, $\mathbb{Q}$.

(c) If F is a field of characteristic p, prove that the prime subfield of F is isomorphic to $\mathbb{Z}_p$.

11. Let $\mathbb{Z}[\sqrt{2}\,] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

(a) Prove that $\mathbb{Z}[\sqrt{2}\,]$ is an integral domain.

(b) Find all of the units in $\mathbb{Z}[\sqrt{2}\,]$.

(c) Determine the field of fractions of $\mathbb{Z}[\sqrt{2}\,]$.

(d) Prove that $\mathbb{Z}[\sqrt{2}i]$ is a Euclidean domain under the Euclidean valuation $\nu(a + b\sqrt{2}\,i) = a^2 + 2b^2$.

12. Let D be a UFD. An element $d \in D$ is a ***greatest common divisor of*** a ***and*** b ***in*** D if $d \mid a$ and $d \mid b$ and d is divisible by any other element dividing both a and b.

(a) If D is a PID and a and b are both nonzero elements of D, prove there exists a unique greatest common divisor of a and b up to associates. That is, if d and d' are both greatest common divisors of a and b, then d and d' are associates. We write $\text{mcd}(a, b)$ for the greatest common divisor of a and b.

(b) Let D be a PID and a and b be nonzero elements of D. Prove that there exist elements s and t in D such that $\text{mcd}(a, b) = as + bt$.

13. Let D be an integral domain. Define a relation on D by $a \sim b$ if a and b are associates in D. Prove that $\sim$ is an equivalence relation on D.

14. Let D be a Euclidean domain with Euclidean valuation ν. If u is a unit in D, show that $\nu(u) = \nu(1)$.

15. Let D be a Euclidean domain with Euclidean valuation ν. If a and b are associates in D, prove that $\nu(a) = \nu(b)$.

16. Show that $\mathbb{Z}[\sqrt{5}\,i]$ is not a unique factorization domain.

17. Prove or disprove: Every subdomain of a UFD is also a UFD.

18. An ideal of a commutative ring R is said to be ***finitely generated*** if there exist elements $a_1, \ldots, a_n$ in R such that every element $r \in R$ can be written as $a_1r_1 + \cdots + a_nr_n$ for some $r_1, \ldots, r_n$ in R. Prove that R satisfies the ascending chain condition if and only if every ideal of R is finitely generated.

19. Let D be an integral domain with a descending chain of ideals $I_1 \supset I_2 \supset I_3 \supset \cdots$. Suppose that there exists an N such that $I_k = I_N$ for all $k \geq N$. A ring satisfying this condition is said to satisfy the ***descending chain condition***, or ***DCC***. Rings satisfying the DCC are called ***Artinian rings***, after Emil Artin. Show that if D satisfies the descending chain condition, it must satisfy the ascending chain condition.

20. Let R be a commutative ring with identity. We define a ***multiplicative subset*** of R to be a subset S such that $1 \in S$ and $ab \in S$ if $a, b \in S$.

(a) Define a relation $\sim$ on $R \times S$ by $(a, s) \sim (a', s')$ if there exists an $s^* \in S$ such that $s^*(s'a - sa') = 0$. Show that $\sim$ is an equivalence relation on $R \times S$.

(b) Let a/s denote the equivalence class of $(a, s) \in R \times S$ and let $S^{-1}R$ be the set of all equivalence classes with respect to $\sim$. Define the operations of addition and multiplication on $S^{-1}R$ by

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$
$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st},$$

respectively. Prove that these operations are well-defined on $S^{-1}R$ and that $S^{-1}R$ is a ring with identity under these operations. The ring $S^{-1}R$ is called the ***ring of quotients*** of R with respect to S.

(c) Show that the map $\psi : R \to S^{-1}R$ defined by $\psi(a) = a/1$ is a ring homomorphism.

(d) If R has no zero divisors and $0 \notin S$, show that ψ is one-to-one.

(e) Prove that P is a prime ideal of R if and only if $S = R \backslash P$ is a multiplicative subset of R.

(f) If P is a prime ideal of R and $S = R \setminus P$, show that the ring of quotients $S^{-1}R$ has a unique maximal ideal. Any ring that has a unique maximal ideal is called a ***local ring***.

18.4 Referencias y Lecturas Recomendadas

[1] Atiyah, M. F. and MacDonald, I. G. *Introduction to Commutative Algebra*. Westview Press, Boulder, CO, 1994.

[2] Zariski, O. and Samuel, P. *Commutative Algebra*, vols. I and II. Springer, New York, 1975, 1960.

18.5 Sage

Ya hemos visto algunos dominios de integridad y de factorización única en los dos capítulos precedentes. Adem´a de lo que ya ehmos visto, Sage se puede usar para algunos de los tópicos de este capítulo, pero la implementación es limitada. Algunas funciones se pueden usar con algunos anillos y no con otros, mientras otras funciones aún no son parte de Sage. Daremos algunos ejemplos, pero esto está lejos de ser exhaustivo.

Cuerpo de Fracciones

Sage muchas veces es capaz de construir un cuerpo de fracciones, o de identificar un cierto cuerpo como un cuerpo de fracciones. Por ejemplo, el anillo de enteros y el cuerpo de los números racionales, están ambos implementados en Sage, y los enteros "saben" que los racionales forman su cuerpo de fracciones.

```
Q = ZZ.fraction_field(); Q
```

```
Rational Field
```

```
Q == QQ
```

```
True
```

En los otros casos Sage construye un cuerpo de fracciones, en el espíritu del Lema 18.3. Luego es posible hacer cálculos básicos en el cuerpo construido.

```
R.<x> = ZZ[]
P = R.fraction_field();P
```

```
Fraction Field of Univariate Polynomial Ring in x over
    Integer Ring
```

```
f = P((x^2+3)/(7*x+4))
g = P((4*x^2)/(3*x^2-5*x+4))
h = P((-2*x^3+4*x^2+3)/(x^2+1))
((f+g)/h).numerator()
```

```
3*x^6 + 23*x^5 + 32*x^4 + 8*x^3 + 41*x^2 - 15*x + 12
```

```
((f+g)/h).denominator()
```

```
-42*x^6 + 130*x^5 - 108*x^4 + 63*x^3 - 5*x^2 + 24*x + 48
```

Subcuerpos Primos

El Corolario 18.7 dice que todo cuerpo de característica p tiene un subcuerpo isomorfo a $\mathbb{Z}_p$. Para un cuerpo finito, la naturaleza exacta de este subcuerpo no es una sorpresa, y Sage nos permite extraerlo fácilmente.

```
F.<c> = FiniteField(3^5)
F.characteristic()
```

```
3
```

```
G = F.prime_subfield(); G
```

```
Finite Field of size 3
```

```
G.list()
```

```
[0, 1, 2]
```

Más en general, los cuerpos mencionados en las conclusiones del Corolario 18.6 y del Corolario 18.7 se conocen como el "subcuerpo primo" del anillo que los contiene. Acá un ejemplo en el caso de característica cero.

```
K.<y>=QuadraticField(-7); K
```

```
Number Field in y with defining polynomial x^2 + 7
```

```
K.prime_subfield()
```

```
Rational Field
```

A grosso modo, todo cuerpo de característica cero contiene una copia de los números racionales (el cuerpo de fracciones de los enteros), lo que puede explicar el extenso soporte en Sage de los anillos y cuerpos que extienden a los enteros y los racionales.

Dominios Integrales

Sage puede determinar si alguns anillos son dominios integrales y podemos comprobar productos en ellos. Pero, nociones de unidades, elementos irreducibles o primos no están implementadas en general (fuera de lo que vimos para polinomios en el capítulo anterior). Peor aún, la construcción que sigue crea un anillo dentro de un cuerpo mayor y por ello algunas de las funciones (como `.is_unit()`) se heredan y dan resultados engañosos. Esto debido a que la construcción de abajo crea un anillo conocido como un "orde en un cuerpo de números."

```
K.<x> = ZZ[sqrt(-3)]; K
```

```
Order in Number Field in a with defining polynomial x^2 + 3
```

```
K.is_integral_domain()
```

```
True
```

```
K.basis()
```

```
[1, a]
```

```
x
```

```
a
```

```
(1+x)*(1-x) == 2*2
```

```
True
```

Lo siguiente es un poco engañoso, pues 4, como elemento de $\mathbb{Z}[\sqrt{3}i]$ no tiene inverso multiplicativo, pero aparentemente podemo calcular uno. (Nota de AB: ¿por qué les molesta acá y no en $\mathbb{Z}$?)

```
four = K(4)
four.is_unit()
```

```
False
```

```
four^-1
```

```
1/4
```

Ideales Principales

Cuando un anillo es un dominio de ideales principales, como los enteros, o polynomios sobre un cuerpo, Sage funciona bien. Más allá de eso la cosa se debilita.

```
T.<x>=ZZ[]
T.is_integral_domain()
```

```
True
```

```
J = T.ideal(5, x); J
```

```
Ideal (5, x) of Univariate Polynomial Ring in x over Integer
    Ring
```

```
Q = T.quotient(J); Q
```

```
Quotient of Univariate Polynomial Ring in x over
Integer Ring by the ideal (5, x)
```

```
J.is_principal()
```

```
Traceback (most recent call last):
...
NotImplementedError
```

```
Q.is_field()
```

```
Traceback (most recent call last):
...
NotImplementedError
```

18.6 Ejercicios en Sage

No hay ejercicios en Sage para esta sección.

19

Reticulados y Álgebras Booleanas

Los axiomas de un anillo dan estructura a las operaciones de adición y multiplicación en un conjunto. Pero, podemos construir estructuras algebraicas, conocidas como reticulados y álgebras Booleanas, que generalizan otro tipo de operaciones. Por ejemplo, las operaciones importantes en conjuntos son inclusión, unión e intersección. Los reticulados son generalizaciones de relaciones de orden en espacios algebraicos, tal como la inclusión en teoría de conjuntos y la desigualdad en los sistemas de números familiares $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, y $\mathbb{R}$. Las álgebra Booleanas generalizan las opraciones de intersección y unión. Los reticulados y las álgebras Booleanas han encontrado aplicaciones en lógica, teoría de circuitos, y probabilidades.

19.1 Reticulados

Conjuntos Parcialmente Ordenados

Comenzamos nuestro estudio de los reticulados y las álgebras Booleanas generalizando la idea de desigualdad. Recordemos que una ***relación*** en un conjunto X es un subconjunto de $X \times X$. Una relación P en X se denomina ***orden parcial*** de X si satisface los siguientes axiomas.

1. La relación es ***refleja***: $(a, a) \in P$ para todo $a \in X$.
2. La relación es ***antisimétrica***: si $(a, b) \in P$ y $(b, a) \in P$, entonces $a = b$.
3. La relación es ***transitiva***: si $(a, b) \in P$ y $(b, c) \in P$, entonces $(a, c) \in P$.

Usualmente escribiremos $a \preceq b$ si $(a, b) \in P$ salvo que algún símbolo esté naturalmente asociado a un orden parcial en particular, tal como $a \leq b$ para los enteros a y b, o $A \subset B$ para conjuntos A y B. Un conjunto X junto a un orden parcial $\preceq$ se denomina ***conjunto parcialmente ordenado***, o ***poset***.

Ejemplo 19.1. El conjunto de los enteros (o racionales or reales) es un poset donde $a \leq b$ tiene el significado usual para dos enteros a y b en $\mathbb{Z}$.

Ejemplo 19.2. Sea X un conjunto cualquiera. Definiremos el ***conjunto potencia*** de X como el conjunto de todos los subconjuntos de X. Denotaremos el conjunto potencia de X como $\mathcal{P}(X)$. Por ejemplo, sea $X = \{a, b, c\}$. Entonces $\mathcal{P}(X)$ es el conjunto de todos los subconjuntos del conjunto $\{a, b, c\}$:

$$\emptyset \qquad \{a\} \qquad \{b\} \qquad \{c\}$$

$$\{a,b\} \qquad \{a,c\} \qquad \{b,c\} \qquad \{a,b,c\}.$$

En el conjunto potencia de cualquier conjunto X, la inclusión conjuntista, $\subset$, es un orden parcial. Podemos representar el orden en $\{a,b,c\}$ esquemáticamente con un diagrama como el de la Figura 19.3.

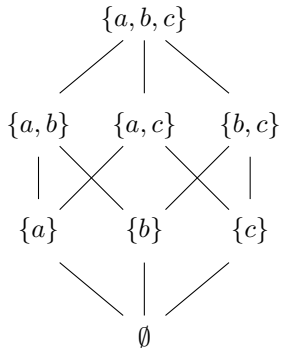


Figura 19.3: Orden parcial en $\mathcal{P}(\{a,b,c\})$

Ejemplo 19.4. Sea G un grupo. El conjunto de los subgrupos de G es un poset, donde el orden parcial es la inclusión conjuntista.

Ejemplo 19.5. Puede haber más de un orden parcial en un conjunto dado. Podemos formar un orden parcial en $\mathbb{N}$ por $a \preceq b$ si $a \mid b$. La relación es ciertamente refleja pues $a \mid a$ para todo $a \in \mathbb{N}$. Si $m \mid n$ y $n \mid m$, entonces $m = n$; luego, la relación también es antisimétrica. La relación es transitiva, pues si $m \mid n$ y $n \mid p$, entonces $m \mid p$.

Ejemplo 19.6. Sea $X = \{1,2,3,4,6,8,12,24\}$ el conjunto de los divisores de 24 con el orden parcial definido en el Ejemplo 19.5. La Figura 19.7 muestra el orden parcial en$X$.

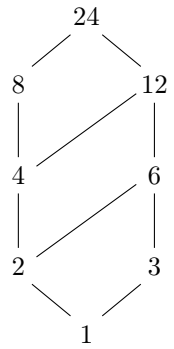


Figura 19.7: Un orden parcial en los divisores de 24

Sea Y un subconjunto de un poset X. Un elemento u en X es una ***cota superior*** de Y si $a \preceq u$ para cada elemento $a \in Y$. Si u es una cota superior de Y tal que $u \preceq v$ para cualquier cota superior v de Y, entonces u es la ***menor de las cotas superiores*** o ***supremo*** de Y. Un elemento l en X se dice ***cota inferior*** de Y si $l \preceq a$ para todo $a \in Y$. Si l es una cota inferior de Y tal que $k \preceq l$ para toda cota inferior k de Y, entonces l es la ***mayor cota inferior*** o ***ínfimo*** de Y.

Ejemplo 19.8. Sea $Y = \{2, 3, 4, 6\}$ contenido en el conjunto X del Ejemplo 19.6. Entonces Y tiene cotas superiores 12 y 24, con 12 una menor cota superior. La única cota inferior es 1; luego, debe ser una mayor cota inferior.

Resulta que, la mayor cota inferior y la menor cota superior resultan ser únicas cuando existen.

Teorema 19.9. *Sea Y un subconjunto no vacío de un poset X. Si Y tiene una menor cota superior, entonces Y tiene una única menor cota superior. Si Y tiene una mayor cota inferior, entonces Y tiene una única mayor cota inferior.*

DEMOSTRACIÓN. Sean u_1 y u_2 menores cotas superiores para Y. Por la definición de menor cota superior, $u_1 \preceq u$ para toda cota superior u de Y. En particular, $u_1 \preceq u_2$. Similarmente, $u_2 \preceq u_1$. Por lo tanto, $u_1 = u_2$ por antisimetría. Un argumento similar muestra que la mayor cota inferior es única. □

En muchos posets es posible definir operaciones binarias usando la menor cota superior y la mayor cota inferior de dos elementos. Un ***reticulado*** es un poset L tal que cada par de elementos en L tiene una menor cota superior y una mayor cota inferior. La menor cota superior de $a, b \in L$ se llama el ***supremo*** de a y b y se denota por $a \vee b$. La mayor cota inferior de $a, b \in L$ se llama el ***ínfimo*** de a y b y se denota por $a \wedge b$.

Ejemplo 19.10. Sea X un conjunto. Entonces el conjunto potencia de X, $\mathcal{P}(X)$, es un reticulado. Para dos conjuntos A y B en $\mathcal{P}(X)$, el supremo de A y B es $A \cup B$. Ciertamente $A \cup B$ es una cota superior de A y B, pues $A \subset A \cup B$ y $B \subset A \cup B$. Si C es algún conjunto que contiene tanto a A como a B, entonces C contiene a $A \cup B$; luego, $A \cup B$ es la menor de las cotas superiores de A y B. Similarmente, el ínfimo de A y B es $A \cap B$.

Ejemplo 19.11. Sea G un grupo y supongamos que X es el conjunto de subgrupos de G. Entonces X es un poset ordenado por inclusión conjuntista, $\subset$. El conjunto de subgrupos de G también es un reticulado. Si H y K so subgrupos de G, el ínfimo de H y K es $H \cap K$. El conjunto $H \cup K$ puede no ser un subgrupo de G. Dejamos como ejercicio demostrar que el supremo de H y K es el subgrupo generado por $H \cup K$.

En teoría de conjuntos tenemos ciertas condiciones de dualidad. Por ejemplo, por las leyes de De Morgan, todo enunciado sobre conjuntos que sea válido para $(A \cup B)'$ también debe ser válido para $A' \cap B'$. También tenemos un principio de dualidad para reticulados.

Axioma 19.12 (Principio de Dualidad)**.** *Cualquier enunciado que sea verdadero para todos los reticulados, sigue siendo verdadero se reemplazamos $\preceq$ por $\succeq$ e intercambiamos $\vee$ y $\wedge$ en todo el enunciado.*

El siguiente teorema nos dice que un reticulado es una estructura algebraica con dos operaciones bianria que satisfacen ciertos axiomas.

Teorema 19.13. *Si L es un reticulado, entonces las operaciones binarias $\vee$ y $\wedge$ satisfacen las siguientes propiedades para $a, b, c \in L$.*

1. *Leyes conmutativas: $a \vee b = b \vee a$ y $a \wedge b = b \wedge a$.*
2. *Leyes asociativas: $a \vee (b \vee c) = (a \vee b) \vee c$ y $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.*
3. *Leyes idempotentes: $a \vee a = a$ y $a \wedge a = a$.*
4. *Leyes de absorción: $a \vee (a \wedge b) = a$ y $a \wedge (a \vee b) = a$.*

DEMOSTRACIÓN. Por el Principio de Dualidad, solo debemos demostrar el primer enunciado de cada parte.

(1) Por definición $a \vee b$ es el supremo de $\{a, b\}$, y $b \vee a$ es el supremo de $\{b, a\}$; pero, $\{a, b\} = \{b, a\}$.

(2) Mostraremos que $a \vee (b \vee c)$ y $(a \vee b) \vee c$ son ambos ínfimos de $\{a, b, c\}$. Sea $d = a \vee b$. Entonces $c \preceq d \vee c = (a \vee b) \vee c$. También sabemos que

$$a \preceq a \vee b = d \preceq d \vee c = (a \vee b) \vee c.$$

Un argumento similar demuestra que $b \preceq (a \vee b) \vee c$. Por lo tanto, $(a \vee b) \vee c$ es una cota superior de $\{a, b, c\}$. Ahora debemos mostrar que $(a \vee b) \vee c$ es el supremo de $\{a, b, c\}$. Sea u alguna cota superior para $\{a, b, c\}$. Entonces $a \preceq u$ y $b \preceq u$; luego, $d = a \vee b \preceq u$. Como $c \preceq u$, sigue que $(a \vee b) \vee c = d \vee c \preceq u$. Por lo tanto, $(a \vee b) \vee c$ es el supremo de $\{a, b, c\}$. El argumento que muestra que $a \vee (b \vee c)$ es el supremos de $\{a, b, c\}$ es igual. En consecuencia, $a \vee (b \vee c) = (a \vee b) \vee c$.

(3) El supremo de a y a es el supremo de $\{a\}$; luego, $a \vee a = a$.

(4) Sea $d = a \wedge b$. Entonces $a \preceq a \vee d$. Por otra parte, $d = a \wedge b \preceq a$, y así $a \vee d \preceq a$. Por lo tanto, $a \vee (a \wedge b) = a$. □

Dado cualquier conjunto L con las operaciones $\vee$ y $\wedge$, que satisfacen las condiciones del teorema previo, es natural preguntarse si este conjunto proviene o no de un reticulado. El siguiente teorema dice que esto siempre es así.

Teorema 19.14. *Sea L un conjunto no-vacío con dos operaciones binarias $\vee$ y $\wedge$ que satisfacen las leyes conmutativa, asociativa, idempotente, y de absorción. Podemos definir un orden parcial en L por $a \preceq b$ si $a \vee b = b$. Más aún, L es un reticulado respecto $a \preceq$ si para todo $a, b \in L$, definimos un supremo y un ínfimo de a y b por $a \vee b$ y $a \wedge b$, respectivamente.*

DEMOSTRACIÓN. Mostraremos primero que L es un poset bajo $\preceq$. Como $a \vee a = a$, $a \preceq a$ y tenemos que $\preceq$ es refleja. Para mostrar que $\preceq$ es antisimétrica, sean $a \preceq b$ y $b \preceq a$. Entonces $a \vee b = b$ y $b \vee a = a$. Por la ley conmutativa, $b = a \vee b = b \vee a = a$. Finalmente, debemos mostrar que $\preceq$ es transitiva. Sean $a \preceq b$ y $b \preceq c$. Entonces $a \vee b = b$ y $b \vee c = c$. Luego,

$$a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c,$$

y $a \preceq c$.

Para mostrar que L es un reticulado, debemos demostrar que $a \vee b$ y $a \wedge b$ son, respectivamente, el supremo y el ínfimo de a y b. Como $a = (a \vee b) \wedge a = a \wedge (a \vee b)$, concluimos que $a \preceq a \vee b$. Similarmente, $b \preceq a \vee b$. Por lo tanto, $a \vee b$ es una cota superior para a y b. Sea u cualquier cota superior para a y b. Entonces $a \preceq u$ y $b \preceq u$. Pero $a \vee b \preceq u$ pues

$$(a \vee b) \vee u = a \vee (b \vee u) = a \vee u = u.$$

La demostración de que $a \wedge b$ es el ínfimo de a y b se deja como ejercicio. □

19.2 Álgebras Booleanas

Investiguemos el ejemplo del conjunto potencia, $\mathcal{P}(X)$, de un conjunto X en mayor detalle. El conjunto potencia es un reticulado ordenado por inclusión. Por la definición de conjunto potencias, el mayor elemento en $\mathcal{P}(X)$ es X mismo y el menor elemento es $\emptyset$, el conjunto vacío. Para cualquier conjunto A en $\mathcal{P}(X)$, sabemos que $A \cap X = A$ y $A \cup \emptyset = A$. Esto sugiere la siguiente definición para reticulados. Un elemento I en un poset X es un ***elemento***

mayor si $a \preceq I$ para todo $a \in X$. Un elemento O es un ***elemento menor*** de X si $O \preceq a$ para todo $a \in X$.

Sea A en $\mathcal{P}(X)$. Recuerde que el complemento de A es

$$A' = X \setminus A = \{x : x \in X \text{ y } x \notin A\}.$$

Sabemos que $A \cup A' = X$ y $A \cap A' = \emptyset$. Podemos generalizar este ejemplo a reticulados. Un reticulado L con mayor elemento I y menor elemento O es ***complementado*** si para cada $a \in L$, existe un a' tal que $a \vee a' = I$ y $a \wedge a' = O$.

En un reticulado L, las operaciones binarias $\vee$ y $\wedge$ satisfacen leyes conmutativas y asociativas; pero, no necesariamente satisfacen la ley distributiva

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c);$$

sin embargo, en $\mathcal{P}(X)$ la ley distributiva se satisface pues

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

para $A, B, C \in \mathcal{P}(X)$. Diremos que un reticulado L es ***distributivo*** si se satisfacen las siguientes leyes distributivas:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

para todo $a, b, c \in L$.

Teorema 19.15. *Un reticulado L es distributivo si y solo si*

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

para todo $a, b, c \in L$.

Demostración. Supongamos que L es un reticulado distributivo.

$$\begin{aligned} a \vee (b \wedge c) &= [a \vee (a \wedge c)] \vee (b \wedge c) \\ &= a \vee [(a \wedge c) \vee (b \wedge c)] \\ &= a \vee [(c \wedge a) \vee (c \wedge b)] \\ &= a \vee [c \wedge (a \vee b)] \\ &= a \vee [(a \vee b) \wedge c] \\ &= [(a \vee b) \wedge a] \vee [(a \vee b) \wedge c] \\ &= (a \vee b) \wedge (a \vee c). \end{aligned}$$

El recíproco es consecuencia directa del Principio de Dualidad. □

Un ***álgebra Booleana*** es un reticulado B con elemento mayor I y elemento menor O tal que B es distributivo y complementado. El conjunto potencia de X, $\mathcal{P}(X)$, es nuestro prototipo de álgebra Booleana. Resulta, que es además una de las álgebras Booleanas más importantes. El siguiente teorema nos permite caracterizar las álgebras Booleanas en términos de las relaciones binarias $\vee$ y $\wedge$ sin mencionar el hecho de que un álgebra Booleana es un poset.

Teorema 19.16. *Un conjunto B es un álgebra Booleana si y solo si existen operaciones binarias$\vee$ y $\wedge$ en B que satisfacen los siguientes axiomas.*

1. *$a \vee b = b \vee a$ y $a \wedge b = b \wedge a$ for $a, b \in B$.*
2. *$a \vee (b \vee c) = (a \vee b) \vee c$ y $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ para $a, b, c \in B$.*

3. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ *y* $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ *para* $a, b, c \in B$.

4. *Existen elementos* I *y* O *tales que* $a \vee O = a$ *y* $a \wedge I = a$ *para todo* $a \in B$.

5. *Para todo* $a \in B$ *existe* $a' \in B$ *tal que* $a \vee a' = I$ *y* $a \wedge a' = O$.

DEMOSTRACIÓN. Sea B un conjunto que satisface (1)–(5) en el teorema. Una de las leyes idempotentes se satisface pues

$$\begin{aligned} a &= a \vee O \\ &= a \vee (a \wedge a') \\ &= (a \vee a) \wedge (a \vee a') \\ &= (a \vee a) \wedge I \\ &= a \vee a. \end{aligned}$$

Observemos que

$$I \vee b = (I \vee b) \wedge I = (I \wedge I) \vee (b \wedge I) = I \vee I = I.$$

Concluimos que se satisface la primera de las dos leyes de absorción, pues

$$\begin{aligned} a \vee (a \wedge b) &= (a \wedge I) \vee (a \wedge b) \\ &= a \wedge (I \vee b) \\ &= a \wedge I \\ &= a. \end{aligned}$$

La otra ley idempotente y de absorción se demuestran de forma similar. Como B también satisface (1)–(3), se cumplen las condiciones del Teorema 19.14; por lo tanto, B es un reticulado. La condición (4) nos dice que B es un reticulado distributivo.

Para $a \in B$, $O \vee a = a$; luego, $O \preceq a$ y O es el menor elemento en B. Para mostrar que I es el mayor elemento en B, mostraremos primero que $a \vee b = b$ es equivalente a $a \wedge b = a$. Como $a \vee I = a$ para todo $a \in B$, usando las leyes de absorción podemos determinar que

$$a \vee I = (a \wedge I) \vee I = I \vee (I \wedge a) = I$$

y $a \preceq I$ para todo a in B. Finalmente, como sabemos que B es complementado po (5), B es un álgebra Booleana.

Recíprocamente, supongamos que B es un álgebra Booleana. Sean I y O el elemento mayor y el elemento menor en B, respectivamente. Si definimos $a \vee b$ y $a \wedge b$ como el supremo y el ínfimo de $\{a, b\}$ respectivamente, entonces B satisface las condiciones (1)–(5). □

Muchas otras identidades se satisfacen en las álgebras Booleanas. Algunas de estas identidades están listada en el siguiente teorema.

Teorema 19.17. *Sea* B *un álgebra Booleana. Entonces*

1. $a \vee I = I$ *y* $a \wedge O = O$ *para todo* $a \in B$.

2. *If* $a \vee b = a \vee c$ *y* $a \wedge b = a \wedge c$ *for* $a, b, c \in B$, *entonces* $b = c$.

3. *If* $a \vee b = I$ *y* $a \wedge b = O$, *entonces* $b = a'$.

4. $(a')' = a$ *para todo* $a \in B$.

5. $I' = O$ *y* $O' = I$.

6. $(a \vee b)' = a' \wedge b'$ *y* $(a \wedge b)' = a' \vee b'$ *(Leyes de De Morgan).*

DEMOSTRACIÓN. Solo demostraremos (2). El resto de las identidades las dejamos como ejercicios. Para $a \vee b = a \vee c$ y $a \wedge b = a \wedge c$, tenemos

$$\begin{aligned} b &= b \vee (b \wedge a) \\ &= b \vee (a \wedge b) \\ &= b \vee (a \wedge c) \\ &= (b \vee a) \wedge (b \vee c) \\ &= (a \vee b) \wedge (b \vee c) \\ &= (a \vee c) \wedge (b \vee c) \\ &= (c \vee a) \wedge (c \vee b) \\ &= c \vee (a \wedge b) \\ &= c \vee (a \wedge c) \\ &= c \vee (c \wedge a) \\ &= c. \end{aligned}$$

□

Álgebras Booleanas Finitas

Un álgebra Booleana es un ***álgebra Booleana finita*** si contiene un número finito de elementos como conjunto. Las álgebras Booleanas finitas son particularmente amigables, pues las podemos clasificar módulo isomorfismo.

Sean B y C álgebras Booleanas. Una función biyectiva $\phi : B \to C$ es un ***isomorfismo*** de álgebras Booleanas si

$$\begin{aligned} \phi(a \vee b) &= \phi(a) \vee \phi(b) \\ \phi(a \wedge b) &= \phi(a) \wedge \phi(b) \end{aligned}$$

para todo a y b en B.

Mostraremos que cualquier álgebra Booleana finita es isomorfa al álgebra Booleana obtenida de tomar el conjunto potencia de algún conjunto finito X. Necesitaremos algunos lemas y definiciones antes de demostrar este resultado. Sea B un álgebra Booleana finita. Un elemento $a \in B$ es un ***átomo*** de B si $a \neq O$ y $a \wedge b = a$ o $a \wedge b = O$ para todo $b \in B$. Equivalentemente, a es un átomo de B si no existe $b \in B$ distinto de cero y distinto de a tal que $O \preceq b \preceq a$.

Lema 19.18. *Sea B un álgebra Booleana finita. Si b es un elemento no nulo de B, entonces existe un átomo a en B tal que $a \preceq b$.*

DEMOSTRACIÓN. Si b es un átomo, sea $a = b$. De lo contrario, elija un elemento b_1, distinto de O y de b, tal que $b_1 \preceq b$. Estamos seguros que esto es posible ya que b no es un átomo. Si b_1 es un átomo, entonces estamos listos. Si no, elegimos b_2, distinto de O y de b_1, tal que $b_2 \preceq b_1$. Nuevamente, si b_2 es un átomo, sea $a = b_2$. Continuando este proceso, obtenemos una cadena

$$O \preceq \cdots \preceq b_3 \preceq b_2 \preceq b_1 \preceq b.$$

Como B es un álgenra Booleana finita, esta cadena debe ser finita. Es decir, para algún k, b_k es un átomo. Sea $a = b_k$. □

Lema 19.19. *Sean a y b átomos en un álgebra Booleana finita B tales que $a \neq b$. Entonces $a \wedge b = O$.*

DEMOSTRACIÓN. Como $a \wedge b$ es el ínfimo de a y b, sabemos que $a \wedge b \preceq a$. Luego, ya sea $a \wedge b = a$ o $a \wedge b = O$. Pero, si $a \wedge b = a$, entonces ya sea $a \preceq b$ o $a = O$. En cualquier caso tenemos una contradicción pues a y b son ambos átomos; por lo tanto, $a \wedge b = O$. □

Lema 19.20. *Sea B un álgebra Booleana y $a, b \in B$. Los siguientes enunciados son equivalentes.*

1. $a \preceq b$.
2. $a \wedge b' = O$.
3. $a' \vee b = I$.

DEMOSTRACIÓN. (1) ⇒ (2). Si $a \preceq b$, entonces $a \vee b = b$. Por lo tanto,

$$\begin{aligned} a \wedge b' &= a \wedge (a \vee b)' \\ &= a \wedge (a' \wedge b') \\ &= (a \wedge a') \wedge b' \\ &= O \wedge b' \\ &= O. \end{aligned}$$

(2) ⇒ (3). If $a \wedge b' = O$, entonces $a' \vee b = (a \wedge b')' = O' = I$.
(3) ⇒ (1). If $a' \vee b = I$, entonces

$$\begin{aligned} a &= a \wedge (a' \vee b) \\ &= (a \wedge a') \vee (a \wedge b) \\ &= O \vee (a \wedge b) \\ &= a \wedge b. \end{aligned}$$

Luego, $a \preceq b$. □

Lema 19.21. *Sea B un álgera Booleana y sean b y c elementos en B tales que $b \not\preceq c$. Entonces existe un átomo $a \in B$ tal que $a \preceq b$ y $a \not\preceq c$.*

DEMOSTRACIÓN. Por el Lema 19.20, $b \wedge c' \neq O$. Luego, existe un átomo a tal que $a \preceq b \wedge c'$. Concluimos que $a \preceq b$ y $a \not\preceq c$. □

Lema 19.22. *Sea $b \in B$ y sean $a_1, \ldots, a_n$ los átomos de B tales que $a_i \preceq b$. Entonces $b = a_1 \vee \cdots \vee a_n$. Más aún, si $a, a_1, \ldots, a_n$ son átomos de B tales que $a \preceq b$, $a_i \preceq b$, y $b = a \vee a_1 \vee \cdots \vee a_n$, entonces $a = a_i$ para algún $i = 1, \ldots, n$.*

DEMOSTRACIÓN. Sea $b_1 = a_1 \vee \cdots \vee a_n$. Como $a_i \preceq b$ para cada i, sabemos que $b_1 \preceq b$. Si podemos mostrar que $b \preceq b_1$, entonces el lema se cumple por la antisimetría. Supongamos que $b \not\preceq b_1$. Entonces existe un átomo a tal que $a \preceq b$ y $a \not\preceq b_1$. Como a es un átomo y $a \preceq b$, deducimos que $a = a_i$ para algún a_i. Pero esto es imposible pues $a \preceq b_1$. Por lo tanto, $b \preceq b_1$.

Ahora supongamos que $b = a_1 \vee \cdots \vee a_n$. Si a es un átomo menor que b,

$$a = a \wedge b = a \wedge (a_1 \vee \cdots \vee a_n) = (a \wedge a_1) \vee \cdots \vee (a \wedge a_n).$$

Pero cada término es O o a con $a \wedge a_i$ solo para un a_i. Luego, por el Lema 19.19, $a = a_i$ para algún i. □

Teorema 19.23. *Sea B un ágebra Booleana finita. Entonces existe un conjunto X tal que B es isomorfo a $\mathcal{P}(X)$.*

DEMOSTRACIÓN. Mostraremos que B es isomorfo a $\mathcal{P}(X)$, donde X es el conjunto de átomos de B. Sea $a \in B$. Por el Lema 19.22, podemos escribir a de forma única como $a = a_1 \vee \cdots \vee a_n$ para $a_1, \ldots, a_n \in X$. Concluimos que es posible definir una función $\phi : B \to \mathcal{P}(X)$ por

$$\phi(a) = \phi(a_1 \vee \cdots \vee a_n) = \{a_1, \ldots, a_n\}.$$

Claramente, ϕ es sobre.

Ahora sean $a = a_1 \vee \cdots \vee a_n$ y $b = b_1 \vee \cdots \vee b_m$ elementos en B, donde cada a_i y cada b_i es un átomo. Si $\phi(a) = \phi(b)$, entonces $\{a_1, \ldots, a_n\} = \{b_1, \ldots, b_m\}$ y $a = b$. Concluimos que ϕ es inyectiva.

El supremo de a y b es preservado por ϕ pues

$$\begin{aligned}
\phi(a \vee b) &= \phi(a_1 \vee \cdots \vee a_n \vee b_1 \vee \cdots \vee b_m) \\
&= \{a_1, \ldots, a_n, b_1, \ldots, b_m\} \\
&= \{a_1, \ldots, a_n\} \cup \{b_1, \ldots, b_m\} \\
&= \phi(a_1 \vee \cdots \vee a_n) \cup \phi(b_1 \wedge \cdots \vee b_m) \\
&= \phi(a) \cup \phi(b).
\end{aligned}$$

Similarmente, $\phi(a \wedge b) = \phi(a) \cap \phi(b)$. □

Dejaremos la demostración del siguiente corolario como un ejercicio.

Corolario 19.24. *El orden de cualquier álgebra Booleana finita es 2^n para algún entero positivo n.*

19.3 El Álgebra de los Circuitos Eléctricos

La utilidad de las álgebras Booleanas se ha vuelto cada vez más clara en las últimas décadas con el desarrollo del computador moderno. El diseño de circuitos integrados se puede expresar en términos de álgebras Booleanas. En esta sección desarrollaremos el álgebra Booleana de los circuitos eléctricos y de los conmutadores; pero, estos resultados se generalizan fácilmente al diseños de circuitos integrados para computadores.

Un ***conmutador*** es un artefacto, ubicado en algún punto de un circuito eléctrico, que controla el flujo de la corriente a través del circuito. Cada conmutador tiene dos estados posibles: puede estar ***abierto***, y no permitir el paso de la corriente a través del circuito, o puede estar ***cerrado***, y permitir el paso de corriente. Estos estados son mutuamente excluyentes. Requerimos que todo conmutador esté en un estado o en el otro—un conmutador no puede estar abierto y cerrado simultáneamente. Además, si un conmutador está siempre en el mismo estado que otro, los denotaremos a ambos por la misma letra; es decir, dos circuitos que etiquetados con la misma letra a estarán abiertos a la vez y cerrados a la vez.

Dados dos conmutadores, podemos construir dos tipos fundamentales de circuitos. Dos conmutadores a y b están en ***serie*** si forman un circuito del tipo ilustrado en la Figura 19.25. La corriente puede pasar entre los terminales A y B de un circuito en serie si y solo si ambos conmutadores a y b están cerrados. Denotaremos esta combinación de conmutadores por $a \wedge b$. Dos conmutadores a y b están en ***paralelo*** si forman un circuito del tipo que aparece en la Figura 19.26. En el caso de un circuito paralelo, la corriente puede pasar entre A y B si alguno de los dos conmutadores está cerrado. Denotaremos una combinación paralela de circuitos a y b por $a \vee b$.

Figura 19.25: $a \wedge b$

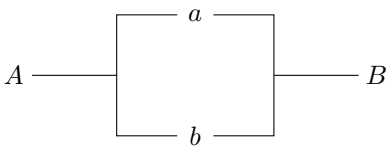


Figura 19.26: $a \vee b$

Podemos construir circuitos eléctrico más complicados a partir de circuitos en serie o en paralelo reemplazando cualquiera de los conmutadores por uno de estos tipos fundamentales de circuitos. Los circuitos construido de esta manera se llaman ***circuitos paralelo-seriales***.

Consideramos que dos circuitos son equivalentes si actúan igual. Es decir, si ponemos los conmutadores en circuitos equivalentes en exactamente los mismos estados, entonces obtendremos el mismo resultado. Por ejemplo, un circuito serial $a \wedge b$ es exactamente el mismo que $b \wedge a$. Notemos que esta es exactamente la ley conmutativa para álgebras Booleanas. De hecho, el conjunto de todos los circuitos paralelo-seriales forma un álgebra Booleana bajo las operaciones $\vee$ y $\wedge$. Podemos usar diagramas para verificar los distintos axiomas de un álgebra Booleana. La ley distributiva, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, está ilustrada en la Figura 19.27. Si a es un conmutador, entonces a' es el conmutador que siempre está abierto cuando a está cerrado y siempre está cerrado cuando a está abierto. Un circuito que siempre está cerrado es I en nuestra álgebra; un circuito que siempre está abierto es O. Las leyes de $a \wedge a' = O$ y $a \vee a' = I$ se muestran en la Figura 19.28.

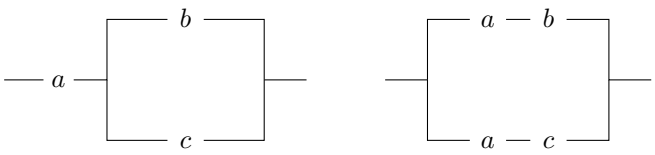


Figura 19.27: $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

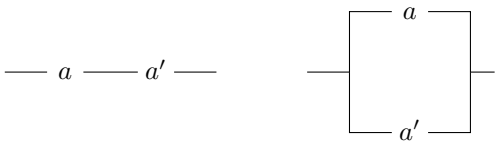


Figura 19.28: $a \wedge a' = O$ y $a \vee a' = I$

Ejemplo 19.29. Toda expresión Booleana representa un circuito de conmutadores. Por ejemplo, dada la expresión $(a \vee b) \wedge (a \vee b') \wedge (a \vee b)$, podemos construir el circuito en la Figura 19.32.

Teorema 19.30. *El conjunto de todos los circuitos es un álgebra Booleana.*

Dejamos como ejercicio la demostración de este teorema para los axiomas de álgebra Booleana aún no verificados. Podemos ahora aplicar las técnicas de álgebras Booleanas a la teoría de conmutadores.

Ejemplo 19.31. Dado un circuito complejo, podemos aplicar las técnicas de álgebra Booleana para reducirlo a un más simple. Consideremos el circuito en la Figura 19.32. Como

$$\begin{aligned}(a \vee b) \wedge (a \vee b') \wedge (a \vee b) &= (a \vee b) \wedge (a \vee b) \wedge (a \vee b') \\ &= (a \vee b) \wedge (a \vee b') \\ &= a \vee (b \wedge b') \\ &= a \vee O \\ &= a,\end{aligned}$$

podemos reemplazar el circuito más complicado por un circuito que contenga solo el conmutador a y lograr la misma función.

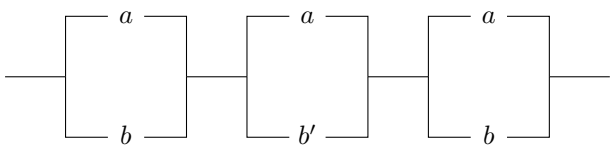


Figura 19.32: $(a \vee b) \wedge (a \vee b') \wedge (a \vee b)$

Sage Sage has a full suite of functionality for both posets and lattices, all as part of its excellent support for combinatorics. There is little in this chapter that cannot be investigated with Sage.

Nota Histórica

George Boole (1815–1864) fue la primera persona en estudiar reticulados. En 1847, publicó *The Investigation of the Laws of Thought*, un libro en el que usó reticulados para formalizar la lógica y el cálculo de proposiciones. Boole pensaba que las matemáticas eran el estudio de forma más que de contenido; es decir, no estaba tan preocupado en qué estaba calculando sino en cómo lo estaba calculando. El trabajo de Boole fue contiuado por su amigo Augustus De Morgan (1806–1871). De Morgan observó que el Principio de Dualidad se cumplía en la Teoría de Conjuntos, como se ilustra por las leyes de De Morgan. El pensaba, como Boole, que las matemáticas eran el estudio de símbolos y operaciones abstractas.

La teoría de conjuntos y la lógica fueron avanzados postriormente por matemáticos tales como Alfred North Whitehead (1861–1947), Bertrand Russell (1872–1970), y David Hilbert (1862–1943). en *Principia Mathematica*, Whitehead y Russell intentaron mostrar la conexión entre matemáticas y lógica mediante la deducción del sistema de números naturales a partir de las reglas de la lógica formal. Si los números naturales podían ser determinados a partir de la lógica misma, entonces también podría serlo buena parte del resto de las matemáticas. Sus planes sufrieron un golpe mortal por parte de Kurt Gödel (1906–1978), quien demostró que siempre existirán problemas "indecidibles" en cualquier sistema axiomático lo suficientemente rico; es decir, en cualquier sistema matemático de alguna importancia, siempre habrá enunciados que no puedan ser demostrados ni refutados.

Como ocurre con frecuencia, esta investigación básica en matemáticas puras posteriormente se volvió indispensable en una amplia gama de aplicaciones. El álgebra Booleana y la lógica se volvieron esenciales en el diseño de circuitos integrados a gra escala que se encuentran en los chips de computadores hoy. Los

sociólogos han usado reticulados y álgebras Booleanas para modelar jerarquías sociales; los biólogos las han usado para dscribir sistemas biológicos.

19.4 Exercises

1. Draw the lattice diagram for the power set of $X = \{a, b, c, d\}$ with the set inclusion relation, $\subset$.

2. Draw the diagram for the set of positive integers that are divisors of 30. Is this poset a Boolean algebra?

3. Draw a diagram of the lattice of subgroups of $\mathbb{Z}_{12}$.

4. Let B be the set of positive integers that are divisors of 36. Define an order on B by $a \preceq b$ if $a \mid b$. Prove that B is a Boolean algebra. Find a set X such that B is isomorphic to $\mathcal{P}(X)$.

5. Prove or disprove: $\mathbb{Z}$ is a poset under the relation $a \preceq b$ if $a \mid b$.

6. Draw the switching circuit for each of the following Boolean expressions.

(a) $(a \vee b \vee a') \wedge a$

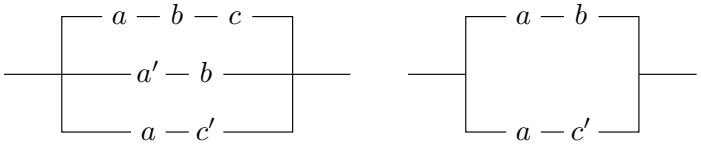
(b) $(a \vee b)' \wedge (a \vee b)$

(c) $a \vee (a \wedge b)$

(d) $(c \vee a \vee b) \wedge c' \wedge (a \vee b)'$

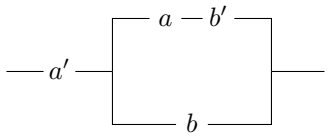
7. Draw a circuit that will be closed exactly when only one of three switches a, b, and c are closed.

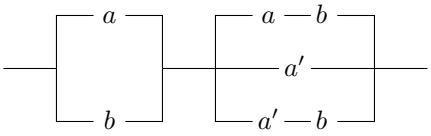
8. Prove or disprove that the two circuits shown are equivalent.

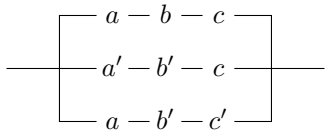


9. Let X be a finite set containing n elements. Prove that $\mathcal{P}(X) = 2^n$. Conclude that the order of any finite Boolean algebra must be 2^n for some $n \in \mathbb{N}$.

10. For each of the following circuits, write a Boolean expression. If the circuit can be replaced by one with fewer switches, give the Boolean expression and draw a diagram for the new circuit.







11. Prove or disprove: The set of all nonzero integers is a lattice, where $a \preceq b$ is defined by $a \mid b$.

12. Let L be a nonempty set with two binary operations $\vee$ and $\wedge$ satisfying the commutative, associative, idempotent, and absorption laws. We can define a partial order on L, as in Theorem 19.14, by $a \preceq b$ if $a \vee b = b$. Prove that the greatest lower bound of a and b is $a \wedge b$.

13. Let G be a group and X be the set of subgroups of G ordered by set-theoretic inclusion. If H and K are subgroups of G, show that the least upper bound of H and K is the subgroup generated by $H \cup K$.

14. Let R be a ring and suppose that X is the set of ideals of R. Show that X is a poset ordered by set-theoretic inclusion, $\subset$. Define the meet of two ideals I and J in X by $I \cap J$ and the join of I and J by $I + J$. Prove that the set of ideals of R is a lattice under these operations.

15. Let B be a Boolean algebra. Prove each of the following identities.

(a) $a \vee I = I$ and $a \wedge O = O$ for all $a \in B$.

(b) If $a \vee b = I$ and $a \wedge b = O$, then $b = a'$.

(c) $(a')' = a$ for all $a \in B$.

(d) $I' = O$ and $O' = I$.

(e) $(a \vee b)' = a' \wedge b'$ and $(a \wedge b)' = a' \vee b'$ (De Morgan's laws).

16. By drawing the appropriate diagrams, complete the proof of Theorem 19.30 to show that the switching functions form a Boolean algebra.

17. Let B be a Boolean algebra. Define binary operations $+$ and $\cdot$ on B by

$$a + b = (a \wedge b') \vee (a' \wedge b)$$
$$a \cdot b = a \wedge b.$$

Prove that B is a commutative ring under these operations satisfying $a^2 = a$ for all $a \in B$.

18. Let X be a poset such that for every a and b in X, either $a \preceq b$ or $b \preceq a$. Then X is said to be a ***totally ordered set***.

(a) Is $a \mid b$ a total order on $\mathbb{N}$?

(b) Prove that $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are totally ordered sets under the usual ordering $\leq$.

19. Let X and Y be posets. A map $\phi : X \to Y$ is ***order-preserving*** if $a \preceq b$ implies that $\phi(a) \preceq \phi(b)$. Let L and M be lattices. A map $\psi : L \to M$ is a ***lattice homomorphism*** if $\psi(a \vee b) = \psi(a) \vee \psi(b)$ and $\psi(a \wedge b) = \psi(a) \wedge \psi(b)$. Show that every lattice homomorphism is order-preserving, but that it is not the case that every order-preserving homomorphism is a lattice homomorphism.

20. Let B be a Boolean algebra. Prove that $a = b$ if and only if $(a \wedge b') \vee (a' \wedge b) = O$ for $a, b \in B$.

21. Let B be a Boolean algebra. Prove that $a = O$ if and only if $(a \wedge b') \vee (a' \wedge b) = b$ for all $b \in B$.

22. Let L and M be lattices. Define an order relation on $L \times M$ by $(a, b) \preceq (c, d)$ if $a \preceq c$ and $b \preceq d$. Show that $L \times M$ is a lattice under this partial order.

19.5 Ejercicios de Programación

1. Una ***Función Booleana*** o ***función de conmutación en*** n ***variables*** es una función $f : \{O, I\}^n \to \{0, I\}$. Un polinomio Booleano es un tipo especial de función Booleana: es cualquier tipo de expresión Booleana formada por una combinación finita de variables $x_1, \ldots, x_n$ junto a O y I, usando las operaciones $\vee$, $\wedge$, y $'$. Los valores de las funciones están definidos en la Tabla 19.33. Escriba un programa para evaluar polinomios Booleanos.

x	y	x'	$x \vee y$	$x \wedge y$
0	0	1	0	0
0	1	1	1	0
1	0	0	1	0
1	1	0	1	1

Cuadro 19.33: Polinomios Booleanos

19.6 Referencias y Lecturas Recomendadas

[1] Donnellan, T. *Lattice Theory.* Pergamon Press, Oxford, 1968.

[2] Halmos, P. R. "The Basic Concepts of Algebraic Logic," *American Mathematical Monthly* **53**(1956), 363–87.

[3] Hohn, F. "Some Mathematical Aspects of Switching," *American Mathematical Monthly* **62**(1955), 75–90.

[4] Hohn, F. *Applied Boolean Algebra.* 2nd ed. Macmillan, New York, 1966.

[5] Lidl, R. and Pilz, G. *Applied Abstract Algebra.* 2nd ed. Springer, New York, 1998.

[6] Whitesitt, J. *Boolean Algebra and Its Applications.* Dover, Mineola, NY, 2010.

19.7 Sage

Sage tiene implementaciones de conjuntos parcialmente ordenados ("posets") y de reticulados, proveyendo representaciones gráficas para ambos.

Creando Conjuntos Parcialmente Ordenados

El Ejemplo 19.6 en el texto, es un buen ejemplo para repetirlo como demostración de comandos Sage. Primero definimos los elementos del conjunto X.

```
X = (24).divisors()
X
```

```
[1, 2, 3, 4, 6, 8, 12, 24]
```

Una posibilidad para crear la relación es especificando *cada* instancia donde un elemento es comparable con otro. Para ello construimos una lista de pares, donde cada par contiene elementos comparables, con el menor primero. Este es el conjunto de relaciones.

```
R = [(a,b) for a in X for b in X if a.divides(b)]; R
```

```
[(1, 1), (1, 2), (1, 3), (1, 4), (1, 6), (1, 8), (1, 12), (1,
    24),
 (2, 2), (2, 4), (2, 6), (2, 8), (2, 12), (2, 24), (3, 3),
     (3, 6),
 (3, 12), (3, 24), (4, 4), (4, 8), (4, 12), (4, 24), (6, 6),
 (6, 12), (6, 24), (8, 8), (8, 24), (12, 12), (12, 24), (24,
     24)]
```

Construimos el poset entregándole al constructor `Poset` una lista con todos los elementos y las relaciones. Luego podemos obtener una visualización del poset. Notemos que el método plot solo muestra las "relaciones de cobertura" — un conjunto minimal de comparaciones que por transitividad permiten recuperar todas las relaciones.

```
D = Poset([X, R])
D.plot()
```

Otra posibilidad para crear un `Poset` es dejar que el constructor de posets recorra todos los pares de elementos, y lo único que le debemos entregar al constructor es una forma de comprobar si dos elementos son comparables. Nuestra función de comparación debe requerir dos elementos y devolver `True` o `False`. Una función "lambda" es una forma de construir una tal función rápidamente. Esta puede ser una idea nueva para usted, pero el dominio de las funciones lambda puede ser muy conveniente. Notemos que "lambda" es una palabra erservada precisamente para este propósito (así, por ejemplo, `lambda` es una elección prohibida para el valor propio de una matriz). Hay otras maneras de definir funciones en Sage, pero una función lambda es lo más rápido cuando la función es simple.

```
divisible = lambda x, y: x.divides(y)
L = Poset([X, divisible])
L == D
```

```
True
```

```
L.plot()
```

Sage ya tiene una colección de posets. Algunos se construyen directamente, mientras otros pertenecen a familias parametrizadas. Use completación con TAB en `Posets.` para ver la lista completa. Acá hay algunos ejemplo.

```
Q = Posets.PentagonPoset()
Q.plot()
```

Ahora una familia parametrizada. Este es un ejemplo clásico donde los elementos son subconjuntos de un conjunto de n elementos y la relación es "subconjunto de."

```
S = Posets.BooleanLattice(4)
S.plot()
```

Y posets aleatorios. Estos pueden ser útiles para experimentos o comprobciones, pero es poco probable que aparezcan con propiedades especiales que pueden ser importantes. Puede intentar el siguiente comando varias veces, variando el segundo argumento que es una cota superior para la probabilidad de que dos elementos cualquiera sean comparables. Recuerde que plot solo muestra las relaciones de cobertura. Mientras más elementos comparables haya, más "estirado verticalmente" será el gráfico.

```
T = Posets.RandomPoset(20,0.05)
T.plot()
```

Propiedades de un Poset

Una vez que tenemos un poset, ¿qué podemos hacer con él? Volvamos a nuestro primer ejemplo, `D`. Por supuesto podemos determinar si un elemento es menor a otro, que es la estructura fundamental de un poset.

```
D.is_lequal(4, 8)
```

```
True
```

```
D.is_lequal(4, 4)
```

```
True
```

```
D.is_less_than(4, 8)
```

```
True
```

```
D.is_less_than(4, 4)
```

```
False
```

```
D.is_lequal(6, 8)
```

```
False
```

```
D.is_lequal(8, 6)
```

```
False
```

Notemos que `6` y `8` no son comparables en este poset (es un orden *parcial*). Los métodos `.is_gequal()` y `.is_greater_than()` funcionan de forma similar, pero devuelven `True` si el primer eleemento es mayor (o igual).

```
D.is_gequal(8, 4)
```

```
True
```

```
D.is_greater_than(4, 8)
```

```
False
```

Podemo encontrar elementos maximales o minimales de un poset. Este es un poset aleatorio construido con una probabilidad de 10%, pero copiado acá para ser repetible.

```
X = range(20)
C = [[18, 7],  [9, 11], [9, 10], [11, 8], [6, 10],
     [10, 2],   [0, 2],  [2, 1],  [1, 8], [8, 12],
     [8, 3],  [3, 15], [15, 7], [7, 16],  [7, 4],
     [16, 17], [16, 13], [4, 19], [4, 14], [14, 5]]
P = Poset([X, C])
P.plot()
```

```
P.minimal_elements()
```

```
[18, 9, 6, 0]
```

```
P.maximal_elements()
```

```
[5, 19, 13, 17, 12]
```

Los elementos de un poset pueden ser particionados en conjuntos de nivel. En las gráficas de los posets, los elementos del mismo nivel se muestran a la misma altura. Cada leverl se obtiene removiendo todos los elementos de los niveles anteriores y escogiendo los elementos minimales del resultado.

```
P.level_sets()
```

```
[[18, 9, 6, 0], [11, 10], [2], [1], [8], [3, 12],
 [15], [7], [16, 4], [13, 17, 14, 19], [5]]
```

Si hacemos que dos elementos de `R` sean comparables cuando antes no lo eran, eso constituye una extensión de `R`. Consideremos todas las posibles extensiones de un one poset — podemos construir un poset a partir de tas ellas, donde la relación es la de inclusión conjuntista. Una extensión lineal es un elemento maximal en este poset de posets. Informalmente, estamos agregando tantas relaciones como sea posible, de manera consistente con el poset original y tal que el resultado es un orden total. En otras palabra, hay un orden de los elementos que es consistente con el orden en el poset. Podemos construir una cosa así, pero la salida no es mñas que una lista de elementos en el orden lineal. Un informático se inclinaría por llamar a esto un "ordenamiento topológico."

```
linear = P.linear_extension(); linear
```

```
[18, 9, 11, 6, 10, 0, 2, 1, 8, 3, 15,
 7, 4, 14, 5, 19, 16, 13, 17, 12]
```

Podemos construir subposets a partir de un subconjunto de los elementos con el orden inducido para producir un poset nuevo. Acá tomamo aproximadamente la "mitad inferior" de poset aleatorio `P` induciendo el subposet en Íla unión de algunos de los conjuntos de nivel.

```
level = P.level_sets()
bottomhalf = sum([level[i] for i in range(5)], [])
B = P.subposet(bottomhalf)
B.plot()
```

El dual de un poset mantiene todos sus elementos e invierte sus comparaciones.

```
Pdual = P.dual()
Pdual.plot()
```

El dual del poset de divisibilidad del Ejemplo 19.6 es como cambiar la relación por "es múltiplo de."

```
Ddual = D.dual()
Ddual.plot()
```

Reticulados

Cada reticulado es poset, de manera que todos los comandos de arriba funcionan igualmente bien para un reticulado. Pero, ¿cómo se construye un reticulado? Fácil — primero creamos un poset y luego lo pasamos al constructor `LatticePoset()`. Pero nos daremos cuenta que simplemente por darle un poset a este constructor, no significa que lo que salga sea un reticulado. Solo si el poset *ya es* un reticulado el resultado será un reticulado para Sage y obtendremos el error `ValueError` si el cambio de estatus es imposible. Finalmente, notemos que algunos de los posets que construye Sage ya son reconocidos como reticulados, tal como el prototípico `BooleanLattice`.

```
P = Posets.AntichainPoset(8)
P.is_lattice()
```

```
False
```

```
LatticePoset(P)
```

```
Traceback (most recent call last):
...
ValueError: not a meet-semilattice: no bottom element
```

Una composición entera de n es una lista de enteros positivos que suman n. Una composición C_1 cubre a una composición C_2 si C_2 se puede formar a partir de C_1 sumando partes consecutivas. Por ejemplo, $C_1 = [2, 1, 2] \succeq [3, 2] = C_2$. Con esta relación, el conjunto de todas las composiciones enteras de un entero fijo n en un poset que también es un reticulado.

```
CP = Posets.IntegerCompositions(5)
C = LatticePoset(CP)
C.plot()
```

El ínfimo (meet) y el supremo (join) son operaciones fundamentales en un reticulado.

```
par = C.an_element().parent()
a = par([1, 1, 1, 2])
b = par([2, 1, 1, 1])
a, b
```

```
([1, 1, 1, 2], [2, 1, 1, 1])
```

```
C.meet(a, b)
```

```
[2, 1, 2]
```

```
c = par([1, 4])
d = par([2, 3])
c, d
```

```
([1, 4], [2, 3])
```

```
C.join(c, d)
```

```
[1, 1, 3]
```

Una vez que un poset adquiere el estatus de reticulado, disponemos de comandos adicionales, o cambian las características de sus resultados.

Un ejemplo de lo primero es el método `.is_distributive()`.

```
C.is_distributive()
```

```
True
```

Un ejemplo de lo segundo es el método `.top()`. Lo que en el texto se llama elemento máximo y elemento mínimo, Sage los llama top y bottom. Para un poset, `.top()` y `.bottom()` pueden entregar un elemento o no (devolviendo `None`), pero para un reticulado se garantiza la obtención de exactamente un elemento.

```
C.top()
```

```
[1, 1, 1, 1, 1]
```

```
C.bottom()
```

```
[5]
```

Notemos que los valores retornados son todos elementos del reticulado, es este caso listas ordenadas de enteros que suman 5.

Los complementos tienen sentido en un reticulado. El resultado del método `.complements()` es un diccionario que tiene elementos del reticulado como índices (keys). Decimos que el diccionario está "indexado" por los elementos del reticulado. El resultado es una lista de complementos del elemento. A esto lo llamamos el "valor" del par índice-valor. (Puede que conozca los diccionarios como "arreglos asociativos", pero en realidad no son más que funciones sofisticadas.)

```
comp = C.complements()
comp[par([1, 1, 1, 2])]
```

```
[[4, 1]]
```

El reticulado de composiciones enteras es un reticulado complementado, como podemos observar por el hecho de que cada elemento tiene un complemento único, evidenciado por las listas de largo 1 en los valores del diccionario. O podemos preguntarle a Sage por medio de `.is_complemented()`. Los diccionarios no tienen un orden inherente, de manera que es posible obtener una salida distinta cada vez que se inspeccione el diccionario.

```
comp
```

```
{[1, 1, 1, 1, 1]: [[5]],
 [1, 1, 1, 2]: [[4, 1]],
 [1, 1, 2, 1]: [[3, 2]],
 [1, 1, 3]: [[3, 1, 1]],
 [1, 2, 1, 1]: [[2, 3]],
 [1, 2, 2]: [[2, 2, 1]],
 [1, 3, 1]: [[2, 1, 2]],
 [1, 4]: [[2, 1, 1, 1]],
 [2, 1, 1, 1]: [[1, 4]],
 [2, 1, 2]: [[1, 3, 1]],
 [2, 2, 1]: [[1, 2, 2]],
 [2, 3]: [[1, 2, 1, 1]],
 [3, 1, 1]: [[1, 1, 3]],
 [3, 2]: [[1, 1, 2, 1]],
 [4, 1]: [[1, 1, 1, 2]],
 [5]: [[1, 1, 1, 1, 1]]}
```

```
[len(e[1]) for e in comp.items()]
```

```
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
```

```
C.is_complemented()
```

```
True
```

Hay muchos más comandos para posets y erticulados. Construya algunos y use completación con TAB para explorar las posibilidades. Hay mucho más de lo que podemos cubrir en un solo capítulo, pero ya tenemos las herramientas básicas para estudiar posets y reticulados en Sage.

19.8 Ejercicios en Sage

1. Use `R = Posets.RandomPoset(30,0.05)` para construir on conjunto parcialmente ordenado (poset) aleatorio. Use `R.plot()` para tener una idea de lo que ubtuvo.

(a) Ilustre el uso de los siguientes métodos de poset: `.is_lequal()`, `.is_less_than()`, `.is_gequal()`, and `.is_greater_than()` para determinar si dos elementos específicos (de su elección) están relacionados o son incomparables.

(b) Use `.minimal_elements()` y `.maximal_elements()` para encontrar tanto el menor como el mayor elemento de su poset.

(c) Use `LatticePoset(R)` para ver si el poset `R` es un reticulado intentando convertirlo en un reticulado.

(d) Encuentre una extensión lineal de su poset. Confirme que cualquier par de elementos comparables en en poset original siguen siendo comparables de la misma forma en la extensión lineal.

2. Construya el poset en los divisores enteros de $72 = 2^3 \cdot 3^2$ con la relación de divisibilidad, y conviértalo en un reticulado.

(a) Determine el elemento cero y el elemento uno usando `.top()` y `.bottom()`.

(b) Determine todos los pares de elementos del reticulado que son complementarios *sin* usar el método `.complement()`, sino solamente los métodos `.meet()` y `.join()`. Mejor si cada par aparece solo una vez.

(c) Determine si el reticulado es distributivo usando solo los métodos `.meet()` and `.join()`, y no el método `.is_distributive()`.

3. Construya varios reticulados diamante con `Posets.DiamondPoset(n)` haciendo variar el valor de `n`. Una vez que le parezca tener suficiente evidencia empírica, responda, con justificaciones, las siguientes preguntas para valores *arbitrarios* de n, basado en observaciones obtenidas de sus experimentos con Sage.

(a) ¿Cuáles son los elementos que tienen complemento y cuáles no lo tienen? ¿Por qué?

(b) Lea la documentación del método `.antichains()` para aaprender lo que es una anticadena. ¿Cuántas anticadenas hay?

(c) ¿Es distributivo el reticulado?

4. Use `Posets.BooleanLattice(4)` para construir una instancia del álgebra Booleana prototípica en 16 elementos (i.e., todos los subconjuntos de un conjunto de 4 elementos).
Luego use `Posets.IntegerCompositions(5)` para construir el poset cuyos 16 elementos son las composiciones del entero 5. Vimos arriba que el reticulado de composición de entero es distributivo y complementado, por lo que forma un álgbera Booleana. Por el Teorema 19.23 podemos concluir que esta dos álgebras Booleanas son isomorfas.
Use el método `.plot()` para visualizar la similaridad. Luego use el método `.hasse_diagram()` en cada reticulado para obtener un grafo dirigido (que también puede dibujar, aunque la incrustación en el plano puede que no sea tan informativa). Emplee el método `.is_isomorphic()` del grafo para verificar que estos dos diagramas de Hasse son realmente "iguales."

5. (Avanzado) Para la pregunta anterior, construya on isomorfismo *explícito* entre las dos álgebras Booleanas. Esto es una biyección (construída con el comando `def`) que convierta composiciones en conjuntos (oo si lo prefiere, conjuntos en composiciones) y que respete las operaciones de ínfimo y supremo (meet y join). Puede poner a prueba e ilustrar su función por su interacción con elementos específicos evaluados en las operaciones de ínfimo y supremo, como está descrito en la definición de isomorfismo de álgebras Boleanas.

20

Vector Spaces

In a physical system a quantity can often be described with a single number. For example, we need to know only a single number to describe temperature, mass, or volume. However, for some quantities, such as location, we need several numbers. To give the location of a point in space, we need x, y, and z coordinates. Temperature distribution over a solid object requires four numbers: three to identify each point within the object and a fourth to describe the temperature at that point. Often n-tuples of numbers, or vectors, also have certain algebraic properties, such as addition or scalar multiplication.

In this chapter we will examine mathematical structures called vector spaces. As with groups and rings, it is desirable to give a simple list of axioms that must be satisfied to make a set of vectors a structure worth studying.

20.1 Definitions and Examples

A ***vector space*** V over a field F is an abelian group with a ***scalar product*** $\alpha \cdot v$ or αv defined for all $\alpha \in F$ and all $v \in V$ satisfying the following axioms.

- $\alpha(\beta v) = (\alpha\beta)v$;
- $(\alpha + \beta)v = \alpha v + \beta v$;
- $\alpha(u + v) = \alpha u + \alpha v$;
- $1v = v$;

where $\alpha, \beta \in F$ and $u, v \in V$.

The elements of V are called ***vectors***; the elements of F are called ***scalars***. It is important to notice that in most cases two vectors cannot be multiplied. In general, it is only possible to multiply a vector with a scalar. To differentiate between the scalar zero and the vector zero, we will write them as 0 and $\mathbf{0}$, respectively.

Let us examine several examples of vector spaces. Some of them will be quite familiar; others will seem less so.

Ejemplo 20.1. The n-tuples of real numbers, denoted by $\mathbb{R}^n$, form a vector space over $\mathbb{R}$. Given vectors $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ in $\mathbb{R}^n$ and α in $\mathbb{R}$, we can define vector addition by

$$u + v = (u_1, \ldots, u_n) + (v_1, \ldots, v_n) = (u_1 + v_1, \ldots, u_n + v_n)$$

and scalar multiplication by

$$\alpha u = \alpha(u_1, \ldots, u_n) = (\alpha u_1, \ldots, \alpha u_n).$$

Ejemplo 20.2. If F is a field, then $F[x]$ is a vector space over F. The vectors in $F[x]$ are simply polynomials, and vector addition is just polynomial addition. If $\alpha \in F$ and $p(x) \in F[x]$, then scalar multiplication is defined by $\alpha p(x)$.

Ejemplo 20.3. The set of all continuous real-valued functions on a closed interval $[a, b]$ is a vector space over $\mathbb{R}$. If $f(x)$ and $g(x)$ are continuous on $[a, b]$, then $(f + g)(x)$ is defined to be $f(x) + g(x)$. Scalar multiplication is defined by $(\alpha f)(x) = \alpha f(x)$ for $\alpha \in \mathbb{R}$. For example, if $f(x) = \sin x$ and $g(x) = x^2$, then $(2f + 5g)(x) = 2 \sin x + 5x^2$.

Ejemplo 20.4. Let $V = \mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Then V is a vector space over $\mathbb{Q}$. If $u = a + b\sqrt{2}$ and $v = c + d\sqrt{2}$, then $u + v = (a + c) + (b + d)\sqrt{2}$ is again in V. Also, for $\alpha \in \mathbb{Q}$, αv is in V. We will leave it as an exercise to verify that all of the vector space axioms hold for V.

Proposición 20.5. *Let V be a vector space over F. Then each of the following statements is true.*

1. $0v = \mathbf{0}$ *for all* $v \in V$.
2. $\alpha\mathbf{0} = \mathbf{0}$ *for all* $\alpha \in F$.
3. *If* $\alpha v = \mathbf{0}$, *then either* $\alpha = 0$ *or* $v = \mathbf{0}$.
4. $(-1)v = -v$ *for all* $v \in V$.
5. $-(\alpha v) = (-\alpha)v = \alpha(-v)$ *for all* $\alpha \in F$ *and all* $v \in V$.

DEMOSTRACIÓN. To prove (1), observe that

$$0v = (0 + 0)v = 0v + 0v;$$

consequently, $\mathbf{0} + 0v = 0v + 0v$. Since V is an abelian group, $\mathbf{0} = 0v$.

The proof of (2) is almost identical to the proof of (1). For (3), we are done if $\alpha = 0$. Suppose that $\alpha \neq 0$. Multiplying both sides of $\alpha v = \mathbf{0}$ by $1/\alpha$, we have $v = \mathbf{0}$.

To show (4), observe that

$$v + (-1)v = 1v + (-1)v = (1 - 1)v = 0v = \mathbf{0},$$

and so $-v = (-1)v$. We will leave the proof of (5) as an exercise. □

20.2 Subspaces

Just as groups have subgroups and rings have subrings, vector spaces also have substructures. Let V be a vector space over a field F, and W a subset of V. Then W is a ***subspace*** of V if it is closed under vector addition and scalar multiplication; that is, if $u, v \in W$ and $\alpha \in F$, it will always be the case that $u + v$ and αv are also in W.

Ejemplo 20.6. Let W be the subspace of $\mathbb{R}^3$ defined by $W = \{(x_1, 2x_1 + x_2, x_1 - x_2) : x_1, x_2 \in \mathbb{R}\}$. We claim that W is a subspace of $\mathbb{R}^3$. Since

$$\begin{aligned}\alpha(x_1, 2x_1 + x_2, x_1 - x_2) &= (\alpha x_1, \alpha(2x_1 + x_2), \alpha(x_1 - x_2)) \\ &= (\alpha x_1, 2(\alpha x_1) + \alpha x_2, \alpha x_1 - \alpha x_2),\end{aligned}$$

W is closed under scalar multiplication. To show that W is closed under vector addition, let $u = (x_1, 2x_1 + x_2, x_1 - x_2)$ and $v = (y_1, 2y_1 + y_2, y_1 - y_2)$ be vectors in W. Then

$$u + v = (x_1 + y_1, 2(x_1 + y_1) + (x_2 + y_2), (x_1 + y_1) - (x_2 + y_2)).$$

Ejemplo 20.7. Let W be the subset of polynomials of $F[x]$ with no odd-power terms. If $p(x)$ and $q(x)$ have no odd-power terms, then neither will $p(x)+q(x)$. Also, $\alpha p(x) \in W$ for $\alpha \in F$ and $p(x) \in W$.

Let V be any vector space over a field F and suppose that $v_1, v_2, \ldots, v_n$ are vectors in V and $\alpha_1, \alpha_2, \ldots, \alpha_n$ are scalars in F. Any vector w in V of the form

$$w = \sum_{i=1}^{n} \alpha_i v_i = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

is called a ***linear combination*** of the vectors $v_1, v_2, \ldots, v_n$. The ***spanning set*** of vectors $v_1, v_2, \ldots, v_n$ is the set of vectors obtained from all possible linear combinations of $v_1, v_2, \ldots, v_n$. If W is the spanning set of $v_1, v_2, \ldots, v_n$, then we say that W is ***spanned*** by $v_1, v_2, \ldots, v_n$.

Proposición 20.8. *Let $S = \{v_1, v_2, \ldots, v_n\}$ be vectors in a vector space V. Then the span of S is a subspace of V.*

Demostración. Let u and v be in S. We can write both of these vectors as linear combinations of the v_i's:

$$u = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$
$$v = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n.$$

Then

$$u + v = (\alpha_1 + \beta_1) v_1 + (\alpha_2 + \beta_2) v_2 + \cdots + (\alpha_n + \beta_n) v_n$$

is a linear combination of the v_i's. For $\alpha \in F$,

$$\alpha u = (\alpha\alpha_1) v_1 + (\alpha\alpha_2) v_2 + \cdots + (\alpha\alpha_n) v_n$$

is in the span of S. □

20.3 Linear Independence

Let $S = \{v_1, v_2, \ldots, v_n\}$ be a set of vectors in a vector space V. If there exist scalars $\alpha_1, \alpha_2 \ldots \alpha_n \in F$ such that not all of the α_i's are zero and

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \mathbf{0},$$

then S is said to be ***linearly dependent***. If the set S is not linearly dependent, then it is said to be ***linearly independent***. More specifically, S is a linearly independent set if

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \mathbf{0}$$

implies that

$$\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$$

for any set of scalars $\{\alpha_1, \alpha_2 \ldots \alpha_n\}$.

Proposición 20.9. *Let $\{v_1, v_2, \ldots, v_n\}$ be a set of linearly independent vectors in a vector space. Suppose that*

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n.$$

Then $\alpha_1 = \beta_1, \alpha_2 = \beta_2, \ldots, \alpha_n = \beta_n$.

DEMOSTRACIÓN. If

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n,$$

then

$$(\alpha_1 - \beta_1)v_1 + (\alpha_2 - \beta_2)v_2 + \cdots + (\alpha_n - \beta_n)v_n = \mathbf{0}.$$

Since $v_1, \ldots, v_n$ are linearly independent, $\alpha_i - \beta_i = 0$ for $i = 1, \ldots, n$. □

The definition of linear dependence makes more sense if we consider the following proposition.

Proposición 20.10. *A set $\{v_1, v_2, \ldots, v_n\}$ of vectors in a vector space V is linearly dependent if and only if one of the v_i's is a linear combination of the rest.*

DEMOSTRACIÓN. Suppose that $\{v_1, v_2, \ldots, v_n\}$ is a set of linearly dependent vectors. Then there exist scalars $\alpha_1, \ldots, \alpha_n$ such that

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \mathbf{0},$$

with at least one of the α_i's not equal to zero. Suppose that $\alpha_k \neq 0$. Then

$$v_k = -\frac{\alpha_1}{\alpha_k} v_1 - \cdots - \frac{\alpha_{k-1}}{\alpha_k} v_{k-1} - \frac{\alpha_{k+1}}{\alpha_k} v_{k+1} - \cdots - \frac{\alpha_n}{\alpha_k} v_n.$$

Conversely, suppose that

$$v_k = \beta_1 v_1 + \cdots + \beta_{k-1} v_{k-1} + \beta_{k+1} v_{k+1} + \cdots + \beta_n v_n.$$

Then

$$\beta_1 v_1 + \cdots + \beta_{k-1} v_{k-1} - v_k + \beta_{k+1} v_{k+1} + \cdots + \beta_n v_n = \mathbf{0}.$$ □

The following proposition is a consequence of the fact that any system of homogeneous linear equations with more unknowns than equations will have a nontrivial solution. We leave the details of the proof for the end-of-chapter exercises.

Proposición 20.11. *Suppose that a vector space V is spanned by n vectors. If $m > n$, then any set of m vectors in V must be linearly dependent.*

A set $\{e_1, e_2, \ldots, e_n\}$ of vectors in a vector space V is called a ***basis*** for V if $\{e_1, e_2, \ldots, e_n\}$ is a linearly independent set that spans V.

Ejemplo 20.12. The vectors $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, and $e_3 = (0, 0, 1)$ form a basis for $\mathbb{R}^3$. The set certainly spans $\mathbb{R}^3$, since any arbitrary vector (x_1, x_2, x_3) in $\mathbb{R}^3$ can be written as $x_1 e_1 + x_2 e_2 + x_3 e_3$. Also, none of the vectors e_1, e_2, e_3 can be written as a linear combination of the other two; hence, they are linearly independent. The vectors e_1, e_2, e_3 are not the only basis of $\mathbb{R}^3$: the set $\{(3, 2, 1), (3, 2, 0), (1, 1, 1)\}$ is also a basis for $\mathbb{R}^3$.

Ejemplo 20.13. Let $\mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. The sets $\{1, \sqrt{2}\,\}$ and $\{1 + \sqrt{2}, 1 - \sqrt{2}\,\}$ are both bases of $\mathbb{Q}(\sqrt{2}\,)$.

From the last two examples it should be clear that a given vector space has several bases. In fact, there are an infinite number of bases for both of these examples. *In general, there is no unique basis for a vector space.* However, every basis of $\mathbb{R}^3$ consists of exactly three vectors, and every basis of $\mathbb{Q}(\sqrt{2}\,)$ consists of exactly two vectors. This is a consequence of the next proposition.

Proposición 20.14. *Let $\{e_1, e_2, \ldots, e_m\}$ and $\{f_1, f_2, \ldots, f_n\}$ be two bases for a vector space V. Then $m = n$.*

DEMOSTRACIÓN. Since $\{e_1, e_2, \ldots, e_m\}$ is a basis, it is a linearly independent set. By Proposition 20.11, $n \leq m$. Similarly, $\{f_1, f_2, \ldots, f_n\}$ is a linearly independent set, and the last proposition implies that $m \leq n$. Consequently, $m = n$. □

If $\{e_1, e_2, \ldots, e_n\}$ is a basis for a vector space V, then we say that the ***dimension*** of V is n and we write $\dim V = n$. We will leave the proof of the following theorem as an exercise.

Teorema 20.15. *Let V be a vector space of dimension n.*

1. *If $S = \{v_1, \ldots, v_n\}$ is a set of linearly independent vectors for V, then S is a basis for V.*
2. *If $S = \{v_1, \ldots, v_n\}$ spans V, then S is a basis for V.*
3. *If $S = \{v_1, \ldots, v_k\}$ is a set of linearly independent vectors for V with $k < n$, then there exist vectors $v_{k+1}, \ldots, v_n$ such that*

$$\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$$

is a basis for V.

Sage Muchos de los cálculos en Sage, en diversos contextos algebraicos, se basan en resolver problemas de álgebra lineal. Por esta razón la funcionalidad de Sage relativa al álgebra lineal es extensa. Más aún, se pueden usar estructura como cuerpos finitos, para encontrar espacios vectoriales en nuevos contextos.

20.4 Exercises

1. If F is a field, show that $F[x]$ is a vector space over F, where the vectors in $F[x]$ are polynomials. Vector addition is polynomial addition, and scalar multiplication is defined by $\alpha p(x)$ for $\alpha \in F$.

2. Prove that $\mathbb{Q}(\sqrt{2}\,)$ is a vector space.

3. Let $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,)$ be the field generated by elements of the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, where a, b, c, d are in $\mathbb{Q}$. Prove that $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,)$ is a vector space of dimension 4 over $\mathbb{Q}$. Find a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,)$.

4. Prove that the complex numbers are a vector space of dimension 2 over $\mathbb{R}$.

5. Prove that the set P_n of all polynomials of degree less than n form a subspace of the vector space $F[x]$. Find a basis for P_n and compute the dimension of P_n.

6. Let F be a field and denote the set of n-tuples of F by F^n. Given vectors $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ in F^n and α in F, define vector addition by

$$u + v = (u_1, \ldots, u_n) + (v_1, \ldots, v_n) = (u_1 + v_1, \ldots, u_n + v_n)$$

and scalar multiplication by

$$\alpha u = \alpha(u_1, \ldots, u_n) = (\alpha u_1, \ldots, \alpha u_n).$$

Prove that F^n is a vector space of dimension n under these operations.

7. Which of the following sets are subspaces of $\mathbb{R}^3$? If the set is indeed a subspace, find a basis for the subspace and compute its dimension.

(a) $\{(x_1, x_2, x_3) : 3x_1 - 2x_2 + x_3 = 0\}$

(b) $\{(x_1, x_2, x_3) : 3x_1 + 4x_3 = 0, 2x_1 - x_2 + x_3 = 0\}$

(c) $\{(x_1, x_2, x_3) : x_1 - 2x_2 + 2x_3 = 2\}$

(d) $\{(x_1, x_2, x_3) : 3x_1 - 2x_2^2 = 0\}$

8. Show that the set of all possible solutions $(x, y, z) \in \mathbb{R}^3$ of the equations

$$\begin{aligned} Ax + By + Cz &= 0 \\ Dx + Ey + Cz &= 0 \end{aligned}$$

form a subspace of $\mathbb{R}^3$.

9. Let W be the subset of continuous functions on $[0, 1]$ such that $f(0) = 0$. Prove that W is a subspace of $C[0, 1]$.

10. Let V be a vector space over F. Prove that $-(\alpha v) = (-\alpha)v = \alpha(-v)$ for all $\alpha \in F$ and all $v \in V$.

11. Let V be a vector space of dimension n. Prove each of the following statements.

(a) If $S = \{v_1, \ldots, v_n\}$ is a set of linearly independent vectors for V, then S is a basis for V.

(b) If $S = \{v_1, \ldots, v_n\}$ spans V, then S is a basis for V.

(c) If $S = \{v_1, \ldots, v_k\}$ is a set of linearly independent vectors for V with $k < n$, then there exist vectors $v_{k+1}, \ldots, v_n$ such that

$$\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$$

is a basis for V.

12. Prove that any set of vectors containing $\mathbf{0}$ is linearly dependent.

13. Let V be a vector space. Show that $\{\mathbf{0}\}$ is a subspace of V of dimension zero.

14. If a vector space V is spanned by n vectors, show that any set of m vectors in V must be linearly dependent for $m > n$.

15. (Linear Transformations) Let V and W be vector spaces over a field F, of dimensions m and n, respectively. If $T : V \to W$ is a map satisfying

$$\begin{aligned} T(u + v) &= T(u) + T(v) \\ T(\alpha v) &= \alpha T(v) \end{aligned}$$

for all $\alpha \in F$ and all $u, v \in V$, then T is called a ***linear transformation*** from V into W.

(a) Prove that the ***kernel*** of T, $\ker(T) = \{v \in V : T(v) = \mathbf{0}\}$, is a subspace of V. The kernel of T is sometimes called the ***null space*** of T.

(b) Prove that the ***range*** or ***range space*** of T, $R(V) = \{w \in W : T(v) = w \text{ for some } v \in V\}$, is a subspace of W.

(c) Show that $T : V \to W$ is injective if and only if $\ker(T) = \{\mathbf{0}\}$.

(d) Let $\{v_1, \ldots, v_k\}$ be a basis for the null space of T. We can extend this basis to be a basis $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_m\}$ of V. Why? Prove that $\{T(v_{k+1}), \ldots, T(v_m)\}$ is a basis for the range of T. Conclude that the range of T has dimension $m - k$.

(e) Let $\dim V = \dim W$. Show that a linear transformation $T : V \to W$ is injective if and only if it is surjective.

16. Let V and W be finite dimensional vector spaces of dimension n over a field F. Suppose that $T : V \to W$ is a vector space isomorphism. If $\{v_1, \ldots, v_n\}$ is a basis of V, show that $\{T(v_1), \ldots, T(v_n)\}$ is a basis of W. Conclude that any vector space over a field F of dimension n is isomorphic to F^n.

17. (Direct Sums) Let U and V be subspaces of a vector space W. The sum of U and V, denoted $U + V$, is defined to be the set of all vectors of the form $u + v$, where $u \in U$ and $v \in V$.

(a) Prove that $U + V$ and $U \cap V$ are subspaces of W.

(b) If $U + V = W$ and $U \cap V = \mathbf{0}$, then W is said to be the ***direct sum.*** In this case, we write $W = U \oplus V$. Show that every element $w \in W$ can be written uniquely as $w = u + v$, where $u \in U$ and $v \in V$.

(c) Let U be a subspace of dimension k of a vector space W of dimension n. Prove that there exists a subspace V of dimension $n - k$ such that $W = U \oplus V$. Is the subspace V unique?

(d) If U and V are arbitrary subspaces of a vector space W, show that

$$\dim(U + V) = \dim U + \dim V - \dim(U \cap V).$$

18. (Dual Spaces) Let V and W be finite dimensional vector spaces over a field F.

(a) Show that the set of all linear transformations from V into W, denoted by $\mathrm{Hom}(V, W)$, is a vector space over F, where we define vector addition as follows:

$$(S + T)(v) = S(v) + T(v)$$
$$(\alpha S)(v) = \alpha S(v),$$

where $S, T \in \mathrm{Hom}(V, W)$, $\alpha \in F$, and $v \in V$.

(b) Let V be an F-vector space. Define the ***dual space*** of V to be $V^* = \mathrm{Hom}(V, F)$. Elements in the dual space of V are called ***linear functionals.*** Let $v_1, \ldots, v_n$ be an ordered basis for V. If $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ is any vector in V, define a linear functional $\phi_i : V \to F$ by $\phi_i(v) = \alpha_i$. Show that the ϕ_i's form a basis for V^*. This basis is called the ***dual basis*** of $v_1, \ldots, v_n$ (or simply the dual basis if the context makes the meaning clear).

(c) Consider the basis $\{(3, 1), (2, -2)\}$ for $\mathbb{R}^2$. What is the dual basis for $(\mathbb{R}^2)^*$?

(d) Let V be a vector space of dimension n over a field F and let V^{**} be the dual space of V^*. Show that each element $v \in V$ gives rise to an element λ_v in V^{**} and that the map $v \mapsto \lambda_v$ is an isomorphism of V with V^{**}.

20.5 References and Suggested Readings

[1] Beezer, R. *A First Course in Linear Algebra*. Available online at http://linear.ups.edu/. 2004–2014.

[2] Bretscher, O. *Linear Algebra with Applications*. 4th ed. Pearson, Upper Saddle River, NJ, 2009.

[3] Curtis, C. W. *Linear Algebra: An Introductory Approach*. 4th ed. Springer, New York, 1984.

[4] Hoffman, K. and Kunze, R. *Linear Algebra*. 2nd ed. Prentice-Hall, Englewood Cliffs, NJ, 1971.

[5] Johnson, L. W., Riess, R. D., and Arnold, J. T. *Introduction to Linear Algebra*. 6th ed. Pearson, Upper Saddle River, NJ, 2011.

[6] Leon, S. J. *Linear Algebra with Applications*. 8th ed. Pearson, Upper Saddle River, NJ, 2010.

20.6 Sage

Muchos cálculos, en áreas aparentemente muy diversas de las matemáticas, se pueden traducir en preguntas sobre combinaciones lineales, u otras áreas de álgebra lineal. Por ende Sage tiene una extensa e importante implementación de tópicos como los espacios vectoriales.

Espacios Vectoriales

La forma más simple de crear u espacio vectorial es comenzando con un cuerpo y usando un exponente para indicar el número de coordenadas de los vectores en el espacio.

```
V = QQ^4; V
```

```
Vector space of dimension 4 over Rational Field
```

```
F.<a> = FiniteField(3^4)
W = F^5; W
```

```
Vector space of dimension 5 over Finite Field in a of size 3^4
```

Los elementos pueden ser obtenidos con el constructor de vectores.

```
v = vector(QQ, [1, 1/2, 1/3, 1/4]); v
```

```
(1, 1/2, 1/3, 1/4)
```

```
v in V
```

```
True
```

```
w = vector(F, [1, a^2, a^4, a^6, a^8]); w
```

```
(1, a^2, a^3 + 1, a^3 + a^2 + a + 1, a^2 + a + 2)
```

```
w in W
```

```
True
```

Notemos que los vectores se muestran con paréntesis, lo que ayuda a distinguirlos de las listas (pero se ven como tuplas). Los vectores se despliegan horizontalmente, pues en Sage no existe la distinción entre "vector fila" y "vector columna", pero una vez que aparezcan las matrices deberemos preocuparnos de esta distinción. Finalmente, notemos cómo los elementos del cuerpo finito han sido convertidos a una representación diferente.

Una vez que tenemos espacios vectoriales llenos de vectores, podemos hacer cálculos con ellos. En última instancia, toda la acción en un espacio vectorial se reduce a suma de vectores y multiplicación por escalares, que juntas crean combinaciones lineales.

```
u = vector(QQ, [ 1, 2,  3, 4,   5,  6])
v = vector(QQ, [-1, 2, -4, 8, -16, 32])
3*u - 2*v
```

```
(5, 2, 17, -4, 47, -46)
```

```
w = vector(F, [1, a^2, a^4, a^6,  a^8])
x = vector(F, [1,   a, 2*a,   a,    1])
y = vector(F, [1, a^3, a^6, a^9, a^12])
a^25*w + a^43*x + a^66*y
```

```
(a^3 + a^2 + a + 2, a^2 + 2*a, 2*a^3 + a^2 + 2, 2*a^3 + a^2 +
    a,
 a^3 + 2*a^2 + a + 2)
```

Subespacios

Sage puede crear subespacios de diferentes formas, tales como en la craci´on de los espacios de columnas o de filas de matrices. Pero la forma más directa es comenzar con un conjunto de vectores y usarlos como conjunto generador.

```
u = vector(QQ, [1, -1, 3])
v = vector(QQ, [2, 1, -1])
w = vector(QQ, [3, 0, 2])
S = (QQ^3).subspace([u, v, w]); S
```

```
Vector space of degree 3 and dimension 2 over Rational Field
Basis matrix:
[   1    0  2/3]
[   0    1 -7/3]
```

```
3*u - 6*v + (1/2)*w in S
```

```
True
```

```
vector(QQ, [4, -1, -2]) in S
```

```
False
```

Notemos que la información mostrada sobre `S` incluye una "matriz base." Las filas de esta matriz forman una base del espacio vectorial. Podemos ubtener la base, como una lista de vectores (no como filas de una matriz), con el método `.basis()`.

```
S.basis()
```

```
[
(1, 0, 2/3),
(0, 1, -7/3)
]
```

Notemos que Sage convirtió el conjunto generador de dos vectores en una base con dos vectores. Esto se debe en parte al hecho que el conjunto original de vectores es linealmente dependiente, pero otro cambio más sustantivo tuvo lugar.

Este es un buen momento para discutir algo se las matemáticas que hacen funcionar las rutinas de Sage. Un espacio vectorial sobre un cuerpo infinito, como los reales o los racionales, es un conjunto infinito. Sin importar cuán enorme parezca la memoria de un computador, siempre será finita. Cómo hace Sage para meter un conjunto infinito en una máquina finita? La idea principal es que un espacio vectorial de dimensión finita tiene un conjunto finito de generadores, que conocemos como una base. Des esta manera, Sage lo único que realmente necesita es conocer los elementos de una base (dos vectores en el ejemplo anterior) para ser capaza de trabajar con la infinidad de posibles elementos del subespacio.

Más aún, para cualquier base asociada a un espacio vectorial, Sage calcula combinaciones lineales para convertirla en otra base "estándar". Esta nueva base tiene la propiedad de que como columnas de una matriz, la matriz está en forma escalonada reducida. Usted lo puede apreciar en la matriz base de arriba. La forma escalonada reducida de una matriz es única, de esta manera la base estándar le permite a Sage reconocer cuándo dos espacios vectoriales son iguales. Acá hay un ejemplo.

```
u = vector(QQ, [1, -1,  3])
v = vector(QQ, [2,  1, -1])
w = vector(QQ, [3,  0,  2])
u + v == w
```

```
True
```

```
S1 = (QQ^3).subspace([u, v, w])
S2 = (QQ^3).subspace([u-v, v-w, w-u])
S1 == S2
```

```
True
```

Como se puede sospechar, es fácil determinar la dimensión de un espacio vectorial.

```
u = vector(QQ, [1, -1,  3,  4])
v = vector(QQ, [2,  1, -1, -2])
S = (QQ^4).subspace([u, v, 2*u + 3*v, -u + 2*v])
S.dimension()
```

```
2
```

Independencia Lineal

Hay diversas formas en Sage para determinar si un conjunto de vectores es linealmente independiente, y para encontrar relaciones de dependencia lineal si es que las hay. La técnica que mostraremos acá es un test simple para saber si un conjunto de vectores es linealmente independiente o no. Simplemente use los vectores como conjunto generador para un subespacio, y verifique la dimensión

de este subespacio. La dimensión es igual al número de vectores en el conjunto generador si y solo si el conjunto generador es linealmente independiente.

```
F.<a> = FiniteField(3^4)
u = vector(F, [a^i for i in range(0,  7, 1)])
v = vector(F, [a^i for i in range(0, 14, 2)])
w = vector(F, [a^i for i in range(0, 21, 3)])
S = (F^7).subspace([u, v, w])
S.dimension()
```

```
3
```

```
S = (F^7).subspace([u, v, a^3*u + a^11*v])
S.dimension()
```

```
2
```

El primer conjunto de vectores, `[u, v, w]`, es linealmente independiente, mientras el segundo conjunto, `[u, v, a^3*u + a^11*v]`, no lo es.

Espacios Vectoriales Abstractos

Sage implementa demasiados espacios vectoriales abstractos de forma directa, tales como P_n, el espacio vectorial de polinomios de grado menor o igual a n. Esto se debe en parte al hecho que un espacio vectorial de dimensión finita sobre un cuerpo F es isomorfo al espacio vectorial F^n. Por esto Sage captura toda la funcionalidad de los espacios vectoriales de dimensión finita, y le deja al usuario realizar la conversión de acuerdo al isomorfismo (lo que puede ser trivial con la elección de una base obvia).

Pero hay instancias en que anillos se comportan naturalmente como espacios vectoriales y podemos aprovechar esta estructura adicional. Veremos mucho más sobre esto en los capítulos sobre cuerpos y teoría de Galois. Como un ejemplo, los cuerpos finitos tienen un generador (uno) y las primeras potencias del generador forman una base. Considere crear n espacio vectorial a partir de los elementos de un cuerpo finito de orden $7^6 = 117\,649$. Como elementos de un cuerpo dabemos que se pueden sumar, de manera que *definiremos* esta como la suma en nuestro espacio vectorial. Para cualquier entero mód 7, podemos multiplicar un elemento del cuerpo por el entero, así es que *definimos* este como nuestro producto por escalares. Más adelante, estaremos seguros que estas definiciones nos llevan a un espacio vectorial, pero créanos por ahora. Acá algunas operaciones en nuestro espacio vectorial nuevo.

```
F.<a> = FiniteField(7^6)
u = 2*a^5 + 6*a^4 + 2*a^3 + 3*a^2 + 2*a + 3
v = 4*a^5 + 4*a^4 + 4*a^3 + 6*a^2 + 5*a + 6
u + v
```

```
6*a^5 + 3*a^4 + 6*a^3 + 2*a^2 + 2
```

```
4*u
```

```
a^5 + 3*a^4 + a^3 + 5*a^2 + a + 5
```

```
2*u + 5*v
```

```
3*a^5 + 4*a^4 + 3*a^3 + a^2 + a + 1
```

Puede que esto le parezca muy parecido a la forma en que sumamos polinomios, y los multiplicamos por escalares. Tendría razón, pero note que en esta construcción de espacio vectorial, hemos ignorado por completo la posibilidad de multiplicar dos elementos del cuerpo entre ellos. Como espacio vectorial con escalares en $\mathbb{Z}_7$, una base consiste de las primeras seis potencias del generador, $\{1, a, a^2, a^3, a^4, a^5\}$. (Note como contar desde cero es natural en este contexto.) Puede que haya notado que Sage consistentemente reescribe los elementos del cuerpo como combinaciones lineales — ahora tenemos una buena explicacíón.

Acá está lo que sabe Sage sobre un cuerpo finito como un espacio vectorial. Primero, sabe que el cuerpo finito *es* un espacio vectorial, y cuál es el cuerpo de escalares.

```
V = F.vector_space(); V
```

```
Vector space of dimension 6 over Finite Field of size 7
```

```
R = V.base_ring(); R
```

```
Finite Field of size 7
```

```
R == FiniteField(7)
```

```
True
```

```
V.dimension()
```

```
6
```

Así, el cuerpo finito (como espacio vectoril) es isomorfo al espacio vectorial $(\mathbb{Z}_7)^6$. Notemos que este no es un isomorfismo de anillos o de cuerpos ya que no se hace cargo completamente de la multiplicación de elementos, aunque ésta es posible en el cuerpo.

Segundo, los elementos del cuerpo pueden ser convertidos fácilmente en elementos del espacio vectorial.

```
x = V(u); x
```

```
(3, 2, 3, 2, 6, 2)
```

```
y = V(v); y
```

```
(6, 5, 6, 4, 4, 4)
```

Notemos que Sage escribe los elementos del cuerpo partiendo de las potencias mayores del generador, mientras la base usada está ordenada partiendo de las potencias menores. Los siguientes cálculos ilustran el isomorfismo que preserva la estructura entre el cuerpo finito mismo y su interpretación como el espacio vectorial, $(\mathbb{Z}_7)^6$.

```
V(u + v) == V(u) + V(v)
```

```
True
```

```
two = R(2)
V(two*u) == two*V(u)
```

```
True
```

Álgebra Lineal

Sage tiene mucha funcionalidad para álgebra lineal de lo que hemos descrito o de lo que necesitaremos en los siguientes capítulos. Cree espacios vectoriales y vectores en ellos (con distintos cuerpos de escalares), y use la completación con TAB en estos objetos para ver la gran cantidad de métodos disponibles.

20.7 Ejercicios en Sage

1. Dados dos subespacios U y W de un espacio vectorial V, su suma $U + W$ puede ser definida como el *conjunto* $U + W = \{u + w \mid u \in U,\ w \in W\}$, en otras palabras, el conjunto de todas las sumas posibles de un elemento de U y un elemento de W.
Note que esto no es la suma directa del texto, ni corresponde al método `direct_sum()` en Sage. Pero, es posible construir este subespacio en Sage como sigue. Tome bases de U y W por separado, para definir listas de vectores. Junte las dos listas usando el signo de suma entre ellas (esto concatena las listas). Ahora construya el subespacio suma creando el subespacio de V generado por este conjunto, usando el método `.subspace()`.
En el espacio vectorial (`QQ^10`) construya dos subespacios que cumplan que (a) tengan dimensión 5 o 6, y (b) tengan una intersección de dimensión 2. Compare sus dimensiones individuales con las dimensiones de su intersección ($U \cap W$, `.intersection()` en Sage) y su suma $U + W$.
Repita el experimento con espacios vectoriales de dimensión 8, y con intersección tan pequeña como sea posible. Conjeture una relación entre estas cuatro dimensiones basado en los resultados de sus experimentos.

2. Podemos construir un cuerpo en Sage que extienda los racionales agregando una raíz cuarta de dos, $\mathbb{Q}[\sqrt[4]{2}]$, con el comando `F.<c> = QQ[2^(1/4)]`. Este es un espacio vectorial de dimensión 4 sobre los racionales, con una base que consiste de las primeras cuatro potencias de $c = \sqrt[4]{2}$ (partiendo de la potencia cero).
El comando `F.vector_space()` le devolverá estos tres ítemes en una tripleta (de manera que tenga cuidado como usa esta salida para extraer lo que necesite). La primera componente de la salida es un espacio vectorial sobre los racionales que es isomorfo a `F`. La siguiente es un isomorfismo de espacios vectoriales (una transformación linea invertible) del espacio entregado al cuerpo, mientras la tercera componente es un isomorfismo en la dirección opuesta. Estos dos isomorfismo pueden ser usados como funciones. Note que este es un comportamiento distinto al obtenido con el método `.vector_space()` aplicado a cuerpos finitos. Construya ejemplos no triviales que muestren que estos isomorfismos de espacios vectoriales se comportan como deben los isomorfismos.

3. Construya un cuerpo finito F de orden p^n en la forma usual. Luego construya el grupo (multiplicativo) de todas las matrices invertibles (nonsingulares) de $m \times m$ sobre este cuerpo con el comando `G = GL(m, F)` ("el grupo lineal general"). ¿Cuál es el orden de este grupo? En otras palabras, encuentre una expresión general para el orden de este grupo.
Su respuesta debiese ser en función de m, p y n. Explique su solución en detalle y verifique con ejemplos en Sage que su respuesta es correcta.
Ayudas: `G.order()` le ayudará a poner a prueba y verificar sus hipótesis. Ejemplos pequeños en Sage (listando todos los elementos del grupo) pueden ayudar a su intuición—que es la razón de que esto sea un ejercicio en Sage. Pequeños quiere decir matrices de 2×2 y 3×3 y cuerpos finitos con $2, 3, 4, 5$ elementos, a lo sumo. Los resultados no dependen realmente de p y n, sino solo de p^n.
Advierta que este grupo es interesante porque contiene representaciones de

todas las transformaciones lineales invertibles del espapcio vectorial F^m en si mismo.

4. ¿Qué pasa si intentamos hacer álgebra lineal sobre un *anillo* que no sea un *cuerpo*? El objeto que más se parece a un espacio vectorial, pero con esta diferencia, se conoce como ***módulo*** (no confundir con las congruencias módulo algo). Usted puede obtener uno fácilmente con una construcción como `ZZ^3`. Ejecute la siguiente celda para crear un módulo y un submódulo.

```
M = ZZ^3
u = M([1, 0, 0])
v = M([2, 2, 0])
w = M([0, 0, 4])
N = M.submodule([u, v, w])
```

Examine las bases y las dimensiones (es decir "rango") del módulo y del submódulo, y verifique si el módulo y el submódulo son iguales. ¿Cómo se diferencia esto de la situación análoga para espacios vectoriales? ¿Puede crear un tercer módulo, `P`, que sea un subconjunto propio de `M` y que contenga propiamente a `N`?

5. un cuerpo finito, F, de orden 5^3 es un espacio vectorial de dimensión 3 sobre $\mathbb{Z}_5$. Supongamos que a es un generador de F. Sea M cualquier matriz de 3×3 con coeficientes en $\mathbb{Z}_5$ (cuidado acá, los elementos son del cuerpo de escalares, no del espacio vectorial). Si convertimos un elemento $x \in F$ en un vector (relativo a la base $\{1, a, a^2\}$), entonces podemos multiplicarlo por M (con M al lado izquierdo) para crear otro vector, que entonces podemos traducir en una combinación lineal de los elementos de la base, y por ende en otro elemento de F. Esta función es un homomorfismo de espacios vectoriales, mejor conocido como una transformación lineal (implementeda con su representación matricial relativa a la base $\{1, a, a^2\}$. Note que cada parte más abajo se vuelve menos general y más específica.

(a) Cree una matriz no-invertible R y dé ejemplos para mostrar que la función descrita por R es un homomorfismode espacios vectoriales de F en F.

(b) Cree una matriz invertible M. La función ahora será un homomorfismo invertible. Determine la función inversa y dé ejemplos para verificar sus propiedades.

(c) Como a es un generador del cuerpo, la función $a \mapsto a^5$ puede ser extendida a un homomorfismo de espacios vectoriales (i.e. una transformación lineal). Encuentre una matriz M que efectúe esta transformación lineal, y de ahí determine que el homomorfismo es invertible.

(d) Ninguna de las tres partes anteriores utiliza las propiedades de la multiplicación en el cuerpo. Pero la función de la tercera parte también preserva la multiplicación en el cuerpo, aunque esto puede no ser obvio en este momento. Estamos afirmando que esta última función es un automorfismo de cuerpos, preservando tanto la suma como la multiplicación. Dé un ejemplo no-trivial de la propiedad de preservación del producto de esta función. (Esta es la ***función de Frobenius*** que será discutida en mayor detalle en el Capítulo 21.)

21

Cuerpos

Es natural preguntarse si cierto cuerpo F está contenido en un cuerpo mayor. Pensemos en los números racionales, que están contenidos dentro de los números reales, que a su vez están contenidos dentro de los números complejos. También podemos estudiar los cuerpos que se encuentran entre $\mathbb{Q}$ y $\mathbb{R}$ y preguntarnos sobre la naturaleza de estos cuerpos.

Más específicamente, si nos dan un cuerpo F y un polinomio $p(x) \in F[x]$, podemos preguntar si es posible, o no, encontrar un cuerpo E que contenga F tal que $p(x)$ se factorice en factores lineales sobre $E[x]$. Por ejemplo, si consideramos el polinomio

$$p(x) = x^4 - 5x^2 + 6$$

en $\mathbb{Q}[x]$, entonces $p(x)$ se factoriza como $(x^2-2)(x^2-3)$. Sin embargo, ambos factores son irreducibles en $\mathbb{Q}[x]$. Si queremos encontrar un cero de $p(x)$, debemos ir a un cuerpo más grande. Ciertamente sirve el cuerpo de los números reales, pues

$$p(x) = (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3}).$$

Es posible encontrar un cuerpo menor en el que $p(x)$ tiene un cero, por ejemplo

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

Queremos ser capaces de calcular y estudiar tales cuerpos para polinomios arbitrarios sobre un cuerpo F.

21.1 Extensiones de cuerpos

Un cuerpo E es una ***extensión de cuerpos*** de un cuerpo F si F es un subcuerpo de E. El cuerpo F se llama ***cuerpo base***. Escribimos $F \subset E$.

Ejemplo 21.1. Por ejemplo, sea

$$F = \mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

y sea $E = \mathbb{Q}(\sqrt{2} + \sqrt{3}\,)$ el menor cuerpo que contiene $\mathbb{Q}$ y $\sqrt{2} + \sqrt{3}$. Tanto E como F son extensiones de los números racionales. Afirmamos que E es una extensión del cuerpo F. Para ver esto, solo necesitamos mostrar que $\sqrt{2}$ está en E. Como $\sqrt{2} + \sqrt{3}$ está en E, $1/(\sqrt{2} + \sqrt{3}\,) = \sqrt{3} - \sqrt{2}$ también debe estar en E. Tomando combinaciones lineales de $\sqrt{2} + \sqrt{3}$ y $\sqrt{3} - \sqrt{2}$, encontramos que tanto $\sqrt{2}$ como $\sqrt{3}$ deben estar en E.

Ejemplo 21.2. Sea $p(x) = x^2+x+1 \in \mathbb{Z}_2[x]$. Como ni 0 ni 1 es una raíz de este polinomio, sabemos que $p(x)$ es irreducible sobre $\mathbb{Z}_2$. Construiremos una extensión del cuerpo $\mathbb{Z}_2$ que contenga un elemento α tal que $p(\alpha) = 0$. Por el Teorema 17.22, el ideal $\langle p(x)\rangle$ generado por $p(x)$ es maximal; luego, $\mathbb{Z}_2[x]/\langle p(x)\rangle$ es un cuerpo. Sea $f(x) + \langle p(x)\rangle$ un elemento arbitrario de $\mathbb{Z}_2[x]/\langle p(x)\rangle$. Por el algoritmo de la división,

$$f(x) = (x^2 + x + 1)q(x) + r(x),$$

donde el grado de $r(x)$ es menor al grado de $x^2 + x + 1$. Por lo tanto,

$$f(x) + \langle x^2 + x + 1\rangle = r(x) + \langle x^2 + x + 1\rangle.$$

Las únicas posibilidades para $r(x)$ son entonces 0, 1, x, y $1 + x$. En consecuencia, $E = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ es un cuerpo con cuatro elementos y debe ser una extensión de $\mathbb{Z}_2$, que contiene un cero α de $p(x)$. El cuerpo $\mathbb{Z}_2(\alpha)$ consiste de los elementos

$$\begin{aligned} 0 + 0\alpha &= 0 \\ 1 + 0\alpha &= 1 \\ 0 + 1\alpha &= \alpha \\ 1 + 1\alpha &= 1 + \alpha. \end{aligned}$$

Notemos que $\alpha^2 + \alpha + 1 = 0$; por lo que, si calculamos $(1 + \alpha)^2$,

$$(1 + \alpha)(1 + \alpha) = 1 + \alpha + \alpha + (\alpha)^2 = \alpha.$$

Otros cálculos se realizan de forma similar. Resumimos estos resultados en las siguientes tablas, que nos dicen cómo sumar y multiplicar elementos en E.

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

Cuadro 21.3: Tabla de sumas para $\mathbb{Z}_2(\alpha)$

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Cuadro 21.4: Tabla de productos para $\mathbb{Z}_2(\alpha)$

El siguiente teorema, de Kronecker, es tan importante y básico para nuestra comprensión de los cuerpos que frecuentemente se conoce como Teorema Fundamental de la Teoría de Cuerpos.

Teorema 21.5. *Sea F un cuerpo y sea $p(x)$ un polinomio no constante en $F[x]$. Entonces existe un cuerpo de extensión E de F y un elemento $\alpha \in E$ tal que $p(\alpha) = 0$.*

Demostración. Para demostrar este teorema, usaremos el método usado en el Ejemplo 21.2. Claramente, podemos suponer que $p(x)$ es un polinomio irreducible. Queremos encontrar una extensión E de F que contenga un elemento α tal que $p(\alpha) = 0$. El ideal $\langle p(x)\rangle$ generado por $p(x)$ es un ideal maximal en $F[x]$ por el Teorema 17.22; luego, $F[x]/\langle p(x)\rangle$ es un cuerpo. Afirmamos que $E = F[x]/\langle p(x)\rangle$ es el cuerpo buscado.

Demostraremos primero que E es una extensión de F. Podemos definir un homomorfismo de anillos conmutativos $\psi : F \to F[x]/\langle p(x)\rangle$, donde $\psi(a) = a + \langle p(x)\rangle$ para $a \in F$. Es fácil verificar que ψ es realmente un homomorfismo de anillos. Observe que

$$\psi(a) + \psi(b) = (a + \langle p(x)\rangle) + (b + \langle p(x)\rangle) = (a + b) + \langle p(x)\rangle = \psi(a + b)$$

y

$$\psi(a)\psi(b) = (a + \langle p(x)\rangle)(b + \langle p(x)\rangle) = ab + \langle p(x)\rangle = \psi(ab).$$

Para demostrar que ψ es 1-1, supongamos que

$$a + \langle p(x)\rangle = \psi(a) = \psi(b) = b + \langle p(x)\rangle.$$

Entonces $a - b$ es un múltiplo de $p(x)$, dado que está en el ideal $\langle p(x)\rangle$. Como $p(x)$ es un polinomio no constante, la única posibilidad es que $a - b = 0$. Por lo tanto, $a = b$ y ψ es inyectivo. Como ψ es 1-1, podemos identificar F con el subcuerpo $\{a + \langle p(x)\rangle : a \in F\}$ de E y ver E como un cuerpo de extensión de F.

Nos falta demostrar que $p(x)$ tiene un cero $\alpha \in E$. Sea $\alpha = x + \langle p(x)\rangle$. Entonces α está en E. Si $p(x) = a_0 + a_1x + \cdots + a_nx^n$, entonces

$$\begin{aligned} p(\alpha) &= a_0 + a_1(x + \langle p(x)\rangle) + \cdots + a_n(x + \langle p(x)\rangle)^n \\ &= a_0 + (a_1x + \langle p(x)\rangle) + \cdots + (a_nx^n + \langle p(x)\rangle) \\ &= a_0 + a_1x + \cdots + a_nx^n + \langle p(x)\rangle \\ &= 0 + \langle p(x)\rangle. \end{aligned}$$

Por lo tanto, hemos encontrado un elemento $\alpha \in E = F[x]/\langle p(x)\rangle$ tal que α es un cero de $p(x)$. □

Ejemplo 21.6. Sea $p(x) = x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$. Entonces $p(x)$ tiene factores irreducibles $x^2 + x + 1$ y $x^3 + x + 1$. Para un cuerpo de extensión E de $\mathbb{Z}_2$ tal que $p(x)$ tenga una raíz en E, podemos tomar E como $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ o como $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$. Dejaremos de ejercicio mostrar que $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ es un cuerpo con $2^3 = 8$ elementos.

Elementos Algebraicos

Un elemento α en una extensión de cuerpos E sobre F es ***algebraico*** sobre F si $f(\alpha) = 0$ para algún polinomio no nulo $f(x) \in F[x]$. Un elemento en E que no es algebraico sobre F es ***trascendente*** sobre F. Un cuerpo de extensión E de un cuerpo F es una ***extensión algebraica*** de F si cada elemento en E es algebraico sobre F. Si E es una extensión de cuerpos de F y $\alpha_1, \ldots, \alpha_n$ están contenidos en E, denotamos por $F(\alpha_1, \ldots, \alpha_n)$ al menor cuerpo que contiene F y $\alpha_1, \ldots, \alpha_n$. Si $E = F(\alpha)$ para cierto $\alpha \in E$, entonces E es una ***extensión simple*** de F.

Ejemplo 21.7. Tanto $\sqrt{2}$ como i son algebraicos sobre $\mathbb{Q}$ pues son ceros de los polinomios $x^2 - 2$ y $x^2 + 1$, respectivamente. Claramente π y e son algebraicos sobre los números reales; sin embargo, es un hecho que son trascendentes sobre $\mathbb{Q}$. Números en $\mathbb{R}$ que sean algebraicos sobre $\mathbb{Q}$ son minoría. Casi todos los números reales son trascendentes sobre $\mathbb{Q}$.[1] (En muchos casos no se sabe si un número específico es trascendente o no; por ejemplo aún no se sabe si $\pi + e$ es trascendente o algebraico.)

Un número complejo que sea algebraico sobre $\mathbb{Q}$ es un ***número algebraico***. Un ***número trascendente*** es un elemento de $\mathbb{C}$ que es trascendente sobre $\mathbb{Q}$.

Ejemplo 21.8. Mostraremos que $\sqrt{2+\sqrt{3}}$ es algebraico sobre $\mathbb{Q}$. Si $\alpha = \sqrt{2+\sqrt{3}}$, entonces $\alpha^2 = 2 + \sqrt{3}$. Por lo tanto, $\alpha^2 - 2 = \sqrt{3}$ y $(\alpha^2 - 2)^2 = 3$. Como $\alpha^4 - 4\alpha^2 + 1 = 0$, debe ocurrir que α es un cero del polinomio $x^4 - 4x^2 + 1 \in \mathbb{Q}[x]$.

Es muy fácil dar un ejemplo de una extensión de cuerpos E sobre un cuerpo F, tal que E contenga un elemento trascendente sobre F. El siguiente teorema caracteriza las extensiones trascendentes.

Teorema 21.9. *Sea E un cuerpo de extensión de F y $\alpha \in E$. Entonces α es trascendente sobre F si y solo si $F(\alpha)$ es isomorfo a $F(x)$, el cuerpo de fracciones de $F[x]$.*

Demostración. Sea $\phi_\alpha : F[x] \to E$ el homomorfismo de evaluación en α. Entonces α es trascendente sobre F si y solo si $\phi_\alpha(p(x)) = p(\alpha) \neq 0$ para todo polinomio no constante $p(x) \in F[x]$. Esto es verdadero si y solo si $\ker \phi_\alpha = \{0\}$; es decir, es verdadero precisamente cuando ϕ_α es 1-1. Luego, E debe contener una copia de $F[x]$. El menor cuerpo que contiene a $F[x]$ es el cuerpo de fracciones $F(x)$. Por el Teorema 18.4, E debe contener una copia de este cuerpo. □

Tenemos una situación más interesante para el caso de las extensiones algebraicas.

Teorema 21.10. *Sea E una extensión de un cuerpo F y $\alpha \in E$ con α algebraico sobre F. Entonces hay un único polinomio mónico e irreducible $p(x) \in F[x]$ tal que $p(\alpha) = 0$. Si $f(x)$ es otro polinomio en $F[x]$ tal que $f(\alpha) = 0$, entonces $p(x)$ divide a $f(x)$.*

Demostración. Sea $\phi_\alpha : F[x] \to E$ el homomorfismo de evaluación. El núcleo de ϕ_α es un ideal principal generado por algún polinomio $p(x) \in F[x]$ con $\operatorname{gr} p(x) \geq 1$. Sabemos que tal polinomio existe, pues $F[x]$ es un dominio de ideales principales y α es algebraico. El ideal $\langle p(x) \rangle$ consiste exactamente de aquellos elementos de $F[x]$ que tienen a α como cero. Si $f(\alpha) = 0$ y $f(x)$ no es el polinomio nulo, entonces $f(x) \in \langle p(x) \rangle$ y $p(x)$ divide a $f(x)$. Así $p(x)$ es un polinomio de grado mínimo que tiene a α como un cero. Cualquier otro polinomio del mismo grado que se anule en α debe ser de la forma $\beta p(x)$ para cierto $\beta \in F$.

Supongamos ahora que $p(x) = r(x)s(x)$ es una factorización de $p(x)$ en factores de grado menor. Como $p(\alpha) = 0$, $r(\alpha)s(\alpha) = 0$; luego, $r(\alpha) = 0$ o $s(\alpha) = 0$, lo que contradice el hecho de que p es de grado mínimo. Por lo tanto, $p(x)$ debe ser irreducible. □

[1] La probabilidad de que un número real elegido al azar en el intervalo $[0, 1]$ sea trascendente sobre los números racionales es uno.

Sea E una extensión del cuerpo F y $\alpha \in E$ un elemento algebraico sobre F. El polinomio mónico único $p(x)$ del teorema anterior se llama ***polinomio minimal*** de α sobre F. El grado de $p(x)$ es el ***grado de*** α ***sobre*** F.

Ejemplo 21.11. Sea $f(x) = x^2 - 2$ y $g(x) = x^4 - 4x^2 + 1$. Estos son los polinomios minimales de $\sqrt{2}$ y $\sqrt{2+\sqrt{3}}$, respectivamente.

Proposición 21.12. *Sea E una extensión del cuerpo F y $\alpha \in E$ algebraico sobre F. Entonces $F(\alpha) \cong F[x]/\langle p(x)\rangle$, donde $p(x)$ es el polinomio minimal de α sobre F.*

Demostración. Sea $\phi_\alpha : F[x] \to E$ el homomorfismo de evaluación. El núcleo de esta función es $\langle p(x)\rangle$, donde $p(x)$ es el polinomio minimal de α. Por el Primer Teorema de Isomorfía de anillos, la imagen ϕ_α en E es isomorfa a $F(\alpha)$ pues contiene tanto a F como a α. □

Teorema 21.13. *Sea $E = F(\alpha)$ una extensión simple de F, con $\alpha \in E$ algebraico sobre F. Supongamos que el grado de α sobre F es n. Entonces todo elemento $\beta \in E$ puede ser expresado de forma única como*

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

con $b_i \in F$.

Demostración. Dado que $\phi_\alpha(F[x]) \cong F(\alpha)$, todo elemento en $E = F(\alpha)$ debe ser de la forma $\phi_\alpha(f(x)) = f(\alpha)$, donde $f(\alpha)$ es un polinomio en α con coeficientes en F. Sea

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

el polinomio minimal de α. Entonces $p(\alpha) = 0$; luego,

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0.$$

Similarmente,

$$\begin{aligned}\alpha^{n+1} &= \alpha\alpha^n \\ &= -a_{n-1}\alpha^n - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha \\ &= -a_{n-1}(-a_{n-1}\alpha^{n-1} - \cdots - a_0) - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha.\end{aligned}$$

Continuando de esta manera, podemos expresar cualquier monomio α^m, $m \geq n$, como combinación lineal de potencias de α menores a n. Por lo tanto, cualquier $\beta \in F(\alpha)$ puede ser escrito como

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}.$$

Para mostrar la unicidad, supongamos que

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

para b_i y c_i en F. Entonces

$$g(x) = (b_0 - c_0) + (b_1 - c_1)x + \cdots + (b_{n-1} - c_{n-1})x^{n-1}$$

está en $F[x]$ y $g(\alpha) = 0$. Como el grado de $g(x)$ es menor que el grado de $p(x)$, el polinomio irreducible de α, $g(x)$ debe ser el polinomio nulo. Concluimos,

$$b_0 - c_0 = b_1 - c_1 = \cdots = b_{n-1} - c_{n-1} = 0,$$

es decir, $b_i = c_i$ para $i = 0, 1, \ldots, n-1$. Hemos demostrado la unicidad. □

Ejemplo 21.14. Como x^2+1 es irreducible sobre $\mathbb{R}$, $\langle x^2+1\rangle$ es un ideal maximal en $\mathbb{R}[x]$. Así $E=\mathbb{R}[x]/\langle x^2+1\rangle$ es una extensión de cuerpos de $\mathbb{R}$ que contiene una raíz de x^2+1. Sea $\alpha = x+\langle x^2+1\rangle$. Podemos identificar E con lo números complejos. Por Proposición 21.12, E es isomorfo a $\mathbb{R}(\alpha)=\{a+b\alpha : a,b\in\mathbb{R}\}$. Sabemos que $\alpha^2=-1$ en E, dado que

$$\begin{aligned}\alpha^2+1 &= (x+\langle x^2+1\rangle)^2+(1+\langle x^2+1\rangle)\\ &= (x^2+1)+\langle x^2+1\rangle\\ &= 0.\end{aligned}$$

Luego, tenemos un isomorfismo de $\mathbb{R}(\alpha)$ con $\mathbb{C}$ definido por la función que envía $a+b\alpha$ a $a+bi$.

Sea E una extensión de un cuerpo F. Si consideramos E como un espacio vectorial sobre F, entonces podemos usar toda la maquinaria de álgebra lineal para trabajar en problemas que encontremos en nuestro estudio de cuerpos. Los elementos en el cuerpo E son vectores; los elementos en el cuerpo F son escalares. Podemos pensar en la adición en E como sumar vectores. Cuando multiplicamos un elemento en E por un elemento de F, estamos multiplicando un vector por un escalar. Este punto de vista para las extensiones de cuerpos es especialmente fructífero si una extensión E de F es un espacio vectorial de dimensión finita sobre F, y el Teorema 21.13 dice que $E=F(\alpha)$ es de dimensión finita sobre F con base $\{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$.

Si un cuerpo de extensión E de un cuerpo F es un espacio vectorial sobre F de dimensión finita n, entonces diremos que E es una ***extensión de grado finito*** n ***sobre*** F. Escribiremos

$$[E:F]=n.$$

para indicar la dimensión de E sobre F.

Teorema 21.15. *Toda extensión finita E de un cuerpo F es una extensión algebraica.*

Demostración. Sea $\alpha\in E$. Como $[E:F]=n$, los elementos

$$1,\alpha,\ldots,\alpha^n$$

no pueden ser linealmente independientes. Luego existen $a_i\in F$, no todos cero, tales que

$$a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0=0.$$

Por lo tanto,

$$p(x)=a_nx^n+\cdots+a_0\in F[x]$$

es un polinomio no nulo con $p(\alpha)=0$. □

Nota 21.16. Teorema 21.15 dice que toda extensión finita de un cuerpo F es una extensión algebraica. Sin embargo, el recíproco es falso. Dejaremos como un ejercicio demostrar que el conjunto de todos los elementos en $\mathbb{R}$ que son algebraicos sobre $\mathbb{Q}$ forma una extensión infinita de $\mathbb{Q}$.

El siguiente es un teorema de conteo similar al Teorema de Lagrange en teoría de grupos. Teorema 21.17 probará una herramienta de gran utilidad en nuestra investigación de extensiones finitas de cuerpos.

Teorema 21.17. *Si E es una extensión finita de F, y K es una extensión finita de E, entonces K es una extensión finita de F y*

$$[K:F]=[K:E][E:F].$$

DEMOSTRACIÓN. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base para E como espacio vectorial sobre F y sea $\{\beta_1, \ldots, \beta_m\}$ una base para K como espacio vectorial sobre E. Afirmamos que $\{\alpha_i\beta_j\}$ es una base para K sobre F. Probaremos primero que estos vectores generan K. Sea $u \in K$. Entonces $u = \sum_{j=1}^{m} b_j\beta_j$ y $b_j = \sum_{i=1}^{n} a_{ij}\alpha_i$, donde $b_j \in E$ y $a_{ij} \in F$. Entonces

$$u = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij}\alpha_i \right) \beta_j = \sum_{i,j} a_{ij}(\alpha_i\beta_j).$$

Así los mn vectores $\alpha_i\beta_j$ generan K sobre F.

Debemos mostrar que los $\alpha_i\beta_j$ son linealmente independientes. Recuerde que un conjunto de vectores $\{v_1, v_2, \ldots, v_n\}$ en un espacio vectorial V es linealmente independiente si

$$c_1v_1 + c_2v_2 + \cdots + c_nv_n = 0$$

implica que

$$c_1 = c_2 = \cdots = c_n = 0.$$

Sea

$$u = \sum_{i,j} c_{ij}(\alpha_i\beta_j) = 0$$

para $c_{ij} \in F$. Debemos demostrar que todos los c_{ij}'s son cero. Podemos reescribir u como

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} c_{ij}\alpha_i \right) \beta_j = 0,$$

donde $\sum_i c_{ij}\alpha_i \in E$. Como los β_j son linealmente independientes sobre E, debe ser el caso que

$$\sum_{i=1}^{n} c_{ij}\alpha_i = 0$$

para todo j. Sin embargo, los α_j también son linealmente independientes sobre F. Por lo tanto, $c_{ij} = 0$ para todo i y j, lo que completa la demostración. □

El siguiente corolario se demuestra fácilmente por inducción.

Corolario 21.18. *Si F_i son cuerpos para $i = 1, \ldots, k$ y F_{i+1} es una extensión finita de F_i, entonces F_k es una extensión finita de F_1 y*

$$[F_k : F_1] = [F_k : F_{k-1}] \cdots [F_2 : F_1].$$

Corolario 21.19. *Sea E una extensión de cuerpos de F. Si $\alpha \in E$ es algebraico sobre F con polinomio minimal $p(x)$ y $\beta \in F(\alpha)$ con polinomio minimal $q(x)$, entonces* $\operatorname{gr} q(x)$ *divide a* $\operatorname{gr} p(x)$.

DEMOSTRACIÓN. Sabemos que $\operatorname{gr} p(x) = [F(\alpha) : F]$ y $\operatorname{gr} q(x) = [F(\beta) : F]$. Como $F \subset F(\beta) \subset F(\alpha)$,

$$[F(\alpha) : F] = [F(\alpha) : F(\beta)][F(\beta) : F].$$ □

Ejemplo 21.20. Determinemos una extensión de cuerpos de $\mathbb{Q}$ que contenga $\sqrt{3} + \sqrt{5}$. Es fácil determinar que el polinomio minimal de $\sqrt{3} + \sqrt{5}$ es $x^4 - 16x^2 + 4$. Se sigue que

$$[\mathbb{Q}(\sqrt{3} + \sqrt{5}\,) : \mathbb{Q}] = 4.$$

Sabemos que $\{1, \sqrt{3}\,\}$ es una base para $\mathbb{Q}(\sqrt{3}\,)$ sobre $\mathbb{Q}$. Luego, $\sqrt{3} + \sqrt{5}$ no puede estar en $\mathbb{Q}(\sqrt{3}\,)$. Se sigue que $\sqrt{5}$ no puede estar en $\mathbb{Q}(\sqrt{3}\,)$ tampoco. Por

lo tanto, $\{1, \sqrt{5}\}$ es una base para $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = (\mathbb{Q}(\sqrt{3}))(\sqrt{5})$ sobre $\mathbb{Q}(\sqrt{3})$ y $\{1, \sqrt{3}, \sqrt{5}, \sqrt{3}\sqrt{5} = \sqrt{15}\}$ es una base para $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$ sobre $\mathbb{Q}$. Este ejemplo muestra que es posible que cierta extensión $F(\alpha_1, \ldots, \alpha_n)$ sea realmente una extensión simple de F aunque $n > 1$.

Ejemplo 21.21. Calculemos una base para $\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}\, i)$, donde $\sqrt{5}$ es la raíz cuadrada positiva de 5 y $\sqrt[3]{5}$ es la raíz cúbica real de 5. Sabemos que $\sqrt{5}\, i \notin \mathbb{Q}(\sqrt[3]{5})$, así es que

$$[\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}\, i) : \mathbb{Q}(\sqrt[3]{5})] = 2.$$

Es fácil determinar que $\{1, \sqrt{5}i\}$ es una base para $\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}\, i)$ sobre $\mathbb{Q}(\sqrt[3]{5})$. También sabemos que $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$ es una base para $\mathbb{Q}(\sqrt[3]{5})$ sobre $\mathbb{Q}$. Luego, una base para $\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}\, i)$ sobre $\mathbb{Q}$ es

$$\{1, \sqrt{5}\, i, \sqrt[3]{5}, (\sqrt[3]{5})^2, (\sqrt[6]{5})^5 i, (\sqrt[6]{5})^7 i = 5\sqrt[6]{5}\, i \text{ o } \sqrt[6]{5}\, i\}.$$

Notemos que $\sqrt[6]{5}\, i$ es un cero de $x^6 + 5$. Podemos demostrar que este polinomio es irreducible sobre $\mathbb{Q}$ usando el Criterio de Eisenstein, con $p = 5$. Por lo tanto,

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[6]{5}\, i) \subset \mathbb{Q}(\sqrt[3]{5}, \sqrt{5}\, i).$$

Pero debe ser el caso que $\mathbb{Q}(\sqrt[6]{5}\, i) = \mathbb{Q}(\sqrt[3]{5}, \sqrt{5}\, i)$, dado que ambas son extensiones de grado 6.

Teorema 21.22. *Sea E una extensión de cuerpos de F. Entonces las siguientes afirmaciones son equivalentes.*

1. *E es una extensión finita de F.*
2. *Existe un número finito de elementos algebraicos $\alpha_1, \ldots, \alpha_n \in E$ tales que $E = F(\alpha_1, \ldots, \alpha_n)$.*
3. *Existe una sucesión de cuerpos*

$$E = F(\alpha_1, \ldots, \alpha_n) \supset F(\alpha_1, \ldots, \alpha_{n-1}) \supset \cdots \supset F(\alpha_1) \supset F,$$

donde cada cuerpo $F(\alpha_1, \ldots, \alpha_i)$ es algebraico sobre $F(\alpha_1, \ldots, \alpha_{i-1})$.

DEMOSTRACIÓN. (1) $\Rightarrow$ (2). Sea E una extensión algebraica finita de F. Entonces E es un espacio vectorial de dimensión finita sobre F y hay una base que consiste de elementos $\alpha_1, \ldots, \alpha_n$ en E tales que $E = F(\alpha_1, \ldots, \alpha_n)$. Cada α_i es algebraico sobre F por el Teorema 21.15.

(2) $\Rightarrow$ (3). Supongamos que $E = F(\alpha_1, \ldots, \alpha_n)$, donde cada α_i es algebraico sobre F. Entonces

$$E = F(\alpha_1, \ldots, \alpha_n) \supset F(\alpha_1, \ldots, \alpha_{n-1}) \supset \cdots \supset F(\alpha_1) \supset F,$$

donde cada cuerpo $F(\alpha_1, \ldots, \alpha_i)$ es algebraico sobre $F(\alpha_1, \ldots, \alpha_{i-1})$.

(3) $\Rightarrow$ (1). Sea

$$E = F(\alpha_1, \ldots, \alpha_n) \supset F(\alpha_1, \ldots, \alpha_{n-1}) \supset \cdots \supset F(\alpha_1) \supset F,$$

donde cada cuerpo $F(\alpha_1, \ldots, \alpha_i)$ es algebraico sobre $F(\alpha_1, \ldots, \alpha_{i-1})$. Como

$$F(\alpha_1, \ldots, \alpha_i) = F(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i)$$

es una extensión simple y α_i es algebraico sobre $F(\alpha_1, \ldots, \alpha_{i-1})$, se sigue que

$$[F(\alpha_1, \ldots, \alpha_i) : F(\alpha_1, \ldots, \alpha_{i-1})]$$

es finita para cada i. Por lo tanto, $[E : F]$ es finita. □

Clausura Algebraica

Dado un cuerpo F, surge la pregunta sobre si es posible encontrar un cuerpo E tal que todo polinomio $p(x)$ tenga una raíz en E. Esto nos lleva al siguiente teorema.

Teorema 21.23. *Sea E una extensión de cuerpos de F. El conjunto de los elementos en E que son algebraicos sobre F forma un cuerpo.*

DEMOSTRACIÓN. Sean $\alpha, \beta \in E$ algebraicos sobre F. Entonces $F(\alpha, \beta)$ es una extensión finita de F. Como todo elemento de $F(\alpha, \beta)$ es algebraico sobre F, $\alpha \pm \beta$, $\alpha\beta$, y α/β $(\beta \neq 0)$ son todos algebraicos sobre F. Por lo tanto, el conjunto de los elementos en E que son algebraicos sobre F forma un cuerpo. □

Corolario 21.24. *El conjunto de todos los números algebraicos forma un cuerpo; es decir, el conjunto de todos los números complejos que son algebraicos sobre $\mathbb{Q}$ constituye un cuerpo.*

Sea E una extensión de cuerpos de un cuerpo F. Definimos la ***clausura algebraica*** de un cuerpo F en E como el cuerpo que consiste de todos los elementos en E que son algebraicos sobre F. Un cuerpo F es ***algebraicamente cerrado*** si todo polinomio no constante en $F[x]$ tiene una raíz en F.

Teorema 21.25. *Un cuerpo F es algebraicamente cerrado si y solo si todo polinomio no constante en $F[x]$ se factoriza en factores lineales sobre $F[x]$.*

DEMOSTRACIÓN. Sea F un cuerpo algebraicamente cerrado. Si $p(x) \in F[x]$ es un polinomio no constante, entonces $p(x)$ tiene una raíz en F, digamos α. Luego, $x - \alpha$ debe ser un factor de $p(x)$ de manera que $p(x) = (x - \alpha)q_1(x)$, donde $\operatorname{gr} q_1(x) = \operatorname{gr} p(x) - 1$. Continúe este proceso con $q_1(x)$ para encontrar la factorización

$$p(x) = (x - \alpha)(x - \beta)q_2(x),$$

donde $\operatorname{gr} q_2(x) = \operatorname{gr} p(x) - 2$. Este proceso debe terminar en algún momento pues el grado de $p(x)$ es finito.

Recíprocamente, supongamos que todo polinomio no constante $p(x)$ en $F[x]$ se factoriza como producto de factores lineales. Sea $ax - b$ uno de esos factores. Entonces $p(b/a) = 0$. Luego, F es algebraicamente cerrado. □

Corolario 21.26. *Un cuerpo algebraicamente cerrado F no tiene extensiones algebraicas E con $E \neq F$.*

DEMOSTRACIÓN. Sea E una extensión algebraica de F; Entonces $F \subset E$. Para $\alpha \in E$, el polinomio minimal de α es $x - \alpha$. Por lo tanto, $\alpha \in F$ y $F = E$. □

Teorema 21.27. *Todo cuerpo F tiene una única clausura algebraica.*

Es un hecho no trivial que todo cuerpo tenga una única clausura algebraica. La demostración no es demasiado difícil, pero requiere algunas herramientas más sofisticadas de teoría de conjuntos. El lector interesado puede encontrar una demostración de este hecho en [3], [4], o [8].

Enunciamos ahora el Teorema Fundamental del Álgebra, demostrado por primera vez por Gauss a los 22 años de edad en su tesis doctoral. Este teorema dice que todo polinomio con coeficientes en los números complejos tiene una raíz en los números complejos. La demostración de este teorema se dará en el Capítulo 23.

Teorema 21.28 (Teorema Fundamental del Álgebra)**.** *El cuerpo de los números complejos es algebraicamente cerrado.*

21.2 Cuerpos de descomposición

Sea F un cuerpo y $p(x)$ un polinomio no constante en $F[x]$. Ya sabemos que podemos encontrar una extensión de cuerpos de F que contiene una raíz de $p(x)$. Sin embargo, quisiéramos saber si existe una extensión E de F que contenga todas las raíces de $p(x)$. En otras palabras, ¿podemos encontrar una extensión de cuerpos de F tal que $p(x)$ se fatoriza como productos de polinomios lineales? ¿Cuál es la "menor" extensión que contiene todas las raíces de $p(x)$?

Sea F un cuerpo y $p(x) = a_0 + a_1x + \cdots + a_nx^n$ un polinomio no constante en $F[x]$. Una extensión de cuerpos E de F es un ***cuerpo de descomposición*** de $p(x)$ si existen $\alpha_1, \ldots, \alpha_n$ en E tales que $E = F(\alpha_1, \ldots, \alpha_n)$ y

$$p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Un polinomio $p(x) \in F[x]$ ***se descompone*** en E si es producto de factores lineales en $E[x]$.

Ejemplo 21.29. Sea $p(x) = x^4 + 2x^2 - 8$ en $\mathbb{Q}[x]$. Entonces $p(x)$ tiene factores irreducibles $x^2 - 2$ y $x^2 + 4$. Por lo tanto, el cuerpo $\mathbb{Q}(\sqrt{2}, i)$ es un cuerpo de descomposición para $p(x)$.

Ejemplo 21.30. Sea $p(x) = x^3 - 3$ en $\mathbb{Q}[x]$. Entonces $p(x)$ tiene una raíz en el cuerpo $\mathbb{Q}(\sqrt[3]{3}\,)$. Sin embargo, este cuerpo no es un cuerpo de descomposición para $p(x)$ pues las raíces cúbicas complejas de 3,

$$\frac{-\sqrt[3]{3} \pm (\sqrt[6]{3}\,)^5 i}{2},$$

no están en $\mathbb{Q}(\sqrt[3]{3}\,)$.

Teorema 21.31. *Sea $p(x) \in F[x]$ un polinomio no constante. Entonces hay un cuerpo de descomposición E para $p(x)$.*

Demostración. Procederemos por inducción sobre el grado de $p(x)$. Si $\operatorname{gr} p(x) = 1$, entonces $p(x)$ es un polinomio lineal y $E = F$. Supongamos que el teorema es cierto para todos los polinomios de grado k con $1 \leq k < n$ y sea $\operatorname{gr} p(x) = n$. Podemos suponer que $p(x)$ es irreducible; de lo contrario, por la hipótesis de inducción, estamos listos. Por el Teorema 21.5, hay un cuerpo K tal que $p(x)$ tiene una raíz α_1 en K. Luego, $p(x) = (x - \alpha_1)q(x)$, con $q(x) \in K[x]$. Como $\operatorname{gr} q(x) = n-1$, hay un cuerpo de descomposición $E \supset K$ para $q(x)$ que contiene los ceros $\alpha_2, \ldots, \alpha_n$ de $p(x)$ por la hipótesis de inducción. Por lo tanto,

$$E = K(\alpha_2, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$$

es un cuerpo de descomposición para $p(x)$. □

Surge ahora la pregunta sobre la unicidad del cuerpo de descomposición. Esta pregunta tiene respuesta afirmativa. Dados dos cuerpos de descomposición K y L de un polinomio $p(x) \in F[x]$, hay un isomorfismo de cuerpos $\phi : K \to L$ que fija F. Para demostrar este resultado, comenzaremos con un lema.

Lema 21.32. *Sea $\phi : E \to F$ un isomorfismo de cuerpos. Sea K una extensión de cuerpos de E y $\alpha \in K$ algebraico sobre E con polinomio minimal $p(x)$. Supongamos que L es una extensión de cuerpos de F tal que β es raíz del polinomio en $F[x]$ obtenido a partir de $p(x)$ como imagen por ϕ. Entonces ϕ se extiende a un único isomorfismo $\overline{\phi} : E(\alpha) \to F(\beta)$ tal que $\overline{\phi}(\alpha) = \beta$ y $\overline{\phi}$ coincide con ϕ en E.*

DEMOSTRACIÓN. Si $p(x)$ tiene grado n, entonces por el Teorema 21.13 podemos escribir cualquier elemento en $E(\alpha)$ como combinación lineal de $1, \alpha, \ldots, \alpha^{n-1}$. Por lo tanto, el isomorfismo que buscamos debe ser

$$\overline{\phi}(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = \phi(a_0) + \phi(a_1)\beta + \cdots + \phi(a_{n-1})\beta^{n-1},$$

donde

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

es un elemento en $E(\alpha)$. El hecho de que $\overline{\phi}$ sea un isomorfismo se podría verificar de forma directa; sin embargo, es más fácil notar que $\overline{\phi}$ es una composición de funciones que ya sabemos que son homomorfismos.

Podemos extender ϕ a un isomorfismo de $E[x]$ a $F[x]$, que también denotaremos por ϕ, haciendo

$$\phi(a_0 + a_1x + \cdots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n.$$

Esta extensión coincide con el isomorfismo original $\phi : E \to F$, pues los polinomios constantes son enviados a polinomios constantes. Por hipótesis, $\phi(p(x)) = q(x)$; luego, ϕ envía $\langle p(x)\rangle$ en $\langle q(x)\rangle$. Por lo tanto, tenemos un isomorfismo $\psi : E[x]/\langle p(x)\rangle \to F[x]/\langle q(x)\rangle$. Por la Proposición 21.12, tenemos isomorfismos $\sigma : E[x]/\langle p(x)\rangle \to E(\alpha)$ y $\tau : F[x]/\langle q(x)\rangle \to F(\beta)$, definidos por evaluación en α y β, respectivamente. Por lo tanto, $\overline{\phi} = \tau\psi\sigma^{-1}$ es el isomorfismo requerido.

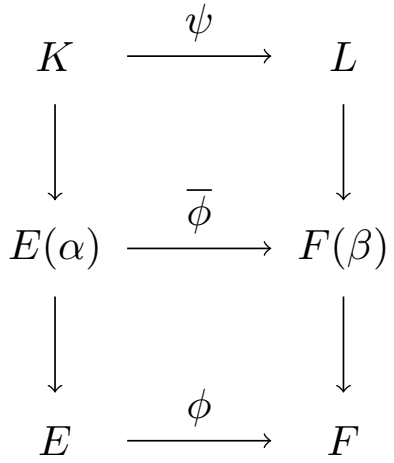
$$\begin{array}{ccc}
E[x]/\langle p(x)\rangle & \xrightarrow{\psi} & F[x]/\langle q(x)\rangle \\
\downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \tau} \\
E(\alpha) & \xrightarrow{\overline{\phi}} & F(\beta) \\
\downarrow & & \downarrow \\
E & \xrightarrow{\phi} & F
\end{array}$$

Dejamos la demostración de la unicidad como ejercicio. □

Teorema 21.33. *Sea $\phi : E \to F$ un isomorfismo de cuerpos y sea $p(x)$ un polinomio no constante en $E[x]$ y $q(x)$ el correspondiente polinomio en $F[x]$ bajo el isomorfismo. Si K es un cuerpo de descomposición para $p(x)$ y L es un cuerpo de descomposición para $q(x)$, entonces ϕ se extiende a un isomorfismo $\psi : K \to L$.*

DEMOSTRACIÓN. Procederemos por inducción en el grado de $p(x)$. Podemos suponer que $p(x)$ es irreducible sobre E. Por lo tanto, $q(x)$ también es irreducible sobre F. Si $\operatorname{gr} p(x) = 1$, entonces por la definición de cuerpo de descomposición, $K = E$ y $L = F$ y no hay nada que demostrar.

Supongamos que el teorema vale para todos los polinomios de grado menor a n. Como K es un cuerpo de descomposición para $p(x)$, todas la raíces de $p(x)$ están en K. Digamos que α es una de esas raíces, tal que $E \subset E(\alpha) \subset K$. De forma similar, podemos encontrar una raíz β de $q(x)$ en L tal que $F \subset F(\beta) \subset L$. Por el Lema 21.32, hay un isomorfismo $\overline{\phi} : E(\alpha) \to F(\beta)$ tal que $\overline{\phi}(\alpha) = \beta$ y $\overline{\phi}$ coincide con ϕ en E.



Escribamos ahora $p(x) = (x-\alpha)f(x)$ y $q(x) = (x-\beta)g(x)$, donde los grados de $f(x)$ y $g(x)$ son menores a los grados de $p(x)$ y $q(x)$, respectivamente. La extensión K es un cuerpo de descomposición para $f(x)$ sobre $E(\alpha)$, y L es un cuerpo de descomposición para $g(x)$ sobre $F(\beta)$. Por la hipótesis de inducción hay un isomorfismo $\psi : K \to L$ tal que ψ coincide con $\overline{\phi}$ en $E(\alpha)$. Luego, hay un isomorfismo $\psi : K \to L$ tal que ψ coincide con ϕ en E. □

Corolario 21.34. *Sea $p(x)$ un polinomio en $F[x]$. Entonces hay un cuerpo de descomposición K para $p(x)$ que es único salvo isomorfismo.*

21.3 Construcciones Geométricas

En la antigua Grecia, se propusieron tres problemas clásicos. Estos problemas son de naturaleza geométrica e involucran construcciones con regla y compás de lo que ahora constituye la geometría que se enseña en el colegio; es decir, solamente tenemos derecho a usar una regla y un compás para resolverlos. Los problemas pueden ser planteados como sigue.

1. Dado un ángulo arbitrario, ¿puede éste ser trisecado usando solamente regla y compás?

2. Dado un círculo arbitrario, ¿puede construirse un cuadrado de la misma área usando solamente regla y compás?

3. Dado un cubo, ¿puede construirse la arista de otro cubo cuyo volumen sea el doble del original usando solamente regla y compás?

Después de aproblemar a los matemáticos durante más de dos mil años, finalmente se ha demostrado que cada una de estas construcciones es imposible. Usaremos la teoría de cuerpos para dar una demostración de que las soluciones no existen. Es bastante sorprendente que las soluciones largamente buscadas a estos tres problemas finalmente se encuentren en el álgebra abstracta.

En primer lugar, determinemos más específicamente lo que queremos decir con una regla y un compás, y examinemos además la naturaleza de estos problemas un poco más en profundidad. Para empezar, la regla permitida *no tiene marcas*. No podemos medir distancias arbitrarias con esta regla. Es solamente una herramienta para trazar la recta que pasa por dos puntos. La afirmación de la imposibilidad de trisecar un ángulo arbitrario significa que existe al menos un ángulo que no se puede trisecar con regla y compás. Ciertamente algunos ángulos particulares sí se pueden trisecar. Podemos construir un ángulo de 30°;

por lo tanto, es posible trisecar un ángulo de 90°. Sin embargo, mostraremos que es imposible construir un ángulo de 20°. Por lo tanto, no podemos trisecar un ángulo de 60°.

Números Constructibles

Un número real α es ***constructible*** si podemos construir un segmento de longitud $|\alpha|$ en un número finito de pasos a partir de un segmento de longitud uno usando regla y compás exclusivamente.

Teorema 21.35. *El conjunto de todos los números reales constructibles forma un subcuerpo F del cuerpo de los números reales.*

DEMOSTRACIÓN. Sean α y β números constructibles. Debemos mostrar que $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, y α/β ($\beta \neq 0$) también son números constructibles. Podemos suponer que tanto α como β son positivos con $\alpha > \beta$. Es bastante claro como construir $\alpha + \beta$ y $\alpha - \beta$. Para encontrar un segmento de longitud $\alpha\beta$, supondremos que $\beta > 1$ y construiremos el triángulo de la Figura 21.36 de manera que los triángulos $\triangle ABC$ y $\triangle ADE$ sean semejantes. Como $\alpha/1 = x/\beta$, el segmento x tiene longitud $\alpha\beta$. Una construcción similar se puede hacer si $\beta < 1$. Dejaremos como ejercicio mostrar que el mismo triángulo puede ser usado para construir α/β si $\beta \neq 0$. □

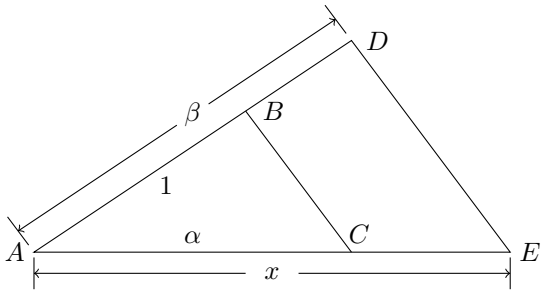


Figura 21.36: Construcción de productos

Lema 21.37. *Si α es un número constructible, entonces $\sqrt{\alpha}$ es un número constructible.*

DEMOSTRACIÓN. En la Figura 21.38 los triángulos $\triangle ABD$, $\triangle BCD$, y $\triangle ABC$ son semejantes; luego, $1/x = x/\alpha$, y $x^2 = \alpha$. □

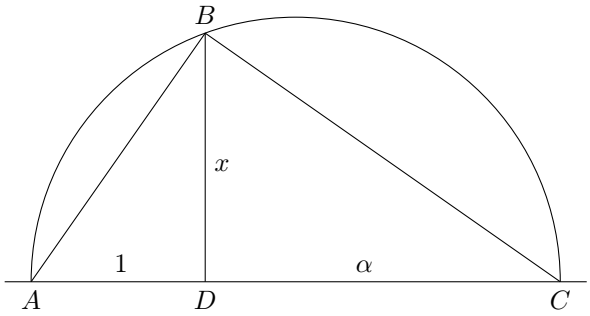


Figura 21.38: Construcción de raíces

Por el Teorema 21.35, podemos localizar en el plano cualquier punto $P = (p, q)$ que tenga coordenadas racionales p y q. Necesitamos saber qué otros puntos pueden ser construidos con regla y compás a partir de los puntos de coordenadas racionales.

Lema 21.39. *Sea F un subcuerpo de $\mathbb{R}$.*

1. *Si una recta contiene dos puntos con coordenadas en F, entonces satisface la ecuación $ax + by + c = 0$, con a, b, y c en F.*

2. *Si una circunferencia tiene su centro en un punto con coordenadas en F y su radio también está en F, entonces satisface la ecuación $x^2 + y^2 + dx + ey + f = 0$, con d, e, y f en F.*

Demostración. Sean (x_1, y_1) y (x_2, y_2) puntos en una recta con x_1, y_1, x_2, y_2 en F. Si $x_1 = x_2$, entonces una ecuación de la recta que pasa por los dos puntos es $x - x_1 = 0$, que tiene la forma $ax + by + c = 0$. Si $x_1 \neq x_2$, entonces una ecuación de la recta que pasa por los dos puntos es

$$y - y_1 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x - x_1),$$

que también puede ser puesta en la forma buscada.

Para demostrar la segunda parte del lema, supongamos que (x_1, y_1) es el centro de una circunferencia de radio r. Entonces una ecuación para la circunferencia es

$$(x - x_1)^2 + (y - y_1)^2 - r^2 = 0.$$

Esta ecuación puede ser fácilmente puesta en la forma buscada. □

Empezando por un cuerpo de números constructibles F, tenemos tres posibilidades para construir puntos adicionales en $\mathbb{R}^2$ usando regla y compás.

1. Para encontrar puntos, posiblemente nuevos, en $\mathbb{R}^2$, podemos tomar la intersección de dos rectas, cada una de las cuales pasa por dos puntos cuyas coordenadas están en F.

2. La intersección de una recta que pasa por dos puntos cuyas coordenadas están en F y un círculo cuyo centro tiene sus coordenadas en F con radio de longitud en F nos podrá dar nuevos puntos en $\mathbb{R}^2$.

3. Podemos obtener nuevos puntos en $\mathbb{R}^2$ intersectando dos círculos cuyos centros tengan coordenadas en F y cuyos radios tengan longitudes en F.

El primer caso no entrega nuevos puntos en $\mathbb{R}^2$, pues la solución de un sistema de dos ecuaciones de la forma $ax + by + c = 0$ con coeficientes en F siempre estará en F. El tercer caso se puede reducir al segundo. Sean

$$x^2 + y^2 + d_1x + e_1y + f_1 = 0$$
$$x^2 + y^2 + d_2x + e_2y + f_2 = 0$$

las ecuaciones de dos círculos, con d_i, e_i, y f_i en F para $i = 1, 2$. Estos círculos tienen la misma intersección que el círculo

$$x^2 + y^2 + d_1x + e_1x + f_1 = 0$$

y la recta

$$(d_1 - d_2)x + b(e_2 - e_1)y + (f_2 - f_1) = 0.$$

La última ecuación corresponde a la cuerda que pasa por los puntos de intersección de los dos círculos (cuando estos puntos existen). Por lo tanto, la intersección de dos círculos puede ser reducida al caso de la intersección de una recta con un círculo.

Considerando el caso de la intersección de una recta con un círculo, debemos determinar la naturaleza de las soluciones del sistema de ecuaciones

$$ax + by + c = 0$$
$$x^2 + y^2 + dx + ey + f = 0.$$

Si eliminamos y de estas ecuaciones, obtenemos una ecuación de la forma $Ax^2 + Bx + C = 0$, con A, B, y C en F. La coordenada x del punto de intersección está dada por

$$x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$$

y está en $F[\sqrt{\alpha}\,]$, con $\alpha = B^2 - 4AC > 0$. Hemos demostrado el siguiente lema.

Lema 21.40. *Sea F un cuerpo de números constructibles. Entonces los puntos determinados por la intersección de círculos y rectas en F están en el cuerpo $F[\sqrt{\alpha}\,]$ para algún α en F.*

Teorema 21.41. *Un número real α es un número constructible si y solo si hay una sucesión de cuerpos*

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_k$$

tales que $F_i = F_{i-1}(\sqrt{\alpha_i}\,)$ con $\alpha_i \in F_i$ y $\alpha \in F_k$. En particular, hay un entero $k > 0$ tal que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k$.

Demostración. La existencia de los F_i y de los α_i es una consecuencia directa del Lema 21.40 y el hecho de que

$$[F_k : \mathbb{Q}] = [F_k : F_{k-1}][F_{k-1} : F_{k-2}] \cdots [F_1 : \mathbb{Q}] = 2^k. \qquad \square$$

Corolario 21.42. *El cuerpo de todos los números constructibles es una extensión algebraica de $\mathbb{Q}$.*

Como podemos ver con el cuerpo de los número constructibles, no toda extensión algebraica de un cuerpo es una extensión finita.

Duplicando el cubo y cuadrando el círculo

Estamos listos para investigar los problemas clásicos de duplicación del cubo y de la cuadratura del círculo. Podemos usar el cuerpo de los números constructibles para determinar exactamente cuándo una construcción geométrica particular es posible.

Duplicar el cubo es imposible Dada la arista de un cubo, es imposible construir la arista de un cubo del doble de su volumen usando únciamente regla y compás. Digamos que el cubo original tiene una arista de longitud 1 y, por lo tanto, su volumen es 1. Si pudiéramos construir un cubo de volumen 2, entonces la arista de este nuevo cubo tendría longitud $\sqrt[3]{2}$. Sin embargo, $\sqrt[3]{2}$ es un cero del polinomio irreducible $x^3 - 2$ sobre $\mathbb{Q}$; luego,

$$[\mathbb{Q}(\sqrt[3]{2}\,) : \mathbb{Q}] = 3$$

Esto es imposible, pues 3 no es una potencia entera de 2.

Cuadrando el círculo Supongamos que tenemos un círculo de radio 1. El área del círculo es π; por lo tanto, debemos ser capaces de construir un cuadrado de lado $\sqrt{\pi}$. Esto es imposible pues π y por lo tanto $\sqrt{\pi}$ son ambos trascendentes. Por lo tanto no se puede construir un cuadrado de la misma área de un círculo usando regla y compás.

Trisecando un Ángulo

Trisecar un ángulo arbitrario es imposible. Demostraremos que es imposible construir un ángulo de 20°. Por lo tanto, un ángulo de 60° no puede ser trisecado. Primero obtendremos la fórmula del coseno para el ángulo triple:

$$\begin{aligned}\cos 3\theta &= \cos(2\theta + \theta) \\ &= \cos 2\theta \cos\theta - \sin 2\theta \sin\theta \\ &= (2\cos^2\theta - 1)\cos\theta - 2\sin^2\theta\cos\theta \\ &= (2\cos^2\theta - 1)\cos\theta - 2(1 - \cos^2\theta)\cos\theta \\ &= 4\cos^3\theta - 3\cos\theta.\end{aligned}$$

El ángulo θ pude ser construido si y solo si $\alpha = \cos\theta$ es constructible. Sea $\theta = 20°$. Entonces $\cos 3\theta = \cos 60° = 1/2$. Por la fórmula del coseno del ángulo triple,

$$4\alpha^3 - 3\alpha = \frac{1}{2}.$$

Por lo tanto, α es una raíz de $8x^3 - 6x - 1$. Este polinomio no tiene factores en $\mathbb{Z}[x]$, y por lo tanto es irreducible sobre $\mathbb{Q}[x]$. Luego, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Concluimos que α no es un número constructible.

Sage Las extensiones del cuerpo de los números racionales son objetos centrales en el estudio de teoría de números, de manera que con los orígenes de Sage en esta disciplina, no es ninguna sorpresa que los cuerpos y las extensiones de los racionales estén extensamente implementados. Sage también contiene una implementación del cuerpo de todos los números algebraicos, con representaciones exactas.

Nota Histórica

La Teoría Algebraica de números usa las herramientas del álgebra para resolver ciertos problemas en teoría de números. La teoría algebraica de números moderna comenzó con Pierre de Fermat (1601–1665). Ciertamente es posible encontrar muchos enteros positivos que satisfagan la ecuación $x^2 + y^2 = z^2$; Fermat conjecturó que la ecuación $x^n + y^n = z^n$ no tiene soluciones enteras positivas si $n \geq 3$. En su copia de la traducción latina del libro *Arithmetica* de Diofanto afirmó que había encontrado una demostración maravillosa de este teorema, pero que el margen del libro era muy angosto para conternerla. Basado en trabajos de otros matemáticos, fue Andrew Wiles quien finalmmente pudo probar el Último Teorema de Fermat en los 90'. El logro de Wiles fue destacado en la primera plana del *New York Times*.

Intentos de demostrar el Último Teorema de Fermat han llevado a contribuciones importantes a la teoría algebraica de números de parte de matemáticos tan notables como Leonhard Euler (1707–1783). Avances significativos en la comprensión del Último Teorema de Fermat fueron hechos por Ernst Kummer (1810–1893). Leopold Kronecker, un alumno de Kummer (1823–1891), se convirtió en uno de los pricipales algebristas del siglo XIX. La teoría de ideales de

Kronecker y su estudio de teoría algebraica de números contribuyó mucho a la comprensión de los cuerpos.

David Hilbert (1862–1943) y Hermann Minkowski (1864–1909) están entre los matemáticos que lideraron el área a comienzos del siglo XX. Hilbert y Minkowski trabajaban en la Universidad de Göttingen en Alemania. Göttingen fue uno de los más importantes centros de investigación en matemáticas durante los últimos dos siglos. El gran número de matemáticos excepcionales que estudiaron allí incluye a Gauss, Dirichlet, Riemann, Dedekind, Noether y Weyl.

André Weil contestó preguntas en teoría de números usando geometría algebraica, un área de las matemáticas que estudia geometría estudiando anillos conmutativos. Desde 1955 hasta 1970, Alexander Grothendieck dominó el área de la geometría algebraica. Pierre Deligne, un alumno de Grothendieck, resolvió varias de las conjeturas de Weil en teoría de números. Una de las más recientes contribuciones al álgebra y a la teoría de números es la demostración por parte de Gerd Falting de la conjetura de Mordell-Weil . Esta conjetura de Mordell y Weil esencialmente dice que ciertos polinomios $p(x, y)$ en $\mathbb{Z}[x, y]$ tienen solamente un número finito de soluciones enteras.

21.4 Ejercicios

1. Muestre que cada uno de los siguientes números es algebraico sobre $\mathbb{Q}$ encontrando su polinomio minimal sobre $\mathbb{Q}$.

(a) $\sqrt{1/3 + \sqrt{7}}$

(b) $\sqrt{3} + \sqrt[3]{5}$

(c) $\sqrt{3} + \sqrt{2}\, i$

(d) $\cos\theta + i \sin\theta$ for $\theta = 2\pi/n$ with $n \in \mathbb{N}$

(e) $\sqrt{\sqrt[3]{2} - i}$

2. Encuentre una base para cada una de las siguientes extensiones de cuerpos. ¿Cuál es el grado de esta extensión?

(a) $\mathbb{Q}(\sqrt{3}, \sqrt{6}\,)$ sobre $\mathbb{Q}$

(b) $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}\,)$ sobre $\mathbb{Q}$

(c) $\mathbb{Q}(\sqrt{2}, i)$ sobre $\mathbb{Q}$

(d) $\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7}\,)$ sobre $\mathbb{Q}$

(e) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}\,)$ sobre $\mathbb{Q}$

(f) $\mathbb{Q}(\sqrt{8}\,)$ sobre $\mathbb{Q}(\sqrt{2}\,)$

(g) $\mathbb{Q}(i, \sqrt{2} + i, \sqrt{3} + i)$ sobre $\mathbb{Q}$

(h) $\mathbb{Q}(\sqrt{2} + \sqrt{5}\,)$ sobre $\mathbb{Q}(\sqrt{5}\,)$

(i) $\mathbb{Q}(\sqrt{2}, \sqrt{6} + \sqrt{10}\,)$ sobre $\mathbb{Q}(\sqrt{3} + \sqrt{5}\,)$

3. Encuentre el cuerpo de descomposición de cada uno de los siguientes polinomios.

(a) $x^4 - 10x^2 + 21$ sobre $\mathbb{Q}$

(b) $x^4 + 1$ sobre $\mathbb{Q}$

(c) $x^3 + 2x + 2$ sobre $\mathbb{Z}_3$

(d) $x^3 - 3$ sobre $\mathbb{Q}$

4. Considere el cuerpo de extensión $\mathbb{Q}(\sqrt[4]{3}, i)$ sobre $\mathbb{Q}$.

(a) Encuentre una base para el cuerpo de extensión $\mathbb{Q}(\sqrt[4]{3}, i)$ sobre $\mathbb{Q}$. Concluya que $[\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}] = 8$.

(b) Encuentre todos los subcuerpos F de $\mathbb{Q}(\sqrt[4]{3}, i)$ tal que $[F : \mathbb{Q}] = 2$.

(c) Encuentre todos los subcuerpos F de $\mathbb{Q}(\sqrt[4]{3}, i)$ tal que $[F : \mathbb{Q}] = 4$.

5. Demuestre que $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ es un cuerpo con 8 elementos. Construya una tabla de multiplicación para el grupo multiplicativo del cuerpo.

6. Demuestre que el polígono regular de 9 lados no es constructible con regla y compas, pero el de 20 lados sí es constructible.

7. Demuestre que el coseno de un grado ($\cos 1^\circ$) es algebraico sobre $\mathbb{Q}$ pero no es constructible.

8. ¿Se puede construir un cubo con tres veces el volumen de un cubo dado?

9. Demuestre que $\mathbb{Q}(\sqrt{3}, \sqrt[4]{3}, \sqrt[8]{3}, \ldots)$ es una extensión algebraica de $\mathbb{Q}$ pero no es una extensión finita.

10. Demuestre o refute: π es algebraico sobre $\mathbb{Q}(\pi^3)$.

11. Sea $p(x)$ un polinomio no constante de grado n en $F[x]$. Demuestre que existe un cuerpo de descomposición E para $p(x)$ tal que $[E : F] \leq n!$.

12. Demuestre o refute: $\mathbb{Q}(\sqrt{2}\,) \cong \mathbb{Q}(\sqrt{3}\,)$.

13. Demuestre que los cuerpos $\mathbb{Q}(\sqrt[4]{3}\,)$ and $\mathbb{Q}(\sqrt[4]{3}\,i)$ son isomorfos pero no iguales.

14. Sea K una extensión algebraica de E, y E una extensión algebraica de F. Demuestre que K es algebraico sobre F. [*Cuidado*: No suponga que las extensiones son finitas.]

15. Demuestre o refute: $\mathbb{Z}[x]/\langle x^3 - 2\rangle$ es un cuerpo.

16. Sea F un cuerpo de característica p. Demuestre que $p(x) = x^p - a$ es irreducible o se descompone completamente en F.

17. Sea E la clausura algebraica de un cuerpo F. Demuestre que todo polinomio $p(x)$ en $F[x]$ se descompone completamente en E.

18. Si todo polinomio irreducible $p(x)$ en $F[x]$ es lineal, demuestre que F es un cuerpo algebraicamente cerrado.

19. Demuestre que si α y β son números constructibles tales que $\beta \neq 0$, entonces también lo es α/β.

20. Demuestre que el conjunto de todos los elementos en $\mathbb{R}$ que son algebraicos sobre $\mathbb{Q}$ forma una extensión de cuerpos de $\mathbb{Q}$ que no es finita.

21. Sea E una extensión algebraica de un cuerpo F, y sea σ un automorfismo de E que fija F. Sea $\alpha \in E$. Demuestre que σ induce una permutación del conjunto de ceros del polinomio minimal de α que están en E.

22. Muestre que $\mathbb{Q}(\sqrt{3}, \sqrt{7}\,) = \mathbb{Q}(\sqrt{3} + \sqrt{7}\,)$. Extienda su demostración para demostrar que $\mathbb{Q}(\sqrt{a}, \sqrt{b}\,) = \mathbb{Q}(\sqrt{a} + \sqrt{b}\,)$, donde $\text{mcd}(a, b) = 1$.

23. Sea E una extensión finita de un cuerpo F. Si $[E : F] = 2$, demuestre que E es un cuerpo de descomposición sobre F para algún polinomio $f(x) \in F[x]$.

24. Demuestre o refute: Dado un polinomio $p(x)$ en $\mathbb{Z}_6[x]$, es posible construir un anillo R tal que $p(x)$ tiene una raíz en R.

25. Sea E una extensión de F y $\alpha \in E$. Determine $[F(\alpha) : F(\alpha^3)]$.

26. Sean α, β trascendente sobre $\mathbb{Q}$. Pruebe que al menos uno de $\alpha\beta$ y $\alpha + \beta$ también es trascendente.

27. Sea E una extensión de cuerpos de F y sea $\alpha \in E$ trascendente sobre F. Demuestre que cada elemento en $F(\alpha)$ que no está en F también es trascendente sobre F.

28. Sea α una raíz de un polinomio irreducible $p(x) \in F[x]$, con $\operatorname{gr} p = n$. Demuestre que $[F(\alpha) : F] = n$.

21.5 Referencias y Lecturas sugeridas

[1] Dean, R. A. *Elements of Abstract Algebra.* Wiley, New York, 1966.

[2] Dudley, U. *A Budget of Trisections.* Springer-Verlag, New York, 1987. An interesting and entertaining account of how not to trisect an angle.

[3] Fraleigh, J. B. *A First Course in Abstract Algebra.* 7th ed. Pearson, Upper Saddle River, NJ, 2003.

[4] Kaplansky, I. *Fields and Rings*, 2nd ed. University of Chicago Press, Chicago, 1972.

[5] Klein, F. *Famous Problems of Elementary Geometry.* Chelsea, New York, 1955.

[6] Martin, G. *Geometric Constructions.* Springer, New York, 1998.

[7] H. Pollard and H. G. Diamond. *Theory of Algebraic Numbers*, Dover, Mineola, NY, 2010.

[8] Walker, E. A. *Introduction to Abstract Algebra.* Random House, New York, 1987. This work contains a proof showing that every field has an algebraic closure.

21.6 Sage

En Sage, y otros lugares, una extensión de los racionales se llama "cuerpo de números." Los cuerpos de números están entre la características más consolidadas de Sage.

Cuerpos de números

Hay varias formas de crear un cuerpo de números. Estamos familiarizados con la sintaxis donde adjuntamos un número irracional que podamos describir con combinaciones de raíces y operaciones aritméticas.

```
M.<a> = QQ[sqrt(2)+sqrt(3)]; M
```

```
Number Field in a with defining polynomial x^4 - 10*x^2 + 1
```

Podemos también especificar el elemento que deseamos adjuntar como una raíz de un polinomio irreducible. Una posibilidad es construir primero el anillo de polinomios de manera que el polinomio tenga la ubicación de sus coeficientes determinada de forma explícita.

```
F.<y> = QQ[]
p = y^3 - 1/4*y^2 - 1/16*y + 1/4
p.is_irreducible()
```

```
True
```

```
N.<b> = NumberField(p, 'b'); N
```

```
Number Field in b with
defining polynomial y^3 - 1/4*y^2 - 1/16*y + 1/4
```

En lugar de construir todo el anillo de polinomios, podemos simplemente introducir una variable como el generador de un anillo de polinomios y luego crear los polinomios a partir de esta variable. Esto nos libera de ponerle un nombre al anillo de polinomios. Note que en este ejemplo ambas instancias de `z` son necesarias.

```
z = polygen(QQ, 'z')
q = z^3 - 1/4*z^2 - 1/16*z + 1/4
q.parent()
```

```
Univariate Polynomial Ring in z over Rational Field
```

```
P.<c> = NumberField(q, 'c'); P
```

```
Number Field in c with
defining polynomial z^3 - 1/4*z^2 - 1/16*z + 1/4
```

Podemos recuperar el polinomio usado para definir un cuerpo de números, incluso si fue construido con la especificación de un elemento irracional. En este caso, el polinomio corresponde al polinomio minimal del elemento.

```
M.polynomial()
```

```
x^4 - 10*x^2 + 1
```

```
N.polynomial()
```

```
y^3 - 1/4*y^2 - 1/16*y + 1/4
```

Para cualquier elemento de un cuerpo de números, Sage es capaz de calcular su polinomio minimal.

```
elemento = -b^2 + 1/3*b + 4
elemento.parent()
```

```
Number Field in b with
defining polynomial y^3 - 1/4*y^2 - 1/16*y + 1/4
```

```
r = elemento.minpoly('t'); r
```

```
t^3 - 571/48*t^2 + 108389/2304*t - 13345/216
```

```
r.parent()
```

```
Univariate Polynomial Ring in t over Rational Field
```

```
r.subs(t=elemento)
```

```
0
```

Reemplazar el `elemento` en su presunto polinomio minimal y obtener 0 no es evidencia suficiente para demostrar que es realmente el polinomio *minimal*, pero al menos es tranquilizador.

Cuerpos de Números Absolutos y Relativos

En Sage podemos adjuntar varios elementos de forma simultánea y podemos crear torres anidadas de cuerpos de números. Sage usa el término "absoluto" para referirse a un cuerpo de números como una extensión de los racionales, y el término "relativo" para referirse a un cuerpo de números construido, o visto, como una extensión de otro cuerpo de números (no trivial).

```
A.<a,b> = QQ[sqrt(2), sqrt(3)]
A
```

```
Number Field in sqrt2 with defining polynomial x^2 - 2 over
its base field
```

```
B = A.base_field(); B
```

```
Number Field in sqrt3 with defining polynomial x^2 - 3
```

```
A.is_relative()
```

```
True
```

```
B.is_relative()
```

```
False
```

El cuerpo de números `A` fue construido como lo que escribiríamos $\mathbb{Q} \subset \mathbb{Q}[\sqrt{3}] \subset \mathbb{Q}[\sqrt{3}, \sqrt{2}]$. Notemos la ligera diferencia en el orden de los elementos adjuntados, y notemos como los cuerpos de números utilizan nombres internos algo más sofisticados (`sqrt2`, `sqrt3`) para los nuevos elementos.

Podemos "aplanar" un cuerpo relativo para verlo como un cuerpo absoluto, lo que podría haber sido nuestra intención desde el comienzo. Aquí crearemos un nuevo cuerpo de números a partir de `A` que lo hace un cuerpo de números absoluto.

```
C.<c> = A.absolute_field()
C
```

```
Number Field in c with defining polynomial x^4 - 10*x^2 + 1
```

Una vez que construimos un cuerpo de números absoluto de esta manera, podemos recuperar isomorfismos hacia y desde el cuerpo absoluto. Recordemos que nuestra torre fue construida por generadores `a` y `b`, mientras la torre aplanada es generada por `c`. El método `.structure()` entrega dos funciones, con el cuerpo absoluto como dominio y codominio (en este orden).

```
fromC, toC = C.structure()
fromC(c)
```

```
sqrt2 - sqrt3
```

```
toC(a)
```

```
1/2*c^3 - 9/2*c
```

```
toC(b)
```

```
1/2*c^3 - 11/2*c
```

Esto nos dice que el generador, `c`, es igual a $\sqrt{2} - \sqrt{3}$, y que, tanto $\sqrt{2}$ como $\sqrt{3}$ pueden ser expresadas como funciones polinomiales de `c`. Con estas conexiones, le sugerimos desarrollar a mano las dos expresiones finales en `c`, y de esa manera apreciar mejor el trabajo que Sage hace al determinarlas por nosotros. Este cálculo es un ejemplo de la conclusión del Teorema 23.12 que viene a continuación.

Muchos de los métodos para cuerpos de números tienen tanto una versión absoluta como una relativa, y según lo que queramos hacer, será más cómodo trabajar en la torre o en la versión plana, de manera que los isomorfismos entre ambas serán de gran valor para traducir tanto las preguntas como las respuestas.

Como espacio vectorial sobre $\mathbb{Q}$, o sobre otro cuerpo de números, los cuerpos de números son extensiones finitas y tienen una dimensión, llamada grado. Estos grados son fáciles de obtener en Sage, aunque en el caso de cuerpos relativos deberemos ser más precisos sobre cuál es el grado buscado.

```
B.degree()
```

```
2
```

```
A.absolute_degree()
```

```
4
```

```
A.relative_degree()
```

```
2
```

Cuerpos de descomposición

Acá hay un ejemplo concreto de cómo usar Sage para construir el cuerpo de descomposición de un polinomio. Consideremos $p(x) = x^4 + x^2 - 1$. Primero construiremos un cuerpo de números con una raíz, para luego factorizar el polinomio sobre este nuevo cuerpo.

```
x = polygen(QQ, 'x')
p = x^4 + x^2 - 1
p.parent()
```

```
Univariate Polynomial Ring in x over Rational Field
```

```
p.is_irreducible()
```

```
True
```

```
M.<a> = NumberField(p, 'a')
y = polygen(M, 'y')
p = p.subs(x = y)
p
```

```
y^4 + y^2 - 1
```

```
p.parent()
```

```
Univariate Polynomial Ring in y over Number Field in a with
defining polynomial x^4 + x^2 - 1
```

```
p.factor()
```

```
(y - a) * (y + a) * (y^2 + a^2 + 1)
```

```
a^2 + 1 in QQ
```

```
False
```

Así nuestro polinomio se factoriza parcialmente en dos factores lineales y uno cuadrático. Pero notemos que el factor cuadrático tiene un coeficiente irracional, $a^2 + 1$, de manera que el factor cuadrático pertenece estrictamente al anillo de polinomios sobre `M` y no sobre `QQ`.

Construiremos una extensión que contenga una raíz del factor cuadrático, lamado `q` acá. Entonces, en lugar de usar la función `polygen()`, construiremos todo un anillo de polinomios `R` sobre `N` con la variable `z`. La razón para hacer esto es que podemos ilustrar como "subir" el polinomio `p` con la sintaxis `R(p)` para pasar de tener coeficientes en `M` a tenerlos en `N`.

```
q = y^2 + a^2 + 1
N.<b> = NumberField(q, 'b')
R.<z> = N[]
s = R(p)
s
```

```
z^4 + z^2 - 1
```

```
s.parent()
```

```
Univariate Polynomial Ring in z over Number Field in b with
defining polynomial y^2 + a^2 + 1 over its base field
```

```
s.factor()
```

```
(z + b) * (z + a) * (z - a) * (z - b)
```

```
a in N, b in N
```

```
(True, True)
```

Así tenemos un cuerpo, `N`, en el que nuestro polinomio se factoriza con todos sus factores lineales. Podemos obtener otra factorización convirtiendo `N` en un cuerpo absoluto y factorizando ahí. Necesitaremos recrear el polinomio sobre `N`, pues una sustitución llevaría elementos del anillo equivocado.

```
P.<c> = N.absolute_field()
w = polygen(P, 'w')
p = w^4 + w^2- 1
p.factor()
```

```
(w - 7/18966*c^7 + 110/9483*c^5 +  923/9483*c^3 +
    3001/6322*c) *
(w - 7/37932*c^7 +  55/9483*c^5 + 923/18966*c^3 -
    3321/12644*c) *
(w + 7/37932*c^7 -  55/9483*c^5 - 923/18966*c^3 +
    3321/12644*c) *
(w + 7/18966*c^7 - 110/9483*c^5 -  923/9483*c^3 -
    3001/6322*c)
```

Esta es una alternativa interesante, en tanto que las raíces del polinomio son expresiones polinomiales en términos de un solo generador `c`. Como las raíces involucran potencias séptimas de `c`, podemos sospechar (pero no estar seguros) que el polinomio minimal de `c` tiene grado 8 y que `P` es una extensión de grado 8 de los racionales. De hecho `P` (o `N`) es un cuerpo de descomposición para $p(x) = x^4 + x^2 - 1$. Sus raíces no son realmente tan horribles como parecen — devolvámoslas al cuerpo relativo.

Primero queremos reescribir un factor (el primero) en la forma $(w - r)$ para identificar la raíz con los signos correctos.

```
(w -  7/18966*c^7 + 110/9483*c^5 + 923/9483*c^3 +
    3001/6322*c) =
(w - (7/18966*c^7 - 110/9483*c^5 - 923/9483*c^3 -
    3001/6322*c))
```

Con los isomorfismos de conversión, podemos reconocer las raíces por lo que son.

```
fromP, toP = P.structure()
fromP(7/18966*c^7 - 110/9483*c^5 - 923/9483*c^3 -
    3001/6322*c)
```

```
-b
```

Así la expresión complicada en términos de `c` es simplemente el opuesto de la raíz adjuntada en el segundo paso de la construcción de la torre de cuerpos de números. Sería un buen ejercicio ver lo que le pasa a las otras tres raíces (teniendo cuidado de escribir correctamente los signos para cada raíz).

Esta es una buena oportunidad para ilustrar el Teorema 21.17.

```
M.degree()
```

```
4
```

```
N.relative_degree()
```

```
2
```

```
P.degree()
```

```
8
```

```
M.degree()*N.relative_degree() == P.degree()
```

```
True
```

Números Algebraicos

El Corolario 21.24 dice que el conjunto de *todos* los números algebraicos forma un cuerpo. Este cuerpo está implementado en Sage como `QQbar`. Esto permite encontrar raíces de polinomios como números exactos que se muestran como aproximaciones.

```
x = polygen(QQ, 'x')
p = x^4 + x^2 - 1
r = p.roots(ring=QQbar); r
```

```
[(-0.7861513777574233?,  1), (0.7861513777574233?,  1),
 (-1.272019649514069?*I, 1), (1.272019649514069?*I, 1)]
```

Así hemos pedido las raíces de un polinomio con coeficientes racionales, especificando que queremos cualquier raíz que pudiera estar fuera de los racionales y dentro del cuerpo de los algebraicos. Como el cuerpo de los números algebraicos contiene todas estas raíces, obtenemos las cuatro raíces del polinomio de grado cuatro. Estas raíces están calculadas de manera de estar en un intervalo y el signo de interrogación indica que los dígitos anteriores son correctos. (Los enteros que siguen a cada una de las raíces, indican la multiplicidad con que ocurre esa raíz. Use la opción `multiplicities=False` para que no aparezcan.) Veamos tras bambalinas como Sage se las arregla con el cuerpo de números algebraicos.

```
r1 = r[0][0]; r1
```

```
-0.7861513777574233?
```

```
r1.as_number_field_element()
```

```
(Number Field in a with defining polynomial y^4 + y^2 - 1, a,
    Ring morphism:
    From: Number Field in a with defining polynomial y^4 +
        y^2 - 1
    To:   Algebraic Real Field
    Defn: a |--> -0.7861513777574233?)
```

Tres cosas están asociadas con esta primera raíz. En primer lugar un cuerpo de números, con generador `a` y un polinomio similar pero no idéntico al polinomio del cual estamos buscando las raíces. En segundo lugar hay una expresión en el generador `a`, que representa la raíz específica. En este caso, la expresión es simple, pero podría ser más complicada en otros ejemplos. Finalmente, hay un homomorfismo del cuerpo de números al "Algebraic Real Field", `AA`, que es el subcuerpo de `QQbar` que contiene solamente números reales, que asocia al generador `a` con el número `-0.7861513777574233?`. Verifiquemos, de dos formas diferentes, que la raíz dada realmente es una raíz.

```
r1^4 + r1^2 - 1
```

```
0
```

```
N, rexact, homomorphism = r1.as_number_field_element()
(rexact)^4 + rexact^2 - 1
```

```
0
```

Ahora que tenemos suficiente teoría para entender el cuerpo de los números algebraicos, y una forma natural de representarlos de forma exacta, podemos considerar las operaciones en el cuerpo. Si tomamos dos números algebraicos y los sumamos, obtenemos otro número algebraico (Corolario 21.24). ¿Cuál es entonces el polinomio minimal resultante? ¿Cómo se obtiene en Sage? Podríamos leer el código fuente si estamos interesados en la respuesta.

Construcciones geométricas

Sage puede hacer muchas cosas, pero aún no es capaz de trazar rectas con regla y compás. Sin embargo, podemos rápidamente determinar que trisectar un ángulo de 60 grados es imposible. Adjuntamos el coseno de un ángulo de

20 grados (en radianes) a los racionales, determinamos el grado de la exensión, y verificamos que no es una potencia entera de 2. Todo en una línea. Bien!

```
log(QQ[cos(pi/9)].degree(), 2) in ZZ
```

```
False
```

21.7 Ejercicios en Sage

1. Construya el polinomio $p(x) = x^5 + 2x^4 + 1$ sobre $\mathbb{Z}_3$. Verifique que no tiene ningún factor lineal evaluando $p(x)$ en cada elemento de $\mathbb{Z}_3$, y después verifique que $p(x)$ es irreducible.
Construya un cuerpo finito de orden 3^5 con el comando `FiniteField()`, pero incluya la opción `modulus` asignando el polinomio $p(x)$ para cambiar la elección automática.
Redefina $p(x)$ como polinomio sobre este cuerpo. Verifique cada uno de los $3^5 = 243$ elementos del cuerpo para ver si son raíces del polinomio y liste todos los elementos que lo sean. Finalmente, pida que Sage factorice $p(x)$ sobre el cuerpo, y comente sobre la relación entre su lista de raíces y su factorización.

2. Este problema continúa el anterior. Construya el anillo de polinomios sobre $\mathbb{Z}_3$ y en este anillo use $p(x)$ para generar un ideal principal. Finalmente construya el cociente del anillo de polinomios por este ideal. Como el polinomio es irreducible, este cociente es un cuerpo, y por la Proposición 21.12 este cociente es isomorfo al cuerpo de números del ejercicio anterior.
Usando sus resultados del ejercicio anterior, construya cinco raíces del polinomio $p(x)$ en este anillo cociente, pero ahora como expresiones en el generador del anillo cociente (que técnicamente es una clase lateral). Use Sage para verificar que de hecho son raíces. Esto ilustra el uso de un anillo cociente para crear un cuerpo de descomposición para un polinomio irreducible sobre un cuerpo finito.

3. La subsección Elementos Algebraicos se basa en álgebra lineal y contiene el Teorema 21.15: toda extensión finita es una extensión algebraica. Este ejercicio le ayudará a entender esa demostración.
El polinomio $r(x) = x^4 + 2x + 2$ es irreducible sobre los racionales (Criterio de Eisenstein con primo $p = 2$). Construya un cuerpo de números que contenga una raíz de $r(x)$. Por el Teorema 21.15, y la observación que le sigue, todo elemento de esta extensión finita es un número algebraico, y por ende satisface algún polinomio sobre el cuerpo base (es el polinomio que Sage produce con el método `.minpoly()`). Este ejercicio le mostrará cómo podemos usar álgebra lineal para determinar este polinomio minimal.
Supongamos que `a` es el generador del cuerpo de números que acaba de crear con $r(x)$. Determinaremos el polinomio minimal de `t = 3a + 1` usando solamente álgebra lineal. De acuerdo a la demostración, las primeras cinco potencias de `t` (empiece contando de cero) serán linealmente dependientes. (¿Por qué?) De esta manera una relación de dependencia lineal de estas potencias entregará los coeficientes de un polinomio con `t` como raíz. Calcule estas cinco potencias, luego construya el sistema lineal apropiado para determinar los coeficientes del polinomio minimal, resuelva el sistema, e interprete sus soluciones.
Ayudas: Los comandos `vector()` y `matrix()` crearán vectores y matrices, y el método `.solve_right()` para matrices puede ser usado para encontrar soluciones. Dado un elemento del cuerpo de números, que necesariamente corresponderá a un polinomio en el generador `a`, el método `.vector()` del elemento, entregará los coeficientes de este polinomio en una lista.

4. Construya el cuerpo de descomposición de $s(x) = x^4 + x^2 + 1$ y encuentre una factorización de $s(x)$ sobre este cuerpo como producto de factores lineales.

5. Forme el cuerpo de números, K, que contenga una raíz del polinomio irreducible $q(x) = x^3 + 3x^2 + 3x - 2$. Póngale un nombre a su raíz `a`. Verifique que $q(x)$ se factoriza, pero no se descompone, sobre K. Con K como cuerpo base, forme una extensión de K donde el factor cuadrático de $q(x)$ tiene una raíz. Póngale un nombre a esta raíz `b`, y llame L a esta segunda extensión de la torre.
Use `M.<c> = L.absolute_field()` formar una versión plana de la torre que será el cuerpo de números absoluto `M`. Encuentre el polinomio que define a `M` usando el método `.polynomial()`. A partir de este polinomio, que debe tener al generador `c` como raíz, debe ser capaz de usar álgebra elemental para escribir el generador como una expresión relativamente simple.
M debería ser el cuerpo de descomposición de $q(x)$. Para ver esto, vuelve a comenzar, y construya un nuevo cuerpo de números, P, usando la expresión simple para `c` que acaba de encontrar. Use `d` como el nombre de la raíz usada para construir `P`. Como `d` es una raíz del polinomio minimal de `c`, debería ser capaz de escribir una expresión para `d` que un alumno de pre-cálculo pueda reconocer.
Ahora factorice el polinomio original $q(x)$ (con coeficientes racionales) sobre P, para verificar que se descompone completamente (como era de esperar). Usando esta factorización, y su expresión simple para `d` escriba expresiones simplificadas para las tres raíces de $q(x)$. Determine si es capaz de convertir entre las dos versiones de las raíces "a mano", y sin usar los isomorfismos proveídos por el método `.structure()` en `M`.

22

Cuerpos Finitos

Los cuerpos finitos aparecen en muchas aplicaciones del álgebra, incluyendo teoría de códigos y criptografía. Ya conocemos un cuerpo finito, $\mathbb{Z}_p$, donde p es primo. En este capítulo mostraremos que existe un único cuerpo finito de orden p^n para cada primo p y para cada entero positivo n. Los cuerpos finitos también son llamados cuerpos de Galois en honor a Évariste Galois, quién fue uno de los primero matemáticos en investigarlos.

22.1 Estructura de Cuerpos Finitos

Recuerde que un cuerpo F tiene ***característica*** p si p es el menor entero positivo tal que para cada elemento no nulo α en F, tenemos $p\alpha = 0$. Si no hay tal entero, entonces F tiene característica 0. Del Teorema 16.19 sabemos que p debe ser primo. Supongamos que F es un cuerpo finito con n elementos. Entonces $n\alpha = 0$ para todo α en F. En consecuencia, la característica de F debe ser p, con p un primo que divide a n. Esta discusión se resume en la siguiente proposición.

Proposición 22.1. *Si F es un cuerpo finito, entonces la característica de F es p, con p primo.*

En todo este capítulo supondremos que p es un primo a menos que indiquemos lo contrario.

Proposición 22.2. *Si F es un cuerpo finito de característica p, entonces el orden de F es p^n para algún $n \in \mathbb{N}$.*

Demostración. Sea $\phi : \mathbb{Z} \to F$ el homomorfismo de anillos definido por $\phi(n) = n \cdot 1$. Como la característica de F es p, el núcleo de ϕ debe ser $p\mathbb{Z}$ y la imagen de ϕ debe ser un subcuerpo de F isomorfo a $\mathbb{Z}_p$. Denotaremos este subcuerpo por K. Como F es un cuerpo finito, debe ser una extensión finita de K y, por lo tanto, una extensión algebraica de K. Supongamos que $[F : K] = n$ es la dimensión de F, donde F es un K espacio vectorial. Deben existir elementos $\alpha_1, \ldots, \alpha_n \in F$ tales que cualquier elemento α en F pueda ser escrito de una única manera en la forma

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n,$$

donde los a_i están en K. Como hay p elementos en K, hay p^n combincaciones lineales posibles de los α_i. Por lo tanto, el orden de F debe ser p^n. □

Lema 22.3 (El sueño del Pibe)**.** *Sea p un primo y sea D un dominio integral de característica p. Entonces*

$$a^{p^n} + b^{p^n} = (a + b)^{p^n}$$

para todo entero positivo n.

DEMOSTRACIÓN. Procederemos por inducción en n. Podemos usar la fórmula del binomio (vea el Capítulo 2, Ejemplo 2.4) para verificar el caso $n = 1$; es decir,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}.$$

Si $0 < k < p$, entonces

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

debe ser divisible por p, pues p no puede dividir a $k!(p-k)!$. Note que D es un dominio integral de característica p, así es que todos los términos de la suma, salvo el primero y el último son cero. Por lo tanto, $(a+b)^p = a^p + b^p$.

Ahora supongamos que el resultado se cumple para todo k, con $1 \leq k \leq n$. Por la hipótesis de inducción,

$$(a+b)^{p^{n+1}} = ((a+b)^p)^{p^n} = (a^p + b^p)^{p^n} = (a^p)^{p^n} + (b^p)^{p^n} = a^{p^{n+1}} + b^{p^{n+1}}.$$

Por lo tanto, el lema es verdadero para $n+1$ y la demostración está completa. □

Sea F un cuerpo. Un polinomio $f(x) \in F[x]$ de grado n es ***separable*** si tiene n raíces distintas en el cuerpo de descomposición de $f(x)$; es decir, $f(x)$ es separable cuando se factoriza en factores lineales distintos sobre el cuerpo de descomposición de f. Una extensión E de F es una ***extensión separable*** de F si todo elemento en E es la raíz de un polinomio separable en $F[x]$.

Ejemplo 22.4. El polinomio $x^2 - 2$ es separable sobre $\mathbb{Q}$ pues se factoriza como $(x - \sqrt{2}\,)(x + \sqrt{2}\,)$. De hecho, $\mathbb{Q}(\sqrt{2}\,)$ es una extensión separable de $\mathbb{Q}$. Sea $\alpha = a + b\sqrt{2}$ un elemento cualquiera en $\mathbb{Q}(\sqrt{2}\,)$. Si $b = 0$, entonces α es una raíz de $x - a$. Si $b \neq 0$, entonces α es la raíz del polinomio separable

$$x^2 - 2ax + a^2 - 2b^2 = (x - (a + b\sqrt{2}\,))(x - (a - b\sqrt{2}\,)).$$

Afortunadamente, tenemos una forma fácil para determinar la separabilidad de cualquier polinomio. Sea

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

un polinomio en $F[x]$. Se define la ***derivada*** de $f(x)$ como

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

Lema 22.5. *Sea F un cuerpo y $f(x) \in F[x]$. Entonces $f(x)$ es separable si y solo si $f(x)$ y $f'(x)$ son relativamente primos.*

DEMOSTRACIÓN. Sea $f(x)$ separable. Entonces $f(x)$ se factoriza sobre algún cuerpo de extensión de F como $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, con $\alpha_i \neq \alpha_j$ para $i \neq j$. Tomando la derivada de $f(x)$, vemos que

$$\begin{aligned} f'(x) = {} & (x-\alpha_2)\cdots(x-\alpha_n) \\ & + (x-\alpha_1)(x-\alpha_3)\cdots(x-\alpha_n) \\ & + \cdots + (x-\alpha_1)\cdots(x-\alpha_{n-1}). \end{aligned}$$

Luego, $f(x)$ y $f'(x)$ no pueden tener ningún factor común.

Para demostrar el recíproco, mostraremos que se cumple la afirmación contrapositiva. Supongamos que $f(x) = (x-\alpha)^k g(x)$, con $k > 1$. Derivando, tenemos

$$f'(x) = k(x-\alpha)^{k-1} g(x) + (x-\alpha)^k g'(x).$$

Por lo tanto, $f(x)$ y $f'(x)$ tienen un factor común. □

Teorema 22.6. *Para cada primo p y para cada entero positivo n, existe un cuerpo finito F con p^n elementos. Más aún, cualquier cuerpo de orden p^n es isomorfo al cuerpo de descomposición de $x^{p^n} - x$ sobre $\mathbb{Z}_p$.*

Demostración. Sea $f(x) = x^{p^n} - x$ y sea F el cuerpo de descomposición de $f(x)$. Por el Lema 22.5, $f(x)$ tiene p^n ceros distintos en F, pues $f'(x) = p^n x^{p^n-1} - 1 = -1$ es relativamente primo con $f(x)$. Afirmamos que las raíces de $f(x)$ forman un subcuerpo de F. Ciertamente 0 y 1 son ceros de $f(x)$. Si α y β son ceros de $f(x)$, entonces $\alpha+\beta$ y $\alpha\beta$ también son ceros de $f(x)$, pues $\alpha^{p^n} + \beta^{p^n} = (\alpha+\beta)^{p^n}$ y $\alpha^{p^n}\beta^{p^n} = (\alpha\beta)^{p^n}$. También debemos mostrar que el inverso aditivo y el inverso multiplicativo de cada raíz de $f(x)$ son raíces de $f(x)$. Para cualquier cero α de $f(x)$, sabemos que $-\alpha$ también es cero de $f(x)$, pues

$$f(-\alpha) = (-\alpha)^{p^n} - (-\alpha) = -\alpha^{p^n} + \alpha = -(\alpha^{p^n} - \alpha) = 0,$$

suponiendo que p is impar. Si $p = 2$, entonces

$$f(-\alpha) = (-\alpha)^{2^n} - (-\alpha) = \alpha + \alpha = 0.$$

Si $\alpha \neq 0$, entonces $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$. Como los ceros de $f(x)$ forman un subcuerpo de F y $f(x)$ se descompone en este subcuerpo, el subcuerpo debe ser todo F.

Sea E cualquier otro cuerpo de orden p^n. Para mostrar que E es isomorfo a F, debemos mostrar que todo elemento en E es una raíz de $f(x)$. Claramente 0 y 1 son raíces de $f(x)$. Sea α un elemento no nulo de E. El orden del grupo multiplicativo de elementos no nulos de E es $p^n - 1$; luego, $\alpha^{p^n-1} = 1$ y $\alpha^{p^n} - \alpha = 0$. Como E contiene p^n elementos, E debe ser un cuerpo de descomposición de $f(x)$; pero, por el Corolario 21.34, el cuerpo de descomposición de cualquier polinomio es único salvo isomorfía. □

El único cuerpo con p^n elementos se llama ***cuerpo de Galois*** de orden p^n. Denotaremos este cuerpo por $\mathrm{GF}(p^n)$.

Teorema 22.7. *Todo subcuerpo del cuerpo de Galois $\mathrm{GF}(p^n)$ tiene p^m elementos, con m un divisor de n. Recíprocamente, si $m \mid n$ para $m > 0$, entonces existe un único subcuerpo de $\mathrm{GF}(p^n)$ isomorfo a $\mathrm{GF}(p^m)$.*

Demostración. Sea F un subcuerpo de $E = \mathrm{GF}(p^n)$. Entonces F debe ser una extensión de K que contiene p^m elementos, donde K es isomorfo a $\mathbb{Z}_p$. Entonces $m \mid n$, pues $[E:K] = [E:F][F:K]$.

Para demostrar el recíproco, supongamos que $m \mid n$ para algún $m > 0$. Entonces $p^m - 1$ divide a $p^n - 1$. En consecuencia, $x^{p^m-1} - 1$ divide a $x^{p^n-1} - 1$. Por lo tanto, $x^{p^m} - x$ debe dividir a $x^{p^n} - x$, y todo cero de $x^{p^m} - x$ también es un cero de $x^{p^n} - x$. Luego, $\mathrm{GF}(p^n)$ contiene, como subcuerpo, un cuerpo de descomposición de $x^{p^m} - x$, que debe ser isomorfo a $\mathrm{GF}(p^m)$. □

Ejemplo 22.8. El reticulado de subcuerpos de $\mathrm{GF}(p^{24})$ está dado en la Figura 22.9.

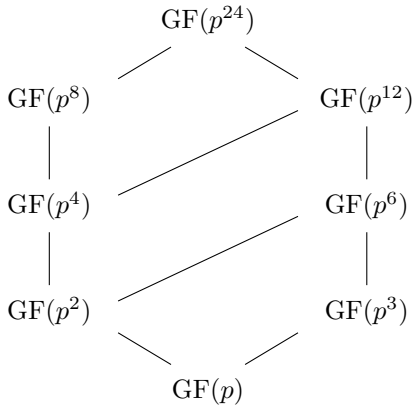


Figura 22.9: Subcuerpos de GF(p^{24})

Con cada cuerpo F tenemos un grupo multiplicativo de elementos no nulos de F que denotaremos por F^*. El grupo multiplicativo de un cuerpo finito cualquiera es cíclico. Este resultado se sigue del resultado más general que demostraremos en el próximo teorema.

Teorema 22.10. *Si G es un subgrupo finito de F^*, el grupo multiplicativo de elementos no nulos de un cuerpo F, entonces G es cíclico.*

DEMOSTRACIÓN. Sea G un subgrupo finito de F^* de orden n. Por el Teorema Fundamental de Grupos Abelianos (Teorema 13.4),

$$G \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}},$$

donde $n = p_1^{e_1} \cdots p_k^{e_k}$ y los $p_1, \ldots, p_k$ son primos (no necesariamente distintos). Sea m el mínimo común múltiplo de $p_1^{e_1}, \ldots, p_k^{e_k}$. Entonces G contiene un elemento de orden m. Como todo α en G satisface $x^r - 1$ para algún r que divide a m, α debe también ser raíz de $x^m - 1$. Como $x^m - 1$ tiene a lo más m raíces en F, $n \leq m$. Por otra parte, sabemos que $m \leq |G|$; por lo tanto, $m = n$. Luego, G contiene un elemento de orden n y tiene que ser cíclico. □

Corolario 22.11. *El grupo multiplicativo de todos los elementos no nulos de un cuerpo finito es cíclico.*

Corolario 22.12. *Toda extensión finita E de un cuerpo finito F es una extensión simple de F.*

DEMOSTRACIÓN. Sea α un generador del grupo cíclico E^* de elementos distintos de cero de E. Entonces $E = F(\alpha)$. □

Ejemplo 22.13. El cuerpo finito GF(2^4) es isomorfo al cuerpo $\mathbb{Z}_2/\langle 1+x+x^4 \rangle$. Por lo tanto, los elementos de GF(2^4) se puede tomar como

$$\{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 : a_i \in \mathbb{Z}_2 \text{ and } 1 + \alpha + \alpha^4 = 0\}.$$

Recordando que $1+\alpha+\alpha^4 = 0$, sumamos y multiplicamos elementos de GF(2^4) exactamente como sumamos y multiplicamos polinomios. El grupo multiplicativo de GF(2^4) es isomorfo a $\mathbb{Z}_{15}$ con generador α:

$$\begin{array}{lll}
\alpha^1 = \alpha & \alpha^6 = \alpha^2 + \alpha^3 & \alpha^{11} = \alpha + \alpha^2 + \alpha^3 \\
\alpha^2 = \alpha^2 & \alpha^7 = 1 + \alpha + \alpha^3 & \alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3 \\
\alpha^3 = \alpha^3 & \alpha^8 = 1 + \alpha^2 & \alpha^{13} = 1 + \alpha^2 + \alpha^3 \\
\alpha^4 = 1 + \alpha & \alpha^9 = \alpha + \alpha^3 & \alpha^{14} = 1 + \alpha^3 \\
\alpha^5 = \alpha + \alpha^2 & \alpha^{10} = 1 + \alpha + \alpha^2 & \alpha^{15} = 1.
\end{array}$$

22.2 Códigos Polinomiales

Sabiendo sobre anillos de polinomios y cuerpos finitos, es posible derivar códigos más sofisticados que los del Capítulo 8. En primer lugar recordemos que un código de bloques (n, k) consiste de una función codificadora inyectiva $E : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ y una función decodificadora $D : \mathbb{Z}_2^n \to \mathbb{Z}_2^k$. El código es corrector de errores si D es sobreyectivo. Un código es lineal si es el espacio nulo de una matriz $H \in \mathbb{M}_{k\times n}(\mathbb{Z}_2)$.

Estamos interesados en una clase de códigos conocidos como códigos cíclicos. Sea $\phi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ un código de bloques (n, k) binario. Entonces ϕ es un ***código cíclico*** si para cada palabra $(a_1, a_2, \ldots, a_n)$ en el código, la palabra formada por desplazamiento cíclico, la n-tupla $(a_n, a_1, a_2, \ldots, a_{n-1})$ también está en el código. Los códigos cíclicos son fáciles de implementar en un computador usando registro de shift [2, 3].

Ejemplo 22.14. Considere los código lineales $(6, 3)$generados por las dos matrices

$$G_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{y} \quad G_2 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Los mensajes del primero se codifican como sigue:

$$\begin{array}{lcllcl} (000) & \mapsto & (000000) & (100) & \mapsto & (100100) \\ (001) & \mapsto & (001001) & (101) & \mapsto & (101101) \\ (010) & \mapsto & (010010) & (110) & \mapsto & (110110) \\ (011) & \mapsto & (011011) & (111) & \mapsto & (111111). \end{array}$$

Es fácil ver que las palabras del código forman un código cíclico. En el segundo, las 3-tuplas se codifican de la siguiente manera:

$$\begin{array}{lcllcl} (000) & \mapsto & (000000) & (100) & \mapsto & (111100) \\ (001) & \mapsto & (001111) & (101) & \mapsto & (110011) \\ (010) & \mapsto & (011110) & (110) & \mapsto & (100010) \\ (011) & \mapsto & (010001) & (111) & \mapsto & (101101). \end{array}$$

Este código no es cíclico, pues (101101) es una palabra del código pero (011011) no lo es.

Códigos Polinomiales

Nos gustaría encontrar un método fácil para obtener códigos cíclicos lineales. Para lograr esto, podemos usar lo que sabemos de cuerpos finitos y anillos de polinomios sobre $\mathbb{Z}_2$. Cualquier n-tupla binaria se puede interpretar como un polinomio en $\mathbb{Z}_2[x]$. Dicho de otra forma, la n-tupla $(a_0, a_1, \ldots, a_{n-1})$ corresponde al polinomio

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},$$

donde el grado de $f(x)$ es a lo más $n-1$. Por ejemplo, el polinomio correspondiente a la 5-tupla (10011) es

$$1 + 0x + 0x^2 + 1x^3 + 1x^4 = 1 + x^3 + x^4.$$

Recíprocamente, dado cualquier polinomio $f(x) \in \mathbb{Z}_2[x]$ con $\operatorname{gr} f(x) < n$ le podemos asociar una n-tupla binaria. El polinomio $x + x^2 + x^4$ corresponde a la 5-tupla (01101).

Fijemos un polinomio no constante $g(x)$ en $\mathbb{Z}_2[x]$ de grado $n-k$. Podemos definir un (n,k)-código C de la siguiente manera. Si $(a_0, \ldots, a_{k-1})$ es una k-tupla a codificar, entonces $f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$ es el correspondiente polinomio en $\mathbb{Z}_2[x]$. Para codificar $f(x)$, lo multiplicamos por $g(x)$. Las palabras en C son todos aquellos polinomios en $\mathbb{Z}_2[x]$ de grado menor a n que son divisibles por $g(x)$. Los Códigos obtenidos de esta manera se llaman ***códigos polinomiales***.

Ejemplo 22.15. Si $g(x) = 1 + x^3$, podemos definir un $(6,3)$-código C como sigue. Para codificar una 3-tupla (a_0, a_1, a_2), multiplicamos el correspondiente polinomio $f(x) = a_0 + a_1x + a_2x^2$ por $1 + x^3$. Estamos definiendo una función $\phi : \mathbb{Z}_2^3 \to \mathbb{Z}_2^6$ como $\phi : f(x) \mapsto g(x)f(x)$. Es fácil verificar que esta función es un homomorfismo de grupos. De hecho, si consideramos $\mathbb{Z}_2^n$ como un espacio vectorial sobre $\mathbb{Z}_2$, ϕ es una transformación lineal de espacios vectoriales (vea el Ejercicio 20.4.15, Capítulo 20). Calculemos el núcleo de ϕ. Observe que $\phi(a_0, a_1, a_2) = (000000)$ exactamente cuando

$$\begin{aligned} 0 + 0x + 0x^2 + 0x^3 + 0x^4 + 0x^5 &= (1 + x^3)(a_0 + a_1x + a_2x^2) \\ &= a_0 + a_1x + a_2x^2 + a_0x^3 + a_1x^4 + a_2x^5. \end{aligned}$$

Como los polinomios sobre un cuerpo forman un dominio integral, $a_0 + a_1x + a_2x^2$ debe ser el polinomio cero. Por lo tanto, $\ker \phi = \{(000)\}$ y ϕ es 1-1.

Para calcular una matriz generadora para C, solo debemos examinar cómo se codifican los polinomios 1, x, y x^2:

$$\begin{aligned} (1 + x^3) \cdot 1 &= 1 + x^3 \\ (1 + x^3)x &= x + x^4 \\ (1 + x^3)x^2 &= x^2 + x^5. \end{aligned}$$

Obtenemos el código correspondiente a la matriz generadora G_1 en el Ejemplo 22.14. la matriz de verificación de paridad para este código es

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Como el menor peso de cualquier palabra no nula del código es 2, este código es capaz de detectar cualquier error único.

Los anillos de Polinomios tienen una estructura muy rica; por lo tanto, nuestro objetivo inmediato es establecer una relación entre los códigos polinomiales y la teoría de anillos. Recuerde que $x^n - 1 = (x-1)(x^{n-1} + \cdots + x + 1)$. El anillo cociente

$$R_n = \mathbb{Z}_2[x]/\langle x^n - 1 \rangle$$

puede ser considerado como el anillo de polinomios de la forma

$$f(t) = a_0 + a_1t + \cdots + a_{n-1}t^{n-1}$$

que satisfacen la condición $t^n = 1$. Es un ejercicio sencillo mostrar que $\mathbb{Z}_2^n$ y R_n son isomorfos como espacios vectoriales. Frecuentemente interpretaremos

los elementos en $\mathbb{Z}_2^n$ con elementos en $\mathbb{Z}[x]/\langle x^n - 1\rangle$. De esta forma podemos interpretar un código lineal como un subconjunto de $\mathbb{Z}[x]/\langle x^n - 1\rangle$.

La estructura adicional de anillo en los códigos polinomiales es muy poderosa para describir códigos cíclicos. Un shift cíclico de una n-tupla puede ser descrito por una multiplicación polinomial. Si $f(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1}$ es un código polinomial en R_n, entonces

$$tf(t) = a_{n-1} + a_0 t + \cdots + a_{n-2}t^{n-1}$$

es la palabra desplazada cíclicamente obtenida de multiplicar $f(t)$ por t. El siguiente teorema entrega una hermosa clasificación de los códigos cíclicos en términos de los ideales de R_n.

Teorema 22.16. *Un código lineal C en $\mathbb{Z}_2^n$ es cíclico si y solo si es un ideal en $R_n = \mathbb{Z}[x]/\langle x^n - 1\rangle$.*

Demostración. Sea C un código cíclico lineal y supongamos que $f(t)$ está en C. Entonces $tf(t)$ también está en C. Así, $t^k f(t)$ está en C para todo $k \in \mathbb{N}$. Como C es un código lineal, cualquier combinación lineal de las palabras $f(t), tf(t), t^2 f(t), \ldots, t^{n-1}f(t)$ también es una palabra del código; por lo tanto, para cada polinomio therefore $p(t)$, $p(t)f(t)$ está en C. Luego, C es un ideal.

Recíprocamente, sea C un ideal en $\mathbb{Z}_2[x]/\langle x^n + 1\rangle$. Supongamos que $f(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1}$ es una palabra en C. Entonces $tf(t)$ es una palabra en C; es decir, $(a_1, \ldots, a_{n-1}, a_0)$ está en C. □

El Teorema 22.16 nos dice que conocer los ideales de R_n es equivalente a conocer los códigos cíclicos en $\mathbb{Z}_2^n$. Afortunadamente es fácil describir los ideales en R_n. El homomorfismo natural $\phi : \mathbb{Z}_2[x] \to R_n$ definido por $\phi[f(x)] = f(t)$ es un homomorfismo epiyectivo. El núcleo de ϕ es el ideal generado por $x^n - 1$. Por el Teorema 16.34, todo ideal C en R_n es de la forma $\phi(I)$, donde I es un ideal en $\mathbb{Z}_2[x]$ que contiene al ideal $\langle x^n - 1\rangle$. Por el Teorema 17.20, sabemos que todo ideal en $\mathbb{Z}_2[x]$ es un ideal principal, pues $\mathbb{Z}_2$ es un cuerpo. Por lo tanto, $I = \langle g(x)\rangle$ para algún polinomio mónico en $\mathbb{Z}_2[x]$. Como $\langle x^n - 1\rangle$ está contenido en I, se debe tener que $g(x)$ divide a $x^n - 1$. Así, todo ideal C en R_n es de la forma

$$C = \langle g(t)\rangle = \{f(t)g(t) : f(t) \in R_n \text{ y } g(x) \mid (x^n - 1) \text{ en } \mathbb{Z}_2[x]\}.$$

El polinomio único de grado mínimo que genera C se llama ***polinomio generador minimal*** de C.

Ejemplo 22.17. Si factorizamos $x^7 - 1$ en sus componentes irreducibles, tenemos

$$x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3).$$

Vemos que $g(t) = (1 + t + t^3)$ genera un ideal C en R_7. Este es un código de bloque $(7, 4)$. Como en el Ejemplo 22.15, es fácil calcular una matriz generadora examinando qué le hace $g(t)$ a los polinomios 1, t, t^2, y t^3. Una matriz generadora para C es

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

En general, podemos determinar una matriz generadora para un código (n, k) C por la forma en que se codifican los elementos t^k. Sea $x^n - 1 = g(x)h(x)$ en $\mathbb{Z}_2[x]$. Si $g(x) = g_0 + g_1 x + \cdots + g_{n-k}x^{n-k}$ and $h(x) = h_0 + h_1 x + \cdots + h_k x^k$, entonces la matriz de $n \times k$

$$G = \begin{pmatrix} g_0 & 0 & \cdots & 0 \\ g_1 & g_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-k} & g_{n-k-1} & \cdots & g_0 \\ 0 & g_{n-k} & \cdots & g_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_{n-k} \end{pmatrix}$$

es una matriz generadora para el código C con generador polinomial $g(t)$. La matriz de verificación de paridad para C es la matriz de $(n-k) \times n$

$$H = \begin{pmatrix} 0 & \cdots & 0 & 0 & h_k & \cdots & h_0 \\ 0 & \cdots & 0 & h_k & \cdots & h_0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ h_k & \cdots & h_0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Dejaremos los detalles de la demostreción de la siguiente proposición como un ejercicio.

Proposición 22.18. *Sea $C = \langle g(t) \rangle$ un código cíclico en R_n ay supongamos que $x^n - 1 = g(x)h(x)$. Entonces G y H son matriz generadora y verificadora para C, respectivamente. Más aún, $HG = 0$.*

Ejemplo 22.19. En el Ejemplo 22.17,

$$x^7 - 1 = g(x)h(x) = (1 + x + x^3)(1 + x + x^2 + x^4).$$

Por lo tanto, una matriz verificadora para este código es

$$H = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Para determinanr las capacidades de detección y corrección de errores de un código cíclico, necesitamos saber algo sobre determinantes. Si $\alpha_1, \ldots, \alpha_n$ son elementos en un cuerpo F, entonces la matriz de $n \times n$

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

se llama ***matriz de Vandermonde***. El determinante de esta matriz se llama ***determinante de Vandermonde***. Necesitaremos el siguiente lema en nuestro estudio de los códigos cíclicos.

Lema 22.20. *Sean $\alpha_1, \ldots, \alpha_n$ elementos en un cuerpo F con $n \geq 2$. Entonces*

$$\det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix} = \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j).$$

En particular, si los α_i son distintos, entonces el determinante es distinto de cero.

DEMOSTRACIÓN. Procederemos por inducción en n. Si $n = 2$, entonces el determinante es $\alpha_2 - \alpha_1$. Supongamos demostrado el resultado para $n-1$ y consideremos el polinomio $p(x)$ definido por

$$p(x) = \det \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} & x \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{n-1}^2 & x^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_{n-1}^{n-1} & x^{n-1} \end{pmatrix}.$$

Expandiendo este determinante por cofactores en la última columna, vemos que $p(x)$ es un polinomio de grado a lo más $n-1$. Además, las raíces de $p(x)$ son $\alpha_1, \ldots, \alpha_{n-1}$, pues la sustitución de cualquiera de esos elementos en la última columna producirá una columna idéntica a otra columna de la matriz. Recuerde que el determinante de una matriz es cero si esta tiene dos columnas idénticas. Por lo tanto,

$$p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{n-1})\beta,$$

donde

$$\beta = (-1)^{n+n} \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{n-1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \cdots & \alpha_{n-1}^{n-2} \end{pmatrix}.$$

Por nuestra hipótesis de inducción,

$$\beta = (-1)^{n+n} \prod_{1 \le j < i \le n-1} (\alpha_i - \alpha_j).$$

Si evaluamos en $x = \alpha_n$, el resultados es una consecuencia inmediata. □

El siguiente teorema nos entrega una estimación de las capacidades de detección y corrección de errores para un polinomio generador en particular.

Teorema 22.21. *Sea $C = \langle g(t) \rangle$ un código cíclico en R_n y supongamos que ω es una raíz n-ésima primitiva de la unidad sobre $\mathbb{Z}_2$. Si s potencias consecutivas de ω son raíces de $g(x)$, entonces la distacia mínima de C es al menos $s+1$.*

DEMOSTRACIÓN. Supongamos que

$$g(\omega^r) = g(\omega^{r+1}) = \cdots = g(\omega^{r+s-1}) = 0.$$

Sea $f(x)$ algún polinomio en C con s o menos coeficientes distintos de cero. Podemos suponer que

$$f(x) = a_{i_0} x^{i_0} + a_{i_1} x^{i_1} + \cdots + a_{i_{s-1}} x^{i_{s-1}}$$

es algún polinomio en C. Es suficiente con demostrar que todos los a_i tienen que ser cero. Como

$$g(\omega^r) = g(\omega^{r+1}) = \cdots = g(\omega^{r+s-1}) = 0$$

y $g(x)$ divide a $f(x)$,

$$f(\omega^r) = f(\omega^{r+1}) = \cdots = f(\omega^{r+s-1}) = 0.$$

Equivalentemente, tenemos el siguiente sistema de ecuaciones:

$$\begin{aligned} a_{i_0}(\omega^r)^{i_0} + a_{i_1}(\omega^r)^{i_1} + \cdots + a_{i_{s-1}}(\omega^r)^{i_{s-1}} &= 0 \\ a_{i_0}(\omega^{r+1})^{i_0} + a_{i_1}(\omega^{r+1})^{i_2} + \cdots + a_{i_{s-1}}(\omega^{r+1})^{i_{s-1}} &= 0 \\ &\vdots \\ a_{i_0}(\omega^{r+s-1})^{i_0} + a_{i_1}(\omega^{r+s-1})^{i_1} + \cdots + a_{i_{s-1}}(\omega^{r+s-1})^{i_{s-1}} &= 0. \end{aligned}$$

Por lo tanto, $(a_{i_0}, a_{i_1}, \ldots, a_{i_{s-1}})$ es una solución del sistema de ecuaciones lineales homogéneo

$$\begin{aligned} (\omega^{i_0})^r x_0 + (\omega^{i_1})^r x_1 + \cdots + (\omega^{i_{s-1}})^r x_{n-1} &= 0 \\ (\omega^{i_0})^{r+1} x_0 + (\omega^{i_1})^{r+1} x_1 + \cdots + (\omega^{i_{s-1}})^{r+1} x_{n-1} &= 0 \\ &\vdots \\ (\omega^{i_0})^{r+s-1} x_0 + (\omega^{i_1})^{r+s-1} x_1 + \cdots + (\omega^{i_{s-1}})^{r+s-1} x_{n-1} &= 0. \end{aligned}$$

Pero este sistema tiene solución única, pues el determinante de la matriz

$$\begin{pmatrix} (\omega^{i_0})^r & (\omega^{i_1})^r & \cdots & (\omega^{i_{s-1}})^r \\ (\omega^{i_0})^{r+1} & (\omega^{i_1})^{r+1} & \cdots & (\omega^{i_{s-1}})^{r+1} \\ \vdots & \vdots & \ddots & \vdots \\ (\omega^{i_0})^{r+s-1} & (\omega^{i_1})^{r+s-1} & \cdots & (\omega^{i_{s-1}})^{r+s-1} \end{pmatrix}$$

no es cero por el Lema 22.20 y las propiedades básicas de los determinantes (Ejercicio). Por lo tanto, esta solución es $a_{i_0} = a_{i_1} = \cdots = a_{i_{s-1}} = 0$. □

Códigos BCH

Entre los códigos más importantes, descubiertos independientemente por A. Hocquenghem en 1959 y por R. C. Bose y D. V. Ray-Chaudhuri en 1960, están los códigos BCH. Los sistemas de comunicación Europeo y Trasantlántico, ambos usan códigos BCH. Las palabras a codificar son de largo 231, y se usa un polinomio de grado 24 para generar el código. Como $231+24 = 255 = 2^8-1$, tenemos un código de bloque $(255, 231)$. Este código BCH es capaz de detectar seis errores y tiene una razón de falla de 1 en 16 millones. Una ventaja de los códigos BCH es que existen algoritmos eficientes de corrección de errores para ellos.

La idea detrás de los códigos BCH es elegir un polinomio generador de grado minimal que tenga la mayor capacidad de detección y corrección de errores. Sea $d = 2r + 1$ para algún $r \geq 0$. Supongamos que ω es una raíz n-ésima primitiva de la unidad sobre $\mathbb{Z}_2$, y sea $m_i(x)$ el polinomio minimal sobre $\mathbb{Z}_2$ de ω^i. Si

$$g(x) = \text{mcm}[m_1(x), m_2(x), \ldots, m_{2r}(x)],$$

entonces el código cíclico $\langle g(t)\rangle$ en R_n se denomina código **BCH *de largo*** n y ***distancia*** d. Por el Teorema 22.21, la distancia mínima de C es al menos d.

Teorema 22.22. *Sea $C = \langle g(t)\rangle$ un código cíclico en R_n. Entonces las siguientes proposiciones son equivalentes.*

1. *El código C es un código* BCH *cuya distancia mínima es al menos d.*

2. *Un polinomio $f(t)$ está en C si y solo si $f(\omega^i) = 0$ para $1 \leq i < d$.*

3. *La matriz*

$$H = \begin{pmatrix} 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{(n-1)(2)} \\ 1 & \omega^3 & \omega^6 & \cdots & \omega^{(n-1)(3)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{2r} & \omega^{4r} & \cdots & \omega^{(n-1)(2r)} \end{pmatrix}$$

es una matriz verificadora para C.

DEMOSTRACIÓN. (1) $\Rightarrow$ (2). If $f(t)$ está en C, entonces $g(x) \mid f(x)$ en $\mathbb{Z}_2[x]$. Luego, para $i = 1, \ldots, 2r$, $f(\omega^i) = 0$ pues $g(\omega^i) = 0$. Recíprocamente, supongamos que $f(\omega^i) = 0$ for $1 \leq i \leq d$. Entonces $f(x)$ es divisible por cada $m_i(x)$, pues $m_i(x)$ es el polinomio minimal de ω^i. Por lo tanto, $g(x) \mid f(x)$ porla definición de $g(x)$. Así, $f(x)$ es una palabra del código.

(2) $\Rightarrow$ (3). Sea $f(t) = a_0 + a_1 t + \cdots + a_{n-1} v t^{n-1}$ be in R_n. La correspondiente n-tupla en $\mathbb{Z}_2^n$ es $\mathbf{x} = (a_0 a_1 \cdots a_{n-1})^{\mathrm{t}}$. By (2),

$$H\mathbf{x} = \begin{pmatrix} a_0 + a_1\omega + \cdots + a_{n-1}\omega^{n-1} \\ a_0 + a_1\omega^2 + \cdots + a_{n-1}(\omega^2)^{n-1} \\ \vdots \\ a_0 + a_1\omega^{2r} + \cdots + a_{n-1}(\omega^{2r})^{n-1} \end{pmatrix} = \begin{pmatrix} f(\omega) \\ f(\omega^2) \\ \vdots \\ f(\omega^{2r}) \end{pmatrix} = 0$$

precisamente cuando $f(t)$ está en C. Luego, H es una matriz verificadora para C.

(3) $\Rightarrow$ (1). Por (3), un polinomio $f(t) = a_0 + a_1 t + \cdots + a_{n-1} t^{n-1}$ está en C exactamente cuando $f(\omega^i) = 0$ for $i = 1, \ldots, 2r$. El menor tal polinomio es $g(t) = \mathrm{mcm}[m_1(t), \ldots, m_{2r}(t)]$. Por lo tanto, $C = \langle g(t) \rangle$. □

Ejemplo 22.23. Es fácil verificar que $x^{15} - 1 \in \mathbb{Z}_2[x]$ se factoriza como

$$x^{15} - 1 = (x+1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1),$$

donde cada uno de estos factores es irreducible. Sea ω una raíz de $1 + x + x^4$. Le cuerpo de Galois $\mathrm{GF}(2^4)$ es

$$\{a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 : a_i \in \mathbb{Z}_2 \text{ and } 1 + \omega + \omega^4 = 0\}.$$

Por el Ejemplo 22.8, ω es una raíz 15 primitiva de la unidad. El polinomio minimal de ω es $m_1(x) = 1 + x + x^4$. Es fácil ver que ω^2 y ω^4 también son raíces de $m_1(x)$. El polinomio minimal de ω^3 es $m_2(x) = 1 + x + x^2 + x^3 + x^4$. Por lo tanto,

$$g(x) = m_1(x)m_2(x) = 1 + x^4 + x^6 + x^7 + x^8$$

tiene raíces ω, ω^2, ω^3, ω^4. Como tanto $m_1(x)$ como $m_2(x)$ dividen a $x^{15} - 1$, el código BCH es un código $(15, 7)$. Si $x^{15} - 1 = g(x)h(x)$, entonces $h(x) = 1 + x^4 + x^6 + x^7$; por lo tanto, una matriz verificadora para este código es

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Sage Los Cuerpos Finitos son importantes en diversas disciplinas aplicadas, tales como criptografía y teoría de códigos (vea la introducción a estos tópicos en otros capítulos). Sage tiene una excelente implementación de los cuerpos finitos que permite una variedad de cálculos con éstos.

22.3 Ejercicios

1. Calcule.

(a) $[\mathrm{GF}(3^6) : \mathrm{GF}(3^3)]$
(b) $[\mathrm{GF}(128) : \mathrm{GF}(16)]$
(c) $[\mathrm{GF}(625) : \mathrm{GF}(25)]$
(d) $[\mathrm{GF}(p^{12}) : \mathrm{GF}(p^2)]$

2. Calcule $[\mathrm{GF}(p^m) : \mathrm{GF}(p^n)]$, con $n \mid m$.

3. ¿Cuál es el reticulado de subcuerpos de $\mathrm{GF}(p^{30})$?

4. Sea α una raíz de x^3+x^2+1 sobre $\mathbb{Z}_2$. Construya un cuerpo finito de orden 8. Muestre que $x^3 + x^2 + 1$ se descompone en $\mathbb{Z}_2(\alpha)$.

5. Construya un cuerpo finito de orden 27.

6. Demuestre o refute: $\mathbb{Q}^*$ es cíclico.

7. Factorice cada uno de los siguientes polinomios en $\mathbb{Z}_2[x]$.

(a) $x^5 - 1$
(b) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
(c) $x^9 - 1$
(d) $x^4 + x^3 + x^2 + x + 1$

8. Demuestre o refute: $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle \cong \mathbb{Z}_2[x]/\langle x^3 + x^2 + 1\rangle$.

9. Determine el número de códigos cíclicos de longitud n para $n = 6$, 7, 8, 10.

10. Demuestre que el ideal $\langle t + 1\rangle$ en R_n es el código en $\mathbb{Z}_2^n$ que consiste de todas las palabras con un número par de unos.

11. Construya todos los códigos BCH de

(a) longitud 7.
(b) longitud 15.

12. Demuestre o refute: Existe un cuerpo finito algebraicamente cerrado.

13. Sea p un primo. Demuestre que el cuerpo de funciones racionales $\mathbb{Z}_p(x)$ es un cuerpo infinito de característica p.

14. Sea D un dominio de integridad de característica p. Demuestre que $(a - b)^{p^n} = a^{p^n} - b^{p^n}$ para todo $a, b \in D$.

15. Muestre que todo elemento en un cuerpo finito puede ser escrito como la suma de dos cuadrados.

16. Sean E y F be subcuerpos de un cuerpo finito K. Si E es isomorfo a F, muestre que $E = F$.

17. Sean $F \subset E \subset K$ cuerpos. Si K es una extensión separable de F, muestre que K también es una extensión separable de E.

18. Sea E una extensión de un cuerpo finito F, donde F tiene q elementos. Sea $\alpha \in E$ algebraico sobre F de grado n. Demuestre que $F(\alpha)$ tiene q^n elementos.

19. Muestre que toda extensión finita de un cuerpo finito F es simple; es decir, si E es una extensión finita de n cuerpo finito F, demuestre que existe un $\alpha \in E$ tal que $E = F(\alpha)$.

20. Muestre que para cada n existe un polinomio irreducible de grado n en $\mathbb{Z}_p[x]$.

21. Demuestre que la ***función de Frobenius*** $\Phi : \mathrm{GF}(p^n) \to \mathrm{GF}(p^n)$ given by $\Phi : \alpha \mapsto \alpha^p$ es un automorfismo de orden n.

22. Muestre que todo elemento en $\mathrm{GF}(p^n)$ puede ser escrito en la forma a^p para un único $a \in \mathrm{GF}(p^n)$.

23. Sean E y F subcuerpos de $\mathrm{GF}(p^n)$. Si $|E| = p^r$ y $|F| = p^s$, ¿cuál es el orden de $E \cap F$?

24. (Teoream de Wilson) Sea p un primo. Demuestre que $(p-1)! \equiv -1 \pmod{p}$.

25. Si $g(t)$ es el polinomio generador minimal para un código cíclico C en R_n, demuestre que el término constante de $g(x)$ es 1.

26. Es concebible que una ráfaga de errores pueda ocurrir durante una transmisión, como en el caso de una sobrecarga de energía. Una ráfaga de interferencia puede alterar varios bits consecutivos de una palabra del código. Los códigos cíclicos permiten detectar tales ráfagas de errores. Sea C un código cíclico (n, k). Demuestre que cualquier ráfaga de hasta $n - k$ dígitos puede ser detectada.

27. Demuestre que los anillos R_n y $\mathbb{Z}_2^n$ son isomorfos como espacios vectoriales.

28. Sea C un código en R_n generado por $g(t)$. Si $\langle f(t) \rangle$ es otro código en R_n, muestre que $\langle g(t) \rangle \subset \langle f(t) \rangle$ si y solo si $f(x)$ divide a $g(x)$ en $\mathbb{Z}_2[x]$.

29. Sea $C = \langle g(t) \rangle$ un código cíclico en R_n y supongamos que $x^n - 1 = g(x)h(x)$, donde $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$ y $h(x) = h_0 + h_1 x + \cdots + h_k x^k$. Definamos G como la matriz de $n \times k$

$$G = \begin{pmatrix} g_0 & 0 & \cdots & 0 \\ g_1 & g_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-k} & g_{n-k-1} & \cdots & g_0 \\ 0 & g_{n-k} & \cdots & g_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_{n-k} \end{pmatrix}$$

y H como la matriz de $(n-k) \times n$

$$H = \begin{pmatrix} 0 & \cdots & 0 & 0 & h_k & \cdots & h_0 \\ 0 & \cdots & 0 & h_k & \cdots & h_0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ h_k & \cdots & h_0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

(a) Demuestre que G es una matriz generadora para C.

(b) Demuestre que H es una matriz verificadora para C.

(c) Muestre que $HG = 0$.

22.4 Ejercicios Adicionales: Corrección de Errores para Códigos BCH

Los códigos BCH tienen algoritmos de corrección de errores muy atractivos. Sea C un código BCH en R_n, y supongamos que se transmite un polinomio $c(t) = c_0+c_1t+\cdots+c_{n-1}t^{n-1}$ del código. Sea $w(t) = w_0+w_1t+\cdots w_{n-1}t^{n-1}$ el polinomio en R_n que es recibido. Si han ocurrido errores en los bits $a_1, \ldots, a_k$, entonces $w(t) = c(t) + e(t)$, donde $e(t) = t^{a_1} + t^{a_2} + \cdots + t^{a_k}$ es el ***polinomio de error***. El decodificador debe determinar los enteros a_i y luego recuperar $c(t)$ a partir de $w(t)$ cambiando el valor de los bit a_i. A partir de $w(t)$ podemos calcular $w(\omega^i) = s_i$ para $i = 1, \ldots, 2r$, donde ω es una raíz n-ésima primitiva de la unidad sobre $\mathbb{Z}_2$. Decimos que el ***síndrome*** de $w(t)$ es $s_1, \ldots, s_{2r}$.

1. Muestre que $w(t)$ es un código polinomial si y solo si $s_i = 0$ para todo i.

2. Muestre que

$$s_i = w(\omega^i) = e(\omega^i) = \omega^{ia_1} + \omega^{ia_2} + \cdots + \omega^{ia_k}$$

para $i = 1, \ldots, 2r$. El ***polinomio localizador de errores*** se define como

$$s(x) = (x + \omega^{a_1})(x + \omega^{a_2}) \cdots (x + \omega^{a_k}).$$

3. Recuerde el código de bloque BCH $(15, 7)$ en el Ejemplo 22.19. Por el Teorema 8.13, este código es capaz de corregir dos errores. Supongamos que estos errores ocurren en los bits a_1 y a_2. El polinomio localizador de errores es $s(x) = (x + \omega^{a_1})(x + \omega^{a_2})$. Muestre que

$$s(x) = x^2 + s_1x + \left(s_1^2 + \frac{s_3}{s_1}\right).$$

4. Sea $w(t) = 1+t^2+t^4+t^5+t^7+t^{12}+t^{13}$. Determine el polinomio originalmente transmitido.

22.5 Referencias y Lecturas Recomendadas

[1] Childs, L. *A Concrete Introduction to Higher Algebra*. 2nd ed. Springer-Verlag, New York, 1995.

[2] Gåding, L. and Tambour, T. *Algebra for Computer Science*. Springer-Verlag, New York, 1988.

[3] Lidl, R. and Pilz, G. *Applied Abstract Algebra*. 2nd ed. Springer, New York, 1998. An excellent presentation of finite fields and their applications.

[4] Mackiw, G. *Applications of Abstract Algebra*. Wiley, New York, 1985.

[5] Roman, S. *Coding and Information Theory*. Springer-Verlag, New York, 1992.

[6] van Lint, J. H. *Introduction to Coding Theory*. Springer, New York, 1999.

22.6 Sage

Habrá notado en este capítulo que los cuerpos finitos son bastante estructurados. También henos visto cuerpos finitos en Sage como ejemplos de anillos y cuerpos. Ahora podemos combinar los dos, principalmente usando comandos que ya conocemos, además de unos pocos nuevos.

Creando Cuerpos Finitos

Por el Teorema 22.6 sabemos que todos los cuerpos finitos de un orden dado son isomorfos y que los órdenes posibles se limitan a las potencias de primos. Podemos usar el comando `FiniteField()`, como antes, o uno equivalente más corto que es `GF()`. Opcionalmente, podemos especificar un polinomio irreducible para la construcción del cuerpo. Podemos ver este polinomio como el generador del ideal principal de un anillo de polinomios, o lo podemos ver como una regla de "re-escritura" para las potencias del generador del cuerpo que nos permite multiplicar elementos y reformularlos como combinaciones lineales de potencias menores.

De no proveerse un polinomio irreducible, Sage usará un polinomio de Conway. Usted puede determinarlos con el comando `conway_polynomial()`, o simplemente construir un cuerpo finito y recuperar el polinomio que lo define con el método `.polynomial()`.

```
F.<a> = GF(7^15); F
```

```
Finite Field in a of size 7^15
```

```
F.polynomial()
```

```
a^15 + 5*a^6 + 6*a^5 + 6*a^4 + 4*a^3 + a^2 + 2*a + 4
```

```
a^15 + 5*a^6 + 6*a^5 + 6*a^4 + 4*a^3 + a^2 + 2*a + 4
```

```
0
```

```
conway_polynomial(7, 15)
```

```
x^15 + 5*x^6 + 6*x^5 + 6*x^4 + 4*x^3 + x^2 + 2*x + 4
```

Solo para facilitar la lectura, coercionamos una lista de coeficientes al anillo de polinomios (obtenido con el método `.parent()` en un polinomio simple) para definir un polinomio.

```
y = polygen(Integers(7), 'y')
P = y.parent()
p = P([4, 5, 2, 6, 3, 3, 6, 2, 1, 1, 2, 5, 6, 3, 5, 1]); p
```

```
y^15 + 5*y^14 + 3*y^13 + 6*y^12 + 5*y^11 + 2*y^10 + y^9 +
y^8 + 2*y^7 + 6*y^6 + 3*y^5 + 3*y^4 + 6*y^3 + 2*y^2 + 5*y + 4
```

```
p.is_irreducible()
```

```
True
```

```
T.<b> = GF(7^15, modulus=p); T
```

```
Finite Field in b of size 7^15
```

Logaritmos en Cuerpos Finitos

Un comando útil que no hemos descrito es el método `.log()` para elementos de un cuerpo finito. Como sabemos que el grupo multiplicativo de lementos

distintos de cero es cíclico, podemos expresar cualquier elemento como una potencia del generador. El método `.log()` devuelve esa potencia.

Usualmente querremos usar el generador como la base de un cálculo de logaritmos en el cuerpo finito. Pero también es posible usar otra base, en el entendimiento que si la base no es un generador del grupo, entonces el logaritmo podría no existir (i.e. puede no haber una solución a la ecuación relevante).

```
F.<a> = GF(5^4)
a^458
```

```
3*a^3 + 2*a^2 + a + 3
```

```
(3*a^3 + 2*a^2 + a + 3).log(a)
```

```
458
```

```
exponent = (3*a^3 + 2*a^2 + a + 3).log(2*a^3 + 4*a^2 + 4*a)
exponent
```

```
211
```

```
(2*a^3 + 4*a^2 + 4*a)^exponent == 3*a^3 + 2*a^2 + a + 3
```

```
True
```

```
(3*a^3 + 2*a^2 + a + 3).log(a^2 + 4*a + 4)
```

```
Traceback (most recent call last):
...
ValueError: No discrete log of 3*a^3 + 2*a^2 + a + 3 found
to base a^2 + 4*a + 4
```

Como ya conocemos muchos comandos en Sage, no hay mucho más que sea necesario introducir para trabajar provechosamente con cuerpos finitos. Los ejercicios exploran formas en que podemos examinar y aprovechar la estructura de los cuerpos finitos en Sage.

22.7 Ejercicios en Sage

1. Cree un cuerpo finito de orden 5^2 y factorice $p(x) = x^{25} - x$ sobre este cuerpo. Comente sobre qué es lo interesante de este resultado y por qué no es una sorpresa.

2. El Corolario 22.11 dice que los elementos distintos de cero de un cuerpo finito forman un grupo cíclico con la multiplicación. El generador usado en Sage es también un generador de este grupo multiplicativo. Para ver esto, cree un cuerpo finito de orden 2^7. Cree dos listas de los elementos del cuerpo: primero, use el método `.list()`, luego use una lista por comprensión para generar las potencias del generador especificado en la creación del cuerpo.
A la segunda lista le faltará el cero para ser el cuerpo completo. Cree el elemento 0 del cuerpo (quizás coercionando 0 para que pertenezca al cuerpo) y agréguelo a la lista de potencias usando `.append()`. Use el comando `sorted()` con cada una de las listas y verifique la igualdad.

3. Los subcuerpos de un cuerpo finito están completamente clasificados por el Teorema 22.7. Es posible crear dos cuerpos finitos de los órdenes apropiados para que se cumpla la relación de extensión/subcuerpo, y traducir de uno a otro. Pero en este ejericicio construiremos un subcuerpo de un cuerpo finito desde cero. Como el grupo de elementos distintos de cero en un cuerpo finito es cíclico, los elementos distintos de cero de un subcuerpo formarán un subgrupo del grupo cíclico, que necesariamente será cíclico.
Cree un cuerpo finito de orden 3^6. La teoría dice que existe un subcuerpo de orden 3^2, pues $2|6$. Determine un generador de orden multiplicactivo 8 para los elementos distintos de cero de este subcuerpo, y construya estos 8 elementos. Agregue el elemento cero del cuerpo a esta lista. Debiera ser claro que este conjunto de 9 elementos es cerrado bajo multiplicación. En ausencia de nuestros teoremas sobre cuerpos finitos y grupos cíclicos, la clausura bajo la suma no es obvia. Escriba una línea que verifique si este conjunto es cerrado bajo sumas, considerando todas la posibles sumas de elementos del conjunto.

4. Este problema investiga la "separabilidad" de $\mathbb{Q}(\sqrt{3},\sqrt{7})$. Usted puede crear este cuerpo de números rápidamente con el constructor `NumberFieldTower`, junto con los polinomios x^2-3 y x^2-7. Aplane la torre con el método `.absolute_field()` y use el método `.structure()` para recuperar los isomorfismos entre la torre y la versión plana del cuerpo. Nombre a la torre como `N` y use `a` y `b` como generadores. Nombre la versión plana como `L` con `c` como generador.
Cree un elemento no trivial ("aleatorio") de `L` usando tantas potencias de `c` como sea posible (verifique el grado de `L` para ver cuántas potencias linealmente independientes existen). Solicite a Sage el polinomio minimal de su elemento aleatorio, asegurando así que el elemento es una raíz. Construya ese polinomio minimal como polinomio sobre `N`, la torre de cuerpos, y encuentre su factorización. Esta factorización debiese tener solo factores lineales. Cada raíz debiese ser una expresión en `a` y `b`. Convierta cada aríz en una expresión con notación matemática que involucre $\sqrt{3}$ y $\sqrt{7}$. Use una de las funciones para verificar que una de las raíces corresponde al elemento aleatorio original.
Cree unos pocos elementos aleatorios más, y encuentre una factorización (en `N` o en `L`). Para que un cuerpo sea separable, todo elemento del cuerpo debe ser una raíz de *algún* polinomio separable. El polinomio minimal es un buen polinomio para probar. (¿Por qué?) Basado en esta evidencia, ¿parece que $\mathbb{Q}(\sqrt{3},\sqrt{7})$ fuera una extensión separable?

5. El Ejercicio 22.3.21 describe el automorfismo de Frobenius de un cuerpo finito. Si `F` es un cuerpo finito en Sage, entonces `End(F)` creará el grupo de automorfismos de `F`.

(a) Trabaje el Ejercicio 22.3.21 para mejorar su comprensión de como y por qué la función de Frobenius es un automorfismo de cuerpos. (Lo que viene será más sencillo si hace esto primero.)

(b) Para algunos cuerpos finito pequeños, pero no triviales identifique el automorfismo de Frobenius dentro del grupo de automorfismos. Pequeños podría significar $p = 2, 3, 5, 7$ y $3 \leq n \leq 10$, con n primo versus compuesto.

(c) Una vez que haya identificado la función de Frobenius, describa los demás automorfismos. En otras palabras, con un poco de investigación, debiese ser posible dar una descripción de los automorfismos que le permita predecir correctamente el grupo completo de automorfismos de un cuerpo finito que no haya explorado aún. (Ayuda: el grupo de automorfismos del grupo es un grupo. ¿Qué pasa si "hace la operación" de la función de Frobenius consigo misma? ¿Qué es exactamente esta operación? Intente

usar la notación multiplicativa de Sage con los elementos del grupode automorfismos.)

(d) ¿Cuál es la "estructura" del grupo de automorfismos? ¿Cuál es el rol especial de la función de Frobenius en este grupo?

(e) Para cualquier cuerpo, el subcuerpo conocido como cuerpo fijo es una construcción importantes, y será lo será más aún en el siguiente capítulo. Dado un automorfismo τ de un cuerpo E, se puede demostrar que el subconjunto, $K = \{b \in E \mid \tau(b) = b\}$, es un subcuerpo de E. Se conoce como el ***cuerpo fijo*** de τ en E. Para cada automorfismo de $E = GF(3^6)$ identifique su cuerpo fijo. Como entendemos la estructura de subcuerpos de un cuerpo finito, es suficiente con determinar el orden de un cuerpo fijo para identificarlo completamente.

6. El Ejercicio 22.3.15 sugiere que todo elemento de un cuerpo finito puede ser escrito (expresado) como suma de cuadrados. Acá se sugieren experimentos computacionales que pueden ayudarle a formular una demostración del ejercicio.

(a) Construya dos cuerpos pequeños pero no demasiado pequeños, uno con $p = 2$ y el otro con un primo impar. Repita lo siguiente con cada cuerpo F.

(b) Escoja un elemento "aleatorio" del cuerpo, digamos $a \in F$. Construya los conjuntos

$$\{x^2 | x \in F\} \qquad\qquad \{a - x^2 | x \in F\}$$

usando conjuntos Sage con el constructor $Set()$. (Cuidado: `set()` es un comando Python que se comporta de forma fundamentalmente diferente.)

(c) Examine el tamaño de los dos conjunto y el tamaño de su intersección (`.intersection()`). Pruebe con diferentes elementos a, quizás usando un bucle para probar *todos* los valores posibles. Note que $p = 2$ se comportará de forma bastante diferente.

(d) Supongamos que tiene un elemento de la intersección. (Puede obtener uno con el método `.an_element()`.) ¿Cómo lelleva esto a la suma de cuadrados propuesta en el ejercicio?

(e) ¿Puede escribir una función en Python que reciba un cuerpo finito cuyo orden sea una potencia de un primo impar y luego liste cada elemento como suma de cuadrados?

23

Teoría de Galois

Un problema cásico de álgebra es encontrar las soluciones de una ecuación polinomial. La solución de la ecuación cuadrática se conoce desde la antiguedad. Matemáticos italianos encontraron soluciones geenrales para las ecuaciones cúbica y cuártica en el siglo XVI; sin embargo, todos los intentos por resolver la ecuación general de grado cinco, o quíntica, fueron infructuosos durante los siguientes trecientos años. Por supuesto, ecuaciones particulares como $x^5 - 1 = 0$ o $x^6 - x^3 - 6 = 0$ podían ser resueltas, pero ninguna solución similar a la fórmula cuadrática fue encontrada para la ecuación general de grado cinco,

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0.$$

Finalmente, al comienzo del siglo XIX, Ruffini y Abel ambos encontraron quínticas que no podían resolverse con ninguna fórmula. Fue Galois, sin embargo, quien produjo la explicación completa mostrando que polinomios podían o no podían ser resueltos mediante fórmulas. Él descubrió la conección entre los grupos y las extensiones de cuerpos. La teoría de Galois demuestra la fuerte interdependencia que existe entre la teoría de grupos y la teoría de cuerpos y ha tenido importantes consecuencias mucho más allá de su objetivo inicial.

En este capítulo demostraremos el Teorema Fundamental de la Teoría de Galois. Este resultado se usará para demostrar la insolubilidad de la quíntica y para demostrar el Teorema Fundamental del Álgebra.

23.1 Automorfismos de Cuerpos

Nuestra primera tarea es la de establecer una conección entre la teoría de grupos y la teoría de cuerpos examinando los automorfismos de cuerpos.

Proposición 23.1. *El conjunto de todos los automorfismos de un cuerpo F es un grupo con la operación de composición de funciones.*

Demostración. Si σ y τ son automorfismos de F, entonces también lo son $\sigma\tau$ y σ^{-1}. La identidad es por cierto un automorfismo; luego, el conjunto de todos los automorfismos de un cuerpo F es un grupo. □

Proposición 23.2. *Sea E una extensión de cuerpos de F. Entonces el conjunto de todos los automorfismos de E que fijan cada elemento de F es un grupo; es decir, el conjunto de todos los automorfismos $\sigma : E \to E$ tales que $\sigma(\alpha) = \alpha$ para todo $\alpha \in F$ es un grupo.*

Demostración. Solo nos falta mostrar que el conjunto de automorfismos de E que fijan cada elemento de F es un subgrupo de todos los automorfismos de E. Sean σ y τ dos automorfismos de E tales que $\sigma(\alpha) = \alpha$ y $\tau(\alpha) = \alpha$ para

todo $\alpha \in F$. Entonces $\sigma\tau(\alpha) = \sigma(\alpha) = \alpha$ y $\sigma^{-1}(\alpha) = \alpha$. Como la identidad fija todo elemento de E, el conjunto de los automorfismos de E que deja fijos los elementos de F es un subgrupo del grupo de todos los automorfismos de E. □

Sea E una extensión de cuerpos de F. Denotaremos el grupo de todos los automorfismos de E como $\mathrm{Aut}(E)$. Definimos el ***grupo de Galois*** de E sobre F como el grupo de los automorfismos de E que fijan todos los elementos de F; es decir,

$$G(E/F) = \{\sigma \in \mathrm{Aut}(E) : \sigma(\alpha) = \alpha \text{ para todo } \alpha \in F\}.$$

Si $f(x)$ es un polinomio en $F[x]$ y E es el cuerpo de descomposición de $f(x)$ sobre F, entonces definimos el grupo de Galois de $f(x)$ como $G(E/F)$.

Ejemplo 23.3. La conjugación compleja, definida como $\sigma : a + bi \mapsto a - bi$, es un automorfism de los números complejos. Como

$$\sigma(a) = \sigma(a + 0i) = a - 0i = a,$$

el automorfismo definido por conjugación compleja está en $G(\mathbb{C}/\mathbb{R})$.

Ejemplo 23.4. Considere los cuerpos $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}\,) \subset \mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$. Entonces para $a, b \in \mathbb{Q}(\sqrt{5}\,)$,

$$\sigma(a + b\sqrt{3}\,) = a - b\sqrt{3}$$

es un automorfismode $\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ que deja $\mathbb{Q}(\sqrt{5}\,)$ fijo. Similarmente,

$$\tau(a + b\sqrt{5}\,) = a - b\sqrt{5}$$

es un automorfismo de $\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ que deja $\mathbb{Q}(\sqrt{3}\,)$ fijo. El automorfismo $\mu = \sigma\tau$ mueve tanto $\sqrt{3}$ como $\sqrt{5}$. Pronto estará claro que $\{\mathrm{id}, \sigma, \tau, \mu\}$ es el grupo de Galois $\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ sobre $\mathbb{Q}$. La próxima tabla muestra que este grupo es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	id	μ	τ
τ	τ	μ	id	σ
μ	μ	τ	σ	id

Podemos también considerar el cuerpo $\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ como un espacio vectorial sobre $\mathbb{Q}$ que tiene base $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\,\}$. No es gran coincidencia que $|G(\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)/\mathbb{Q})| = [\mathbb{Q}(\sqrt{3}, \sqrt{5}\,) : \mathbb{Q})] = 4$.

Proposición 23.5. *Sea E una extensión de cuerpos de F y sea $f(x)$ un polinomio en $F[x]$. Entonces cualquier automorfismo en $G(E/F)$ define una permutación de las raíces de $f(x)$ que están en E.*

Demostración. Sea

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

y supponga que $\alpha \in E$ es un cero de $f(x)$. Entonces para $\sigma \in G(E/F)$,

$$\begin{aligned} 0 &= \sigma(0) \\ &= \sigma(f(\alpha)) \\ &= \sigma(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n) \\ &= a_0 + a_1\sigma(\alpha) + a_2[\sigma(\alpha)]^2 + \cdots + a_n[\sigma(\alpha)]^n; \end{aligned}$$

por lo tanto, $\sigma(\alpha)$ también es un cero de $f(x)$. □

Sea E una extensión algebraica de un cuerpo F. Dos elementos $\alpha, \beta \in E$ son ***conjugados*** sobre F si tienen el mismo polinomio minimal. Por ejemplo, en el cuerpo $\mathbb{Q}(\sqrt{2})$ los elementos $\sqrt{2}$ y $-\sqrt{2}$ son conjugados sobre $\mathbb{Q}$ pues ambos son raíces del polinomio irreducible $x^2 - 2$.

Existe un recíproco para la proposición anterior. La demostración sigue directamente del Lema 21.32.

Proposición 23.6. *Si α y β son conjugados sobre F, entonces existe un isomorfismo $\sigma : F(\alpha) \to F(\beta)$ tal que σ es la identidad cuando se restringe a F.*

Teorema 23.7. *Sea $f(x)$ un polinomio en $F[x]$ y supongamos que E es el cuerpo de descomposición para $f(x)$ sobre F. Si $f(x)$ no tiene raíces repetidas, entonces*

$$|G(E/F)| = [E : F].$$

Demostración. Procederemos por inducción en el grado de $f(x)$. Si el grado de $f(x)$ es 0 o 1, entonces $E = F$ y no hay nada que mostrar . Supongamos que el resultado se cumple para todos los polinomios de grado k con $0 \leq k < n$. Supongamos que el grado de $f(x)$ is n. Sea $p(x)$ un factor irreducible de $f(x)$ de grado r. Como todas las raíces de $p(x)$ están en E, podemos escoger una de esas raíces, digamos α, de manera que $F \subset F(\alpha) \subset E$. Entonces

$$[E : F(\alpha)] = n/r \quad \text{and} \quad [F(\alpha) : F] = r.$$

Si β es cualquier otra raíz de $p(x)$, entonces $F \subset F(\beta) \subset E$. Por el Lema 21.32, existe un único isomorfismo $\sigma : F(\alpha) \to F(\beta)$ para cada β que fija todos los elementos de F. Como E es un cuerpo de descomposición de $p(x)$, hay exactamente r tales isomorfismos. Para cada uno de estos automorfismos, podemos usar la hipótesis de inducción en $[E : F(\alpha)] = n/r < n$ para concluir que

$$|G(E/F(\alpha))| = [E : F(\alpha)].$$

Por lo tanto, existen

$$[E : F] = [E : F(\alpha)][F(\alpha) : F] = n$$

automorfismos posibles de E que fijan F, y $|G(E/F)| = [E : F]$. □

Corolario 23.8. *Sea F un cuerpo finito con una extensión finita E tal que $[E : F] = k$. Entonces $G(E/F)$ es cíclico de orden k.*

Demostración. Sea p la característica de E y de F y supongamos que los órdenes de E y F son p^m y p^n, respectivamente. Entonces $nk = m$. Podemos suponer además que E es el cuerpo de descomposición de $x^{p^m} - x$ sobre un subcuerpo de orden p. Por lo tanto, E también debe ser el cuerpo de descomposición de $x^{p^m} - x$ sobre F. Aplicando el Teorema 23.7, encontramos que $|G(E/F)| = k$.

Para demostrar que $G(E/F)$ es cíclico, debemos encontrar un generador para $G(E/F)$. Sea $\sigma : E \to E$ definido como $\sigma(\alpha) = \alpha^{p^n}$. Afirmamos que σ es el elemento en $G(E/F)$ que estamos buscando. En primer lugar debemos mostrar que σ está en $\mathrm{Aut}(E)$. Si α y β están en E,

$$\sigma(\alpha + \beta) = (\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \sigma(\alpha) + \sigma(\beta)$$

por el Lema 22.3. Es fácil mostrar que $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$. Como σ es un homomorfismo no nulo de cuerpos, debe ser inyectivo. También debe ser sobreyectivo, pues E es un cuerpo finito. Sabemos que σ está en $G(E/F)$, pues

F es el cuerpo de descomposición de el cuerpo de descomposición de $x^{p^n} - x$ sobre el cuerpo base de orden p. Esto significa que σ deja fijo todos los elementos en F. Finalmente, debemos mostrar que el orden de σ es k. Por el Teorema 23.7, sabemos que

$$\sigma^k(\alpha) = \alpha^{p^{nk}} = \alpha^{p^m} = \alpha$$

es la identidad de $G(E/F)$. Pero σ^r no puede ser la identidad para $1 \leq r < k$; de lo contrario, $x^{p^{nr}} - x$ tendría p^m raíces, lo que es imposible. □

Ejemplo 23.9. Podemos ahora confirmar que el gruo de Galoi de $\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ sobre $\mathbb{Q}$ en el Ejemplo 23.4 es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Por cierto, el grupo $H = \{\mathrm{id}, \sigma, \tau, \mu\}$ es un subgrupo de $G(\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)/\mathbb{Q})$; pero, H debe ser todo $G(\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)/\mathbb{Q})$, pues

$$|H| = [\mathbb{Q}(\sqrt{3}, \sqrt{5}\,) : \mathbb{Q}] = |G(\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)/\mathbb{Q})| = 4.$$

Ejemplo 23.10. Calculemos el grupo de Galois de

$$f(x) = x^4 + x^3 + x^2 + x + 1$$

sobre $\mathbb{Q}$. Sabemos que $f(x)$ es irreducible por el Ejercicio 17.4.20 en el Capítulo 17. Más aún, como $(x-1)f(x) = x^5 - 1$ podemos usar el Teorema de DeMoivre para determinar que las raíces de $f(x)$ son ω^i, donde $i = 1, \ldots, 4$ y

$$\omega = \cos(2\pi/5) + i\sin(2\pi/5).$$

Luego, el cuerpo de descomposición de $f(x)$ debe ser $\mathbb{Q}(\omega)$. Podemos definir automorfismos σ_i de $\mathbb{Q}(\omega)$ como $\sigma_i(\omega) = \omega^i$ para $i = 1, \ldots, 4$. Es fácil verificar que estos son realmente automorfismos diferetnes en $G(\mathbb{Q}(\omega)/\mathbb{Q})$. Como

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = |G(\mathbb{Q}(\omega)/\mathbb{Q})| = 4,$$

los σ_i deben ser todo $G(\mathbb{Q}(\omega)/\mathbb{Q})$. Por lo tanto, $G(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_4$ pues ω es un generador para el grupo de Galois.

Extensiones Separables

Muchos de los resultados que hemos recién demostrado dependen del hecho de que un polinomio $f(x)$ en $F[x]$ no tiene raíces repetidas en su cuerpo de descomposición. Es evidente que debemos saber exactamente cuándo un polinomio se factoriza como producto de factores lineales distintos en su cuerpo de descomposición. Sea E el cuerpo de descomposición de un polinomio $f(x)$ en $F[x]$. Supongamos que $f(x)$ se factoriza sobre E como

$$f(x) = (x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2} \cdots (x - \alpha_r)^{n_r} = \prod_{i=1}^{r} (x - \alpha_i)^{n_i}.$$

Definimos la ***multiplicidad*** de una raíz α_i de $f(x)$ como n_i. Una raíz con multiplicidad 1 se llama ***raíz simple***. Recuerde que un polinomio $f(x) \in F[x]$ de grado$n$ es ***separable*** si tiene n raíces distintas en su cuerpo de descomposición E. Equivalentemente, $f(x)$ es separable si se factoriza como producto de factores lineales diferentes sobre $E[x]$. Una extensión E de F es una ***extensión separable*** de F si cada elemento en E es raíz de un polinomio separable en $F[x]$. Recuerde además que $f(x)$ es separable si y solo si $\mathrm{mcd}(f(x), f'(x)) = 1$ (Lema 22.5).

Proposición 23.11. *Sea $f(x)$ un polinomio irreducible sobre F. Si la característica de F es 0, entonces $f(x)$ es separable. Si la característica de F es p y $f(x) \neq g(x^p)$ para algún $g(x)$ en $F[x]$, entonces $f(x)$ también es separable.*

DEMOSTRACIÓN. Supongamos primero que $\operatorname{char} F = 0$. Como $\operatorname{gr} f'(x) < \operatorname{gr} f(x)$ y $f(x)$ es irreducible, la única forma de que $\operatorname{mcd}(f(x), f'(x)) \neq 1$ es si $f'(x)$ es el polinomio cero; sin embargo, esto es imposible en un cuerpo de característica cero. Si $\operatorname{char} F = p$, entonces $f'(x)$ puede ser el polinomio cero si cada coeficiente de $f'(x)$ es un múltiplo de p. Esto solo puede pasar si tenemos un polinomio de la forma $f(x) = a_0 + a_1x^p + a_2x^{2p} + \cdots + a_nx^{np}$. □

Las extensiones de un cuerpo F de la forma $F(\alpha)$ están entre las más fáciles de estudiar y entender. Dada una extensión de cuerpos E de F, La pregunta obvia es cuando es posible encontrar un elemento $\alpha \in E$ tal que $E = F(\alpha)$. En este caso, α se llama ***elemento primitivo***. Ya sabemos que los elementos primitivos existen para ciertas extensiones. Por ejemplo,

$$\mathbb{Q}(\sqrt{3}, \sqrt{5}\,) = \mathbb{Q}(\sqrt{3} + \sqrt{5}\,)$$

y

$$\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}\,i) = \mathbb{Q}(\sqrt[6]{5}\,i).$$

El Corolario 22.12 nos dice que existe un elemento primitivo para cualquier extensión finita de un cuerpo finito. El siguiente teorema nos dice que muchas veces es posible encontrar un elemento primitivo.

Teorema 23.12 (Teorema del Elemento Primitivo)**.** *Sea E una extensión finita separable de un cuerpo F. Entonces existe un $\alpha \in E$ tal que $E = F(\alpha)$.*

DEMOSTRACIÓN. Ya sabemos que no hay problema cuando F es un cuerpo finito. Supongamos que E es una extensión finita de un cuerpo infinito. Demostraremos el resultado para $F(\alpha, \beta)$. El resultado general es consecuencia de éste por un simple argumento de inducción. Sean $f(x)$ y $g(x)$ los polinomios minimales de α y β, respectivamente. Sea K el cuerpo en que tanto $f(x)$ y $g(x)$ se descomponen. Supongamos que $f(x)$ tiene ceros $\alpha = \alpha_1, \ldots, \alpha_n$ en K y que $g(x)$ tiene ceros $\beta = \beta_1, \ldots, \beta_m$ en K. Todos estos ceros tienen multiplicidad 1, pues E es separable sobre F. Como F es infinito, podemos encontrar a en F tal que

$$a \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}$$

para todo i y j con $j \neq 1$. Por lo tanto, $a(\beta - \beta_j) \neq \alpha_i - \alpha$. Sea $\gamma = \alpha + a\beta$. Entonces

$$\gamma = \alpha + a\beta \neq \alpha_i + a\beta_j;$$

luego, $\gamma - a\beta_j \neq \alpha_i$ para todo i, j con $j \neq 1$. Defina $h(x) \in F(\gamma)[x]$ como $h(x) = f(\gamma - ax)$. Entonces $h(\beta) = f(\alpha) = 0$. Pero $h(\beta_j) \neq 0$ para $j \neq 1$. Luego, $h(x)$ y $g(x)$ tienen un solo factor común en $F(\gamma)[x]$; es decir, el polinomio minimal de β sobre $F(\gamma)$ debe ser lineal, pues β es el único cero común a $g(x)$ y $h(x)$. Así $\beta \in F(\gamma)$ y $\alpha = \gamma - a\beta$ está en $F(\gamma)$. Luego, $F(\alpha, \beta) = F(\gamma)$. □

23.2 El Teorema Fundamental

El objetivo de esta sección es demostrar el Teorema Fundamental de la Teoría de Galois. Este teorema explica la conección entre los subgrupos de $G(E/F)$ y los cuerpos intermedios entre E y F.

Proposición 23.13. *Sea $\{\sigma_i : i \in I\}$ una colección de automorfismos de un cuerpo F. Entonces*

$$F_{\{\sigma_i\}} = \{a \in F : \sigma_i(a) = a \text{ para todo } \sigma_i\}$$

es un subcuerpo de F.

Demostración. Sean $\sigma_i(a) = a$ y $\sigma_i(b) = b$. Entonces

$$\sigma_i(a \pm b) = \sigma_i(a) \pm \sigma_i(b) = a \pm b$$

y

$$\sigma_i(ab) = \sigma_i(a)\sigma_i(b) = ab.$$

Si $a \neq 0$, entonces $\sigma_i(a^{-1}) = [\sigma_i(a)]^{-1} = a^{-1}$. Finalmente, $\sigma_i(0) = 0$ y $\sigma_i(1) = 1$ como σ_i es un automorfismo. □

Corolario 23.14. *Sea F un cuerpo y sea G un subgrupo de $\mathrm{Aut}(F)$. Entonces*

$$F_G = \{\alpha \in F : \sigma(\alpha) = \alpha \text{ para todo } \sigma \in G\}$$

es un subcuerpo de F.

El subcuerpo $F_{\{\sigma_i\}}$ de F se llama ***cuerpo fijo*** de $\{\sigma_i\}$. El cuerpo fijo por un subgrupo G de $\mathrm{Aut}(F)$ se denotará como F_G.

Ejemplo 23.15. Sea $\sigma : \mathbb{Q}(\sqrt{3}, \sqrt{5}\,) \to \mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ el automorfismo que envía $\sqrt{3}$ en $-\sqrt{3}$. Entonces $\mathbb{Q}(\sqrt{5}\,)$ es el subcuerpo de $\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ fijo por σ.

Proposición 23.16. *Sea E un cuerpo de descomposición sobre F de un polinomio separable. Entonces $E_{G(E/F)} = F$.*

Demostración. Sea $G = G(E/F)$. Claramente, $F \subset E_G \subset E$. Además, E debe ser un cuerpo de descomposición de E_G y $G(E/F) = G(E/E_G)$. Por el Teorema 23.7,

$$|G| = [E : E_G] = [E : F].$$

Por lo tanto, $[E_G : F] = 1$. Concluimos que $E_G = F$. □

Muchos matemáticos aprendieron por primera vez teoría de Galois a través de la monografía de Emil Artin sobre el tema [1]. La astuta demostración del lema siguiente se debe a Artin.

Lema 23.17. *Sea G un grupo finito de automorfismos de E y sea $F = E_G$. Entonces $[E : F] \leq |G|$.*

Demostración. Sea $|G| = n$. Debemos mostrar que cualquier conjunto de $n+1$ elementos $\alpha_1, \ldots, \alpha_{n+1}$ en E es linealmente dependiente sobre F; es decir, debemos encontrar elementos $a_i \in F$, no todos cero, tales que

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_{n+1}\alpha_{n+1} = 0.$$

Supongamos que $\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n$ son los automorfismos en G. El sistema de ecuaciones lineales homogéneo

$$\begin{aligned}
\sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\
\sigma_2(\alpha_1)x_1 + \sigma_2(\alpha_2)x_2 + \cdots + \sigma_2(\alpha_{n+1})x_{n+1} &= 0 \\
&\vdots \\
\sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0
\end{aligned}$$

tiene más incógnita que ecuaciones. De álgebra lineal sabemos que este sistema tiene una solución no trivial, digamos $x_i = a_i$ para $i = 1, 2, \ldots, n+1$. Como σ_1 es la identidad, la primera ecuación se traduce a

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_{n+1}\alpha_{n+1} = 0.$$

El problema es que algunos de los a_i podrían estar en E pero no en F. Debemos mostrar que esto es imposible.

Supongamos que al menos uno de los a_i está en E pero no en F. Reordenando los α_i podemos suponer que a_1 es distinto de cero. Como cualquier múltiplo de una solución también es una solución, podemos suponer además que $a_1 = 1$. De todas las posibles soluciones que satisfacen esta descripción, elegimos la que tenga el menor número de términos distintos de cero. Nuevamente, reordenando $\alpha_2, \ldots, \alpha_{n+1}$ si fuera necesario, podemos suponer que a_2 está en E pero no en F. Como F es el subcuerpo de E cuyos elementos quedan fijos por G, existe σ_i en G tal que $\sigma_i(a_2) \neq a_2$. Aplicando σ_i a cada ecuación en el sistema, obtenemos el mismo sistema homogéneo, pues G es un grupo. Por lo tanto, $x_1 = \sigma_i(a_1) = 1$, $x_2 = \sigma_i(a_2)$, …, $x_{n+1} = \sigma_i(a_{n+1})$ también es solución del sistema original. Sabemos que una combinación lineal de dos soluciones de un sistema homogéneo es nuevamente una solución; concluimos que

$$\begin{aligned} x_1 &= 1 - 1 = 0 \\ x_2 &= a_2 - \sigma_i(a_2) \\ &\vdots \\ x_{n+1} &= a_{n+1} - \sigma_i(a_{n+1}) \end{aligned}$$

debe ser otra solución del sistema. Esta es una solución no trivial pues $\sigma_i(a_2) \neq a_2$, y tiene menos términos distintos de cero que nuestra solución original. Esto es una contradicción, pues elnúmero de términos distintos de cero de nuestra solución original se había supuesto minimal. Podemos concluir que $a_1, \ldots, a_{n+1} \in F$. □

Sea E una extensión algebraica de F. Si todo polinomio irreducible en $F[x]$ con una raíz en E tiene todas sus raíces en E, entonces E se llama ***extensión normal*** de F; es decir, todo polinomio irreducible en$F[x]$ que contiene una raíz en E es el producto de factores lineales en $E[x]$.

Teorema 23.18. *Sea E una extensión de cuerpos de F. Entonces las siguientes proposiciones son equivalentes.*

1. *E es una extensión finita, normal y separable de F.*
2. *E es el cuerpo de descomposición sobre F de un polinomio separable.*
3. *$F = E_G$ para algún grupo finito G de automorfismos de E.*

Demostración. (1) ⇒ (2). Sea E una extensión finita, normal y separable de F. Por el Teorema del Elemento Primitivo, podemos encontrar α en E tal que $E = F(\alpha)$. Sea $f(x)$ el polinomio minimal de α sobre F. El cuerpo E debe contener todas las raíces de $f(x)$ pues es una extensión normal de F; luego, E es un cuerpo de descomposición para $f(x)$.

(2) ⇒ (3). Sea E el cuerpo de descomposición sobre F de un polinomio separable. Por la Proposición 23.16, $E_{G(E/F)} = F$. Como $|G(E/F)| = [E : F]$, este grupo es finito.

(3) ⇒ (1). Sea $F = E_G$ para cierto grupo finito de automorfismos G de E. Como $[E : F] \leq |G|$, E es una extensión finita de F. Para mostrar que E es

una extensión finita y normal de F, sea $f(x) \in F[x]$ un polinomio irreducible mónico que tenga una raíz α en E. Debemos mostrar que $f(x)$ es el producto de factores lineales distintos en $E[x]$. Por la Proposición 23.5, los automorfismos en G permutan las raíces de $f(x)$ que están en E. Por lo tanto, si hacemos actuar G en α, podemos obtener raíces distintas $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ en E. Sea $g(x) = \prod_{i=1}^{n}(x - \alpha_i)$. Entonces $g(x)$ es separable sobre F y $g(\alpha) = 0$. Cualquier automorfismo σ en G permuta los factores de $g(x)$ pues permuta estas raíces; luego, cuando σ actúa en $g(x)$, debe fijar los coeficientes de $g(x)$. Por lo tanto, los coeficientes de $g(x)$ están en F. Como $\operatorname{gr} g(x) \leq \operatorname{gr} f(x)$ y $f(x)$ es el polinomio minimal de α, $f(x) = g(x)$. □

Corolario 23.19. *Sea K una extensión de cuerpos de F tal que $F = K_G$ para cierto grupo finito de automorfismos G de K. Entonces $G = G(K/F)$.*

Demostración. Como $F = K_G$, G es un subgrupo de $G(K/F)$. Luego,

$$[K : F] \leq |G| \leq |G(K/F)| = [K : F].$$

Se sigue que $G = G(K/F)$, tienen el mismo orden. □

Antes de determiar la correspondencia exacta entre extensiones de cuerpos y automorfismos de cuerpos, volvamos a un ejemplo familiar.

Ejemplo 23.20. En el Ejemplo 23.4 examinamos los automorfismos de $\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ que fijan $\mathbb{Q}$. La Figura 23.21 compara el reticulado de extensiones de cuerpos de $\mathbb{Q}$ con el reticulado de subgrupos de $G(\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)/\mathbb{Q})$. El Teorema Fundamental de la Teoría de Galois nos dice cuál es la relación entre estos dos reticulados.

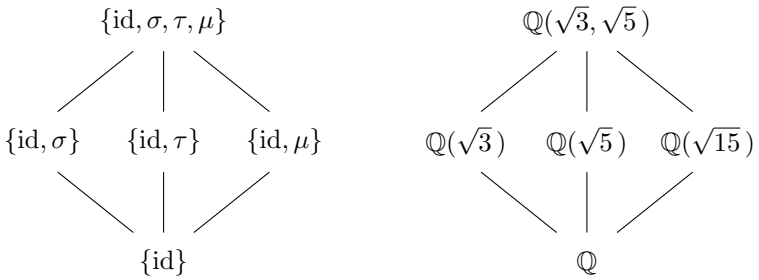


Figura 23.21: $G(\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)/\mathbb{Q})$

Estamos preparados para enunciar y demostrar el Teorema Fundamental de la Teoría de Galois.

Teorema 23.22 (Teorema Fundamental de la Teoría de Galois)**.** *Sea F un cuerpo finito o un cuerpo de característica cero. Si E es una extensión normal finita de F con grupo de Galois $G(E/F)$, entonces las siguientes proposiciones son verdaderas.*

1. *La función $K \mapsto G(E/K)$ es una biyección entre los subcuerpos K de E que contienen F y los subgrupos de $G(E/F)$.*
2. *Si $F \subset K \subset E$, entonces*

$$[E : K] = |G(E/K)| \text{ y } [K : F] = [G(E/F) : G(E/K)].$$

3. *$F \subset K \subset L \subset E$ si y solo si $\{\mathrm{id}\} \subset G(E/L) \subset G(E/K) \subset G(E/F)$.*

4. *K es una extensión normal de F si y solo si $G(E/K)$ es un subgrupo normal de $G(E/F)$. En ese caso*

$$G(K/F) \cong G(E/F)/G(E/K).$$

DEMOSTRACIÓN. (1) Supongamos que $G(E/K) = G(E/L) = G$. Tanto K como L son cuerpos fijos de G; luego, $K = L$ y la función definida por $K \mapsto G(E/K)$ es 1-1. PAra mostrar que la función es sobreyectiva, sea G un subgrupo de $G(E/F)$ y sea K el cuerpo fijo por G. Entonces $F \subset K \subset E$; Así, E es una extensión normal de K. Luego, $G(E/K) = G$ y la función $K \mapsto G(E/K)$ es una biyección.

(2) Por el Teorema23.7, $|G(E/K)| = [E : K]$; por lo tanto,

$$|G(E/F)| = [G(E/F) : G(E/K)] \cdot |G(E/K)| = [E : F] = [E : K][K : F].$$

Luego, $[K : F] = [G(E/F) : G(E/K)]$.

(3) La proposición se ilustra en la Figura 23.23. Dejamos su demostración como un ejercicio.

(4) Esto requiere un poco más de trabajo. Sea K una extensión normal de F. Si σ está en $G(E/F)$ y τ está en $G(E/K)$, debemos demostrar que $\sigma^{-1}\tau\sigma$ está en $G(E/K)$; es decir, debemos mostrar que $\sigma^{-1}\tau\sigma(\alpha) = \alpha$ para todo $\alpha \in K$. Supongamos que $f(x)$ es el polinomio minimal de α sobre F. Entonces $\sigma(\alpha)$ también es una raíz de $f(x)$ que está en K, pues K es una extensión normal de F. Luego, $\tau(\sigma(\alpha)) = \sigma(\alpha)$ y $\sigma^{-1}\tau\sigma(\alpha) = \alpha$.

Recíprocamente, sea $G(E/K)$ un subgrupo normal de $G(E/F)$. Debemos demostrar que $F = K_{G(K/F)}$. Sea $\tau \in G(E/K)$. Para todo $\sigma \in G(E/F)$ existe $\overline{\tau} \in G(E/K)$ tal que $\tau\sigma = \sigma\overline{\tau}$. De esta manera, para todo $\alpha \in K$

$$\tau(\sigma(\alpha)) = \sigma(\overline{\tau}(\alpha)) = \sigma(\alpha);$$

luego, $\sigma(\alpha)$ es el cuerpo fijo de $G(E/K)$. Sea $\overline{\sigma}$ la restricción de σ a K. Entonces $\overline{\sigma}$ es un automorfismo de K que fija F, pues $\sigma(\alpha) \in K$ para todo $\alpha \in K$; luego, $\overline{\sigma} \in G(K/F)$. A continuación, mostraremos que el cuerpo fijo de $G(K/F)$ es F. Sea β un elemento en K que queda fijo por todos los automorfismos en $G(K/F)$. En particular, $\overline{\sigma}(\beta) = \beta$ para todo $\sigma \in G(E/F)$. Por lo tanto, β pertenece al cuerpo fijo F de $G(E/F)$.

Finalmente, debemos mostrar que si K es una extensión normal de F, entonces

$$G(K/F) \cong G(E/F)/G(E/K).$$

Sea $\sigma \in G(E/F)$, y sea σ_K el automorfismo de K obtenido restringiendo σ a K. Como K es una extensión normal, el argumento del párrafo precedente muestra que $\sigma_K \in G(K/F)$. Tenemos así una función $\phi : G(E/F) \to G(K/F)$ definida por $\sigma \mapsto \sigma_K$. Esta función es un homomorfismo de grupos pues

$$\phi(\sigma\tau) = (\sigma\tau)_K = \sigma_K\tau_K = \phi(\sigma)\phi(\tau).$$

El núcleo de ϕ es $G(E/K)$. Por (2),

$$|G(E/F)|/|G(E/K)| = [K : F] = |G(K/F)|.$$

Luego, la imagen de ϕ es $G(K/F)$ y ϕ es sobreyectiva. Por el Primer Teorema de Isomorfía, tenemos

$$G(K/F) \cong G(E/F)/G(E/K). \qquad \square$$

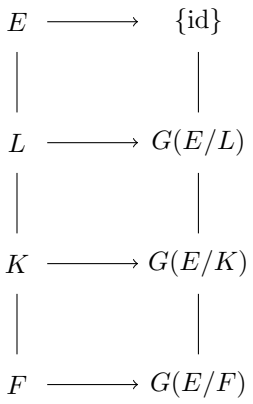


Figura 23.23: Subgrupos de $G(E/F)$ y subcuerpos de E

Ejemplo 23.24. En este ejemplo ilustraremos el Teorema Fundamental de la Teoría de Galois determinando el reticulado de subgrupos del grupo de Galois de $f(x) = x^4 - 2$. Compararemos este reticulado con el reticulado de extensiones de cuerpo de $\mathbb{Q}$ que están contenidas en el cuerpo de descomposición de $x^4 - 2$. El cuerpo de descomposición de $f(x)$ es $\mathbb{Q}(\sqrt[4]{2}, i)$. Para ver esto, notemos que $f(x)$ se factoriza como $(x^2 + \sqrt{2}\,)(x^2 - \sqrt{2}\,)$; así, las raíces de $f(x)$ son $\pm\sqrt[4]{2}$ y $\pm\sqrt[4]{2}\,i$. Primero adjuntamos la raíz $\sqrt[4]{2}$ a $\mathbb{Q}$ y luego adjuntamos la raíz i de $x^2 + 1$ a $\mathbb{Q}(\sqrt[4]{2}\,)$. Entonces el cuerpo de descomposición de $f(x)$ es $\mathbb{Q}(\sqrt[4]{2}\,)(i) = \mathbb{Q}(\sqrt[4]{2}, i)$.

Como $[\mathbb{Q}(\sqrt[4]{2}\,) : \mathbb{Q}] = 4$ y i no está en $\mathbb{Q}(\sqrt[4]{2}\,)$, debe ocurrir que $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2}\,)] = 2$. Luego, $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$. El conjunto

$$\{1, \sqrt[4]{2}, (\sqrt[4]{2}\,)^2, (\sqrt[4]{2}\,)^3, i, i\sqrt[4]{2}, i(\sqrt[4]{2}\,)^2, i(\sqrt[4]{2}\,)^3\}$$

es una base de $\mathbb{Q}(\sqrt[4]{2}, i)$ sobre $\mathbb{Q}$. El reticulado de extensiones de $\mathbb{Q}$ contenidas en $\mathbb{Q}(\sqrt[4]{2}, i)$ está ilustrado en la figura 23.25(a).

El grupo de Galois G de $f(x)$ debe ser de orden 8. Sea σ el automorfismo definido por $\sigma(\sqrt[4]{2}\,) = i\sqrt[4]{2}$ y $\sigma(i) = i$, y sea τ el automorfismo definido por conjugación compleja; es decir, $\tau(i) = -i$. Entonces G tiene un elemento de orden 4 y un elemento de orden 2. Es fácil verificar con un cálculo directo que los elementos de G son $\{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ y que se satisfacen las relaciones $\tau^2 = \mathrm{id}$, $\sigma^4 = \mathrm{id}$, y $\tau\sigma\tau = \sigma^{-1}$; luego, G es isomorfo a D_4. El reticulado de subgrupos de G está ilustrado en la Figura 23.25(b).

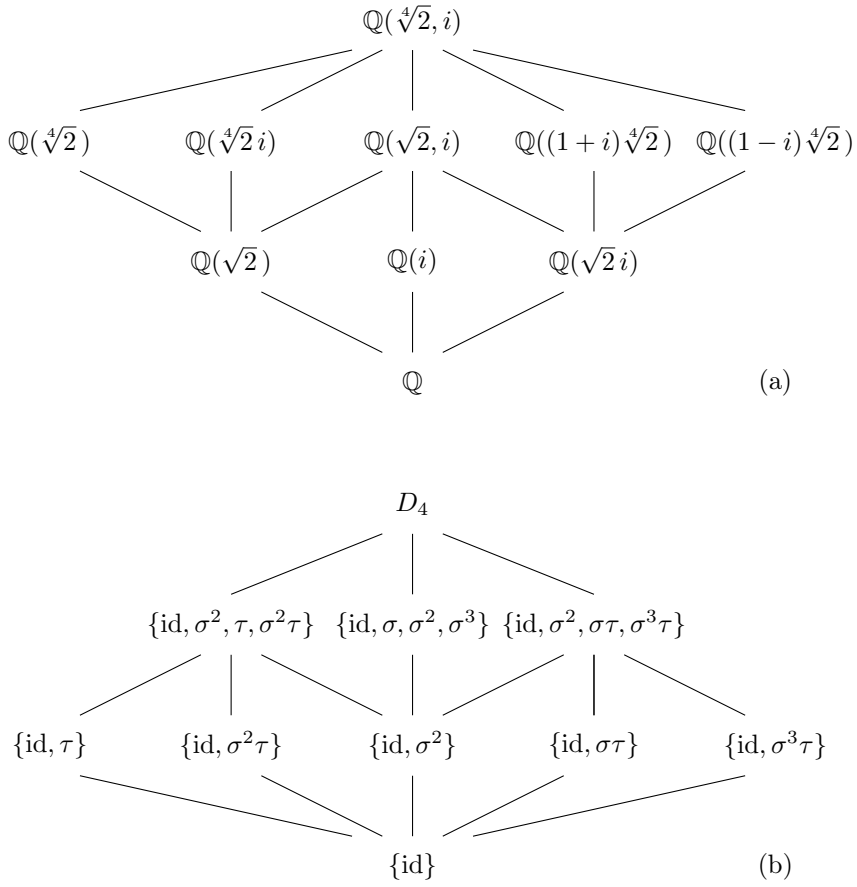


Figura 23.25: Grupo de Galois de $x^4 - 2$

Historical Note

Las fórmulas para las soluciones generales de las ecuaciones cúbicas y cuárticas fueron descubiertas en el siglo XVI. Los intentos de encontrar fórmulas similares para la ecuación quínticas desafiaron a algunos de los mejores matemáticos de la historia. En 1798, P. Ruffini envió una publicación afirmando que tal solución no era posible; pero su trabajoono fue bien recibido. En 1826, Niels Henrik Abel (1802–1829) finalmente ofreció la primera demostración correcta de que las ecuaciones quínticas no siempre se pueden resolver por radicales.

El trabajo de Abel fue una inspiración para Évariste Galois. Nacido en 1811, Galois comenzó a mostrar talento matemático extraordinario a los 14 años. Postuló a la École Polytechnique en varias ocasiones; pero tuvo gran dificultad en cumplir con los requisitos formales de admisión, y los examinadores no reconocieron su genialidad matemática. Finalmente fue admitido a la École Normale en 1829.

Galois desarrolló una teoría de solubilidad para polinomios. En 1829, a los 17 años, Galois presentó dos artículos sobre la solución de ecuaciones algebraicas a la Academia de Ciencias de París. Estos artículos fueron enviados a Cauchy, quién aparentemente los perdió. Un tercer artículo fue enviado a Fourier, quien murió antes de poder leerlo. Otro fue presentado, pero no fue publicado hasta 1846.

Las ideas democráticas de Galois lo llevaron a meterse en la Revolución de

1830. Fue expulsado de la escuelas y enviado a prisión por su participación en la revuelta. Luego de su liberación en 1832, se vio involucrado en un duelo, posiblemente por motivos amorosos. Seguro de que moriría, ocupó la tarde antes de su muerte delineando su trabajo y sus principales ideas de investigación en una larga carta a su amigo Chevalier. De hecho murió al día siguiente, con 20 años de edad.

23.3 Aplicaciones

Solubilidad por Radicales

En toda esta sección supondremos que los cuerpos tienen característica cero para asegurar que los polinomios irreducibles no tengan raíces repetidas. El objetivo inmediato de esta sección es determinar cuándo las raíces de un polinomio $f(x)$ se pueden calcular con un número finito de operaciones con los coeficientes de $f(x)$. Las operaciones permitidas son suma, resta, multipicación, división y extracción de raíces n-ésimas. Por cierto la solución de la ecuación cuadrática, $ax^2 + bx + c = 0$, ilustra este proceso:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

La única de estas operaciones que puede requerir un cuerpo más grande es la de extraer raíces n-ésimas. Esto nos lleva a la siguiente definición.

Una extensión E de un cuerpo F es una ***extensión por radicales*** si existe una cadena de subcuerpos

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r = E$$

tal que para $i = 1, 2, \ldots, r$, tenemos $F_i = F_{i-1}(\alpha_i)$ y $\alpha_i^{n_i} \in F_{i-1}$ para ciertos enteros positivos n_i. Un polinomio $f(x)$ es ***soluble por radicales*** sobre F si el cuerpo de descomposición K de $f(x)$ sobre F está contenido en una extensión por radicales de F. Nuestro objetivo es llegar a un criterio que nos diga si un polinomio $f(x)$ es o no soluble por radicales examinando su grupo de Galois $f(x)$.

El polinomio más fácil de resolver por radicales es uno de la forma $x^n - a$. Como vimos en el Capítulo 4, las raíces de $x^n - 1$ se llaman ***raíces n-ésimas de la unidad***. Estas raíces forman un subgrupo finito del cuerpo de descomposición de $x^n - 1$. Por el Corolario 22.11, las raíces n-ésimas de la unidad forman un grupo cíclico. Cualquier generador de este grupo es una ***raíz n-ésima primitiva de la unidad***.

Ejemplo 23.26. El polinomio $x^n - 1$ es soluble por radicales sobre $\mathbb{Q}$. Las raíces de este polinomio son $1, \omega, \omega^2, \ldots, \omega^{n-1}$, donde

$$\omega = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right).$$

El cuerpo de descomposición de $x^n - 1$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\omega)$.

Demostraremos que un polinomio es soluble por radicales si y solo si su grupo de Galois es soluble. Recuerde que una serie subnormal de un grupo G es una sucesión finita de subgrupos

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\},$$

tal que H_i es normal en H_{i+1}. Un grupo G es soluble si tiene una serie subnormal $\{H_i\}$ tal que todos los grupos cociente H_{i+1}/H_i son abelianos. Por

ejemplo, si examinamos la serie $\{\mathrm{id}\} \subset A_3 \subset S_3$, vemos que S_3 es soluble. Por otra parte, S_5 no es soluble, por el Teorema 10.11.

Lema 23.27. *Sea F un cuerpo de característica cero y E el cuerpo de descomposición de $x^n - a$ sobre F con $a \in F$. Entonces $G(E/F)$ es un grupo soluble.*

Demostración. Las raíces de $x^n - a$ son $\sqrt[n]{a}, \omega\sqrt[n]{a}, \ldots, \omega^{n-1}\sqrt[n]{a}$, con ω una raíz n-ésima primitiva de la unidad. Supongamos que F contiene todas las raíces n-ésimas de la unidad. Si ζ es una de las raíces de $x^n - a$, entonces las diferentes raíces de $x^n - a$ son $\zeta, \omega\zeta, \ldots, \omega^{n-1}\zeta$, y $E = F(\zeta)$. Como $G(E/F)$ permuta las raíces de $x^n - a$, los elemento en $G(E/F)$ deben estar determinados por su acción en estas raíces. Sean σ y τ en $G(E/F)$ y supongamos que $\sigma(\zeta) = \omega^i\zeta$ y $\tau(\zeta) = \omega^j\zeta$. If F contains the roots of unity, entonces

$$\sigma\tau(\zeta) = \sigma(\omega^j\zeta) = \omega^j\sigma(\zeta) = \omega^{i+j}\zeta = \omega^i\tau(\zeta) = \tau(\omega^i\zeta) = \tau\sigma(\zeta).$$

Por lo tanto, $\sigma\tau = \tau\sigma$ y $G(E/F)$ es abeliano, en particular es soluble.

Ahora supongamos que F no contiene raíces n-ésimass primitivas de la unidad. Sea ω un generador del grupo cíclico de las raíces n-ésimas de la unidad. Sea α un cero de $x^n - a$. Como α y $\omega\alpha$ están ambos en el cuerpo de descomposición de $x^n - a$, $\omega = (\omega\alpha)/\alpha$ también está en E. Sea $K = F(\omega)$. Entonces $F \subset K \subset E$. Since K es el cuerpo de descomposición de $x^n - 1$, K es una etensión normal de F. Por lo tanto, cualquier automorfismo σ en $G(F(\omega)/F)$ está determinado por $\sigma(\omega)$. Se debe tener que $\sigma(\omega) = \omega^i$ para algún entero i pues todos los ceros de $x^n - 1$ son potencias de ω. Si $\tau(\omega) = \omega^j$ está en $G(F(\omega)/F)$, entonces

$$\sigma\tau(\omega) = \sigma(\omega^j) = [\sigma(\omega)]^j = \omega^{ij} = [\tau(\omega)]^i = \tau(\omega^i) = \tau\sigma(\omega).$$

Por lo tanto, $G(F(\omega)/F)$ es abeliano. Por el Teorema Fundamental de la Teoría de Galois, la serie

$$\{\mathrm{id}\} \subset G(E/F(\omega)) \subset G(E/F)$$

es una serie normal. Por el argumento anterior, $G(E/F(\omega))$ es abeliano. Como

$$G(E/F)/G(E/F(\omega)) \cong G(F(\omega)/F)$$

también es abeliano, $G(E/F)$ es soluble. □

Lema 23.28. *Sea F un cuerpo de característica cero y sea*

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r = E$$

una extensión radical de F. Entonces existe una extensión radical normal

$$F = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_r = K$$

tal que K contiene a E y K_i es una extensión normal de K_{i-1}.

Demostración. Como E es una extensión radical de F, existe una cadena de subcuerpos

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r = E$$

tal que para $i = 1, 2, \ldots, r$, tenemos $F_i = F_{i-1}(\alpha_i)$ y $\alpha_i^{n_i} \in F_{i-1}$ para ciertos enteros positivos n_i. Construiremos una extensión radical normal de F,

$$F = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_r = K$$

tal que $K \supseteq E$. Defina K_1 como el cuerpo de descomposición de $x^{n_1} - \alpha_1^{n_1}$. Las ríces de este polinomio son $\alpha_1, \alpha_1\omega, \alpha_1\omega^2, \ldots, \alpha_1\omega^{n_1-1}$, donde ω es una raíz n_1-ésima primitiva de la unidad. Si F contiene las n_1 raíces de la unidad, entonces $K_1 = F(\alpha_!)$. Por otra parte, supongamos que F no contiene raíces n_1-ésimas primitivas de la unidad. Si β es una raíz de $x^{n_1} - \alpha_1^{n_1}$, entonces todas las raíces de $x^{n_1} - \alpha_1^{n_1}$ son $\beta, \omega\beta, \ldots, \omega^{n_1-1}$, con ω una raíz n_1-ésima primitiva de la unidad. En este caso, $K_1 = F(\omega\beta)$. Luego, K_1 es una extensión radical normal de F que contiene a F_1. Continuando de esta manera, obtenemos

$$F = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_r = K$$

tal que K_i es una extensión normal de K_{i-1} y $K_i \supseteq F_i$ para $i = 1, 2, \ldots, r$. □

Demostraremos ahora el teorema principal sobre solubilidad por radicales.

Teorema 23.29. *Sea $f(x)$ un polinomio en $F[x]$, con* $\operatorname{char} F = 0$. *Si $f(x)$ es soluble por radicales, entonces el grupo de Galois de $f(x)$ sobre F es soluble.*

Demostración. Como $f(x)$ es soluv¡ble por radicales existe una extensión E de F por radicales $F = F_0 \subset F_1 \subset \cdots \subset F_n = E$. Por el Lema 23.28, podemos suponer que E es un cuerpo de descomposición de $f(x)$ y F_i es normal sobre F_{i-1}. Por el Teorema Fundamental de la Teoría de Galois, $G(E/F_i)$ es un subgrupo normal de $G(E/F_{i-1})$. Por lo tanto, tenemos una serie subnormal de subgrupos de $G(E/F)$:

$$\{\mathrm{id}\} \subset G(E/F_{n-1}) \subset \cdots \subset G(E/F_1) \subset G(E/F).$$

Nuevamente por el Teorema Fundamental de la Teoría de Galois, sabemos que

$$G(E/F_{i-1})/G(E/F_i) \cong G(F_i/F_{i-1}).$$

Por el Lema 23.27, $G(F_i/F_{i-1})$ es soluble; luego, $G(E/F)$ también es soluble. □

El recíproco del Teorema 23.29 también es verdadero. Para una demostración, vea cualquiera de las referencias al final de este capítulo.

Insolubilidad de la Quíntica

Estamos ahora en condiciones de encontrar un polinomio de grado cinco que no es soluble por radicales. Simplemente debemos encontrar un polinomio cuyo grupo de Galois sea S_5. Empezaremos con un lema.

Lema 23.30. *Si p es primo, entonces cualquier subgrupo de S_p que contenga una transposición y un ciclo de largo p es todo S_p.*

Demostración. Sea G un subgrupo de S_p que contenga una transposición σ y τ un ciclo de largo p. Podemos suponer que $\sigma = (12)$. El orden de τ es p y τ^n es un ciclo de largo p para $1 \leq n < p$. Por lo tanto, podemos suponer que $\mu = \tau^n = (12i_3 \ldots i_p)$ para algún n, donde $1 \leq n < p$ (vea el Ejercicio 5.3.13 en el Capítulo 5). Observando que $(12)(12i_3 \ldots i_p) = (2i_3 \ldots i_p)$ y $(2i_3 \ldots i_p)^k(12)(2i_3 \ldots i_p)^{-k} = (1i_k)$, podemos obtener todas las transposiciones de la forma $(1n)$ para $1 \leq n < p$. Pero, estas transposiciones generan todas las transpociciones en S_p, pues $(1j)(1i)(1j) = (ij)$. Las transposiciones generan S_p. □

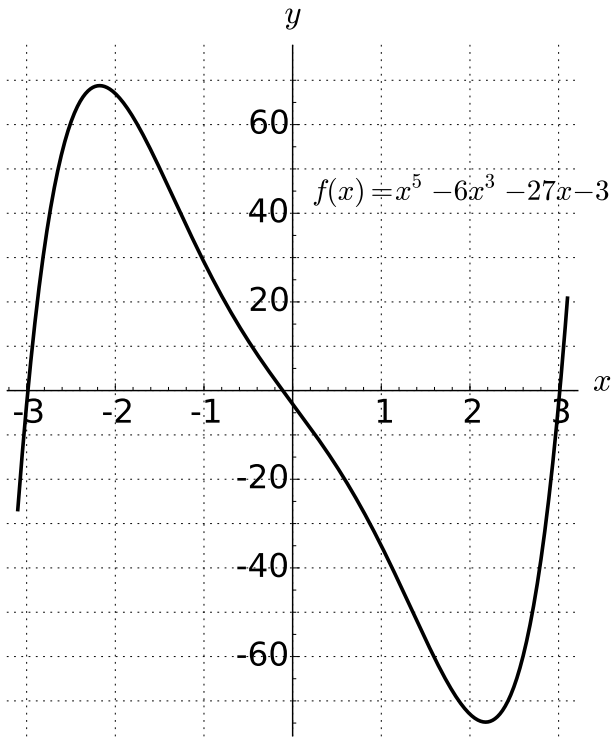


Figura 23.31: El grafo de $f(x) = x^5 - 6x^3 - 27x - 3$

Ejemplo 23.32. Mostraremos que $f(x) = x^5 - 6x^3 - 27x - 3 \in \mathbb{Q}[x]$ no es soluble. Afirmamos que el grupo de Galois de $f(x)$ sobre $\mathbb{Q}$ es S_5. Por el Criterio de Eisenstein, $f(x)$ es irreducible y, por lo tanto, es separable. La derivada de $f(x)$ es $f'(x) = 5x^4 - 18x^2 - 27$; luego, poniendo $f'(x) = 0$ y resolviendo, vemos que las únicas raíces reales de $f'(x)$ son

$$x = \pm\sqrt{\frac{6\sqrt{6}+9}{5}}.$$

Por lo tanto, $f(x)$ puede tener a lo sumo un máximo y un mínimo. Es fácil mostrar que $f(x)$ cambia de signo entre -3 y -2, entre -2 y 0, y una vez más entre 0 y 4 (Figura 23.31). Por lo tanto, $f(x)$ tiene precisamente tres raíces reales diferentes. Las restantes dos raíces de $f(x)$ deben ser complejos conjugados. Sea K el cuerpo de descomposición de $f(x)$. Como $f(x)$ tiene cincoraíces distintas en K y todo automorfismode K que fija a $\mathbb{Q}$ está determinado por la forma en que permuta las raíces de $f(x)$, sabemos que $G(K/\mathbb{Q})$ es un subgrupo de S_5. Como f es irreducible, hay un elemento en $\sigma \in G(K/\mathbb{Q})$ tal que $\sigma(a) = b$ para dos raíces a y b de $f(x)$. El automorfismo de $\mathbb{C}$ que envía $a+bi \mapsto a-bi$ dejas fijas las raíces reales e intercambia las raíces complejas; por ende, $G(K/\mathbb{Q})$ contiene una transposición. Si α es una de las raíces reale de $f(x)$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ por el Ejercicio 21.4.28. Como $\mathbb{Q}(\alpha)$ es un subcuerpo de K, debe ser que $[K : \mathbb{Q}]$ es divisible por 5. Como $[K : \mathbb{Q}] = |G(K/\mathbb{Q})|$ y $G(K/\mathbb{Q}) \subset S_5$, sabemos que $G(K/\mathbb{Q})$ contiene un ciclo de largo 5. Por el Lema 23.30, S_5 está generado por una transposición y un elemento de orden 5; por lo tanto, $G(K/\mathbb{Q})$ es todo S_5. Por el Teorema 10.11, S_5 no es soluble. Por lo tanto, $f(x)$ no se puede resolver por radicales.

El Teorema Fundamental del Álgebra

Parece apropiado que el último teorema que enunciemos y demostremos sea el Teorema Fundamental del Álgebra. Este teorema fue demostrado por primera vez por Gauss en su tesis doctoral. Antes de la demostración de Gauss, los matemáticos sospechaban que podrían existir polinomios sin soluciones sobre los números reales y los números complejos. El Teorema Fundamental del Álgebra establece que todo polinomio sobre los números complejos se factoriza como producto de factores lineales.

Teorema 23.33 (Teorema Fundamental del Álgebra)**.** *El cuerpo de los números complejos es algebraicamente cerrado; es decir, todo polinomio no constante en* $\mathbb{C}[x]$ *tiene una raíz en*$\mathbb{C}$.

Demostración. Supongamos que E es una extensión propia finita de los números complejos. Como toda extensión finita de un cuerpo de característica cero es una extensión simple, existe $\alpha \in E$ tal que $E = \mathbb{C}(\alpha)$ con α la raíz de un polinomio irreducible $f(x)$ en $\mathbb{C}[x]$. El cuerpo de descomposición L de $f(x)$ es una extensión normal finita y separable de $\mathbb{C}$ que contiene a E. Debemos mostrar que es imposible que L sea una extensión propia de $\mathbb{C}$.

Supongamos que L es una extensión propia de $\mathbb{C}$. Como L es el cuerpo de descomposición de $f(x)(x^2 + 1)$ sobre $\mathbb{R}$, L es una extensión normal finita y separable de $\mathbb{R}$. Sea K el cuerpo fijo de un 2-subgrupo de Sylow G de $G(L/\mathbb{R})$. Entonces $L \supset K \supset \mathbb{R}$ y $|G(L/K)| = [L : K]$. Como $[L : \mathbb{R}] = [L : K][K : \mathbb{R}]$, sabemos que $[K : \mathbb{R}]$ debe ser impar. Así, $K = \mathbb{R}(\beta)$ con β un elemento cuyo polinomio minimal $f(x)$ es de grado impar. Por lo tanto, $K = \mathbb{R}$.

Sabemos ahora que $G(L/\mathbb{R})$ debe ser un 2-grupo. Por lo tanto $G(L/\mathbb{C})$ es un 2-grupo. Hemos supuesto que $L \neq \mathbb{C}$; por lo tanto, $|G(L/\mathbb{C})| \geq 2$. Por el primer Teorema de Sylow y el Teorema Fundamental de la Teoría de Galois, existe un subgrupo G de $G(L/\mathbb{C})$ de índice 2 y un cuerpo E fijo por G. Entonces $[E : \mathbb{C}] = 2$ y existe un elemento $\gamma \in E$ con polinomio minimal $x^2 + bx + c$ en $\mathbb{C}[x]$. Este polinomio tiene raíces $(-b \pm \sqrt{b^2 - 4c})/2$ que están en $\mathbb{C}$, pues $b^2 - 4c$ está en $\mathbb{C}$. Esto es imposible; luego, $L = \mathbb{C}$. □

Si bien esta demostración es estrictamente algebraica, estuvimos forzados a usar resultados de Cálculo. Es necesario suponer el axioma del Supremo para demostrar que todo polinomio de grado impar tiene una raíz real y que todo número real positivo tiene una raíz cuadrada. Pareciera que no hay forma de evitar esta dificultad para hacer un argumento puramente algebraico. Es bastante impresionante que haya varias demostraciones elegantes del Teorema Fundamental del Álgebra que usan análisis complejo. También es importante notar que podemos obtener una demostración de un teorema tan importante como este desde dos áreas muy diferentes de las matemáticas.

Sage Cuerpos, extensiones de cuerpos, raíces de polinomios, y teoría de grupos — Sage lo tiene todo, así que es posible estudiar en detalle ejemplos muy complicados de la teoría de Galois con Sage.

23.4 Ejercicios

1. Obtenga cada uno de los siguientes grupos de Galois. ¿Cuáles de las siguientes extension de cuerpos son extensiones normales? Si la extensión no es normal, encuentre una extensión normal $\mathbb{Q}$ en la que esté contenida.

(a) $G(\mathbb{Q}(\sqrt{30})/\mathbb{Q})$
(b) $G(\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q})$
(c) $G(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$
(d) $G(\mathbb{Q}(\sqrt{2},\sqrt[3]{2},i)/\mathbb{Q})$
(e) $G(\mathbb{Q}(\sqrt{6},i)/\mathbb{Q})$

2. Determine la separabilidad de cada uno de los siguientes polinomios.

(a) x^3+2x^2-x-2 sobre $\mathbb{Q}$
(b) x^4+2x^2+1 sobre $\mathbb{Q}$
(c) x^4+x^2+1 sobre $\mathbb{Z}_3$
(d) x^3+x^2+1 sobre $\mathbb{Z}_2$

3. Indique el orden y describa un generador del grupo de Galois de GF(729) sobre GF(9).

4. Obtenga los grupos de Galois de cada uno de los siguientes polinomios en $\mathbb{Q}[x]$; determine la solubilidad por radicales de cada uno de los polinomios.

(a) x^5-12x^2+2
(b) x^5-4x^4+2x+2
(c) x^3-5
(d) x^4-x^2-6
(e) x^5+1
(f) $(x^2-2)(x^2+2)$
(g) x^8-1
(h) x^8+1
(i) x^4-3x^2-10

5. Encuentre un elemento primitivo en el cuerpo de descomposición de cada uno de los siguientes polinomios en $\mathbb{Q}[x]$.

(a) x^4-1
(b) x^4-8x^2+15
(c) x^4-2x^2-15
(d) x^3-2

6. Demuestre que el grupo de Galois de un polinomio cuadrático irreducible es isomorfo a $\mathbb{Z}_2$.

7. Demuestre que el grupo de Galois de un polinomio cúbico irreducible es isomorfo a S_3 o a $\mathbb{Z}_3$.

8. Sean $F \subset K \subset E$ cuerpos. Si E es una extensión normal de F, muestre que E también es una extensión normal de K.

9. Sea G el grupo de Galois de un polinomio de grado n. Demuestre que $|G|$ divide a $n!$.

10. Sea $F \subset E$. Si $f(x)$ es soluble sobre F, muestre que $f(x)$ también es soluble sobre E.

11. Construya un polinomio $f(x)$ en $\mathbb{Q}[x]$ de grado 7 que no sea soluble por radicales.

12. Sea p un número primo. Demuestre que existe un polinomio $f(x) \in \mathbb{Q}[x]$ de grado p con grupo de Galois isomorfo a S_p. Concluya que para todo primo p con $p \geq 5$ existe un polinomio de grado p que no es soluble por radicales.

13. Sea p un número primo y sea $\mathbb{Z}_p(t)$ el cuerpo de funciones racionales sobre $\mathbb{Z}_p$. Demuestre que $f(x) = x^p - t$ es un polinomio irreducible en $\mathbb{Z}_p(t)[x]$. Muestre que $f(x)$ no es separable.

14. Sea E una extensión de cuerpos de F. Supongamos que K y L son dos cuerpos intermedios. Si existe un elemento $\sigma \in G(E/F)$ tal que $\sigma(K) = L$, entonces K y L se llaman ***cuerpos conjugados.*** Demuestre que K y L son conjugados si y solo si $G(E/K)$ y $G(E/L)$ son subgrupos conjugados de $G(E/F)$.

15. Sea $\sigma \in \text{Aut}(\mathbb{R})$. Si a es un número real positivo, muestre que $\sigma(a) > 0$.

16. Sea K el cuerpo de descomposición de $x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$. Demuestre o refute que K es una extensión por radicales.

17. Sea F un cuerpo tal que $\text{char}\, F \neq 2$. Demuestre que el cuerpo de descomposición de $f(x) = ax^2 + bx + c$ es $F(\sqrt{\alpha}\,)$, donde $\alpha = b^2 - 4ac$.

18. Demuestre o refute: Dos subgrupos diferentes de un grupo de Galois tienen cuerpos fijos diferentes.

19. Sea K el cuerpo de descomposición de un polinomio sobre F. Si E es una extensión de cuerpos de F contenida en K y $[E : F] = 2$, entonces E es el cuerpo de descomposición de algún polinomio en $F[x]$.

20. Sabemos que el polinomio ciclotómico

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

es irreducible sobre $\mathbb{Q}$ para cada primo p. Sea ω un cero de $\Phi_p(x)$, y consideremos el cuerpo $\mathbb{Q}(\omega)$.

(a) Muestre que $\omega, \omega^2, \ldots, \omega^{p-1}$ son raíces distintas de $\Phi_p(x)$, y concluya que son todas las raíces de $\Phi_p(x)$.

(b) Muestre que $G(\mathbb{Q}(\omega)/\mathbb{Q})$ es abeliano de orden $p - 1$.

(c) Muestre que el cuerpo fijo de $G(\mathbb{Q}(\omega)/\mathbb{Q})$ es $\mathbb{Q}$.

21. Sea F un cuerpo finito o un cuerpo de característica cero. Sea E una extensión normal finita de F con grupo de Galois $G(E/F)$. Demuestre que $F \subset K \subset L \subset E$ si y solo si $\{\text{id}\} \subset G(E/L) \subset G(E/K) \subset G(E/F)$.

22. Sea F un cuerpo de característica cero y sea $f(x) \in F[x]$ un polinomio separable de grado n. Si E es el cuerpo de descomposición de $f(x)$, sean $\alpha_1, \ldots, \alpha_n$ las raíces de $f(x)$ en E. Sea $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$. Definimos el ***discriminante*** de $f(x)$ como Δ^2.

(a) Si $f(x) = x^2 + bx + c$, muestre que $\Delta^2 = b^2 - 4c$.

(b) Si $f(x) = x^3 + px + q$, muestre que $\Delta^2 = -4p^3 - 27q^2$.

(c) Demuestre que Δ^2 está en F.

(d) Si $\sigma \in G(E/F)$ es una transposición de dos raíces de $f(x)$, muestre que $\sigma(\Delta) = -\Delta$.

(e) Si $\sigma \in G(E/F)$ es una permutación par de las raíces de $f(x)$, muestre que $\sigma(\Delta) = \Delta$.

(f) Demuestre que $G(E/F)$ es isomorfo a un subgrupo de A_n si y solo si $\Delta \in F$.

(g) Determine el grupo de Galois de $x^3 + 2x - 4$ y $x^3 + x - 3$.

23.5 Referencias y Lecturas Recomendadas

[1] Artin, E. *Theory: Lectures Delivered at the University of Notre Dame (Notre Dame Mathematical Lectures, Number 2)*. Dover, Mineola, NY, 1997.

[2] Edwards, H. M. *Galois Theory*. Springer-Verlag, New York, 1984.

[3] Fraleigh, J. B. *A First Course in Abstract Algebra*. 7th ed. Pearson, Upper Saddle River, NJ, 2003.

[4] Gaal, L. *Classical Galois Theory with Examples*. American Mathematical Society, Providence, 1979.

[5] Garling, D. J. H. *A Course in Galois Theory*. Cambridge University Press, Cambridge, 1986.

[6] Kaplansky, I. *Fields y Rings*. 2nd ed. University of Chicago Press, Chicago, 1972.

[7] Rothman, T. "The Short Life of Évariste Galois," *Scientific American*, April 1982, 136–49.

23.6 Sage

Nuestra capacidad de examinar cuerpos con Sage nos permitirá estudiar los principales conceptos de la Teoría de Galois con facilidad. Examinaremos rigurosamente el Ejemplo 7 usando las herramientas computacionales a nuestra disposición.

Grupos de Galois

Repetiremos el Ejemplo 23.24 y analizaremos cuidadosamente el cuerpo de descomposición del polinomio $p(x) = x^4 - 2$. Comenzamos con un cuerpo de extención inicial que contenga al menos una raíz.

```
x = polygen(QQ, 'x')
N.<a> = NumberField(x^4 - 2); N
```

```
Number Field in a with defining polynomial x^4 - 2
```

El método `.galois_closure()` crea una extensión que contiene todas las raíces del polinomio usado para definir el cuerpo de números.

```
L.<b> = N.galois_closure(); L
```

```
Number Field in b with defining polynomial x^8 + 28*x^4 + 2500
```

```
L.degree()
```

```
8
```

```
y = polygen(L, 'y')
(y^4 - 2).factor()
```

```
(y - 1/120*b^5 -  19/60*b) *
(y - 1/240*b^5 + 41/120*b) *
(y + 1/240*b^5 - 41/120*b) *
(y + 1/120*b^5 +  19/60*b)
```

De la factorización, es claro que L es el cuerpo de descomposición del polinomio, si bien la factorización no es linda. Es fácil entonces obtener el grupo de Galois de esta extensión de cuerpos.

```
G = L.galois_group(); G
```

```
Galois group of Number Field in b with
defining polynomial x^8 + 28*x^4 + 2500
```

Podemos examinar e identificar este grupo. Note que como el cuerpo es una extensión de grado 8, el grupo se describe como un grupo de permutaciones en 8 símbolos. (Es solo una coincidencia que el grupo tiene 8 elementos.) Dada la escasez de grupos no abelianos de orden 8, no es difícil descubrir la naturaleza de este grupo.

```
G.is_abelian()
```

```
False
```

```
G.order()
```

```
8
```

```
G.list()
```

```
[(), (1,2,8,7)(3,4,6,5),
(1,3)(2,5)(4,7)(6,8), (1,4)(2,3)(5,8)(6,7),
(1,5)(2,6)(3,7)(4,8), (1,6)(2,4)(3,8)(5,7),
(1,7,8,2)(3,5,6,4), (1,8)(2,7)(3,6)(4,5)]
```

```
G.is_isomorphic(DihedralGroup(4))
```

```
True
```

Ahí está. Pero puede no ser muy satisfactorio. Veamos en mayor profundidad para entender mejor. Empezaremos del principio y crearemos el cuerpo de descomposición de $p(x) = x^4 - 2$ nuevamente, pero la principal diferencia es que las raíces serán extremadamente obvias de manera que podamos trabajar más cuidadosamente con el grupo de Galois y los cuerpos fijos. En el camino, veremos otro ejemplo donde el álgebra lineal nos permite ciertos cálculos. La siguiente construcción debiese resultar familiar a esta altura.

```
x = polygen(QQ, 'x')
p = x^4 - 2
N.<a> = NumberField(p); N
```

```
Number Field in a with defining polynomial x^4 - 2
```

```
y = polygen(N, 'y')
p = p.subs(x=y)
p.factor()
```

```
(y - a) * (y + a) * (y^2 + a^2)
```

```
M.<b> = NumberField(y^2 + a^2); M
```

```
Number Field in b with defining polynomial y^2 + a^2 over
its base field
```

```
z = polygen(M, 'z')
(z^4 - 2).factor()
```

```
(z - b) * (z - a) * (z + a) * (z + b)
```

Lo que debemos notar acá es que hemos organizado el cuerpo de descomposición de manera de que las cuatro raíces, `a, -a, b, -b`, son funciones muy sencillas en términos de los generadores. En una notación más tradicional, `a` es $2^{\frac{1}{4}} = \sqrt[4]{2}$, y `b` es $2^{\frac{1}{4}}i = \sqrt[4]{2}i$ (o sus negativos).

Veremos que es más sencillo realizar cálculos en la torre aplanada, una construcción ya familiar.

```
L.<c> = M.absolute_field(); L
```

```
Number Field in c with defining polynomial x^8 + 28*x^4 + 2500
```

```
fromL, toL = L.structure()
```

Podemos volver a nuestro polinomio original (sobre los racionales), y preguntar por sus raíces en la torre aplanada, diseñada a la medida para contener estas raíces.

```
roots = p.roots(ring=L, multiplicities=False); roots
```

```
[1/120*c^5 +  19/60*c,
 1/240*c^5 - 41/120*c,
-1/240*c^5 + 41/120*c,
-1/120*c^5 -  19/60*c]
```

Hmmm. ¿Se ven correctas? Si volvemos a la factorización obtenida en el cuerpo construído con el método `.galois_closure()`, se ven bien. Pero podemos mejorarlas.

```
[fromL(r) for r in roots]
```

```
[b, a, -a, -b]
```

Sí, esas son las raíces.

El comando `End()` creará el grupo de automorfismos del cuerpo `L`.

```
G = End(L); G
```

```
Automorphism group of Number Field in c with
defining polynomial x^8 + 28*x^4 + 2500
```

Podemos verificar que cada uno de estos automorfismos fija los números racionales. Si un homomorfismo de cuerpos fija el 1, entonces fija los enteros, y por ende fija todas las fracciones de enteros.

```
[tau(1) for tau in G]
```

```
[1, 1, 1, 1, 1, 1, 1, 1]
```

Así, cada elemento de `G` fija los números racionales y por ende `G` es el grupo de Galois del cuerpo de descomposición `L` sobre los racionales.

La Proposición 23.5 es fundamental. Dice que todo automorfismo en el grupo de Galois de un cuerpo de extensión induce una permutación de las raíces de un polinomio con coeficientes en el cuerpo base. Tenemos acá todos estos ingredientes. Evaluaremos cada automorfismo del grupo de Galois en cada una de las cuatro raíces de nuestro polinomio, que en cada caso debiera ser otra raíz. (Usamos el constructor `Sequence()` para obtener una salida bien diagramada.)

```
Sequence([[fromL(tau(r)) for r in roots] for tau in G],
    cr=True)
```

```
[
[b, a, -a, -b],
[-b, -a, a, b],
[a, -b, b, -a],
[b, -a, a, -b],
[-a, -b, b, a],
[a, b, -b, -a],
[-b, a, -a, b],
[-a, b, -b, a]
]
```

Cada fila de esta salida es una lista de raíces, pero permutadas, y así corresponde a una permutación de cuatro objetos (las raíces). Por ejemplo, la segunda fila muestra que el segundo automorfismo intercambia `a` con `-a`, y `b` con `-b`. (Note que la primera fila es el resultado del automorfismo identidad, de manera que podemos comparar mentalmente la primera fila con cualquier otra para imaginar la forma de "dos filas" de una permutación.) Podemos numerar las raíces, del 1 al 4, y crear cada permutacióncomo un elemento de S_4. Es más de lo que se requiere, pero podemos construir el grupo de permutaciones dejando que *todos* estos elementos generen un grupo.

```
S4 = SymmetricGroup(4)
elements = [S4([1, 2, 3, 4]),
            S4([4, 3, 2, 1]),
            S4([2, 4, 1, 3]),
            S4([1, 3, 2, 4]),
            S4([3, 4, 1, 2]),
            S4([2, 1, 4, 3]),
            S4([4, 2, 3, 1]),
            S4([3, 1, 4, 2])]
elements
```

```
[(), (1,4)(2,3), (1,2,4,3), (2,3), (1,3)(2,4),
 (1,2)(3,4), (1,4), (1,3,4,2)]
```

```
P = S4.subgroup(elements)
P.is_isomorphic(DihedralGroup(4))
```

```
True
```

Note que hemos construido un isomorfismo del grupo de Galois a un grupo de permutaciones *usando solo cuatro símbolos*, en lugar de los ocho usados previamente.

Cuerpo Fijos

En un ejercicio Sage anterior, calculamos los cuerpos fijos de automorfismos individuales para cuerpos finitos. Esto fue "fácil" en el sentido de que podíamos verificar con cada uno de los elementos en el cuerpo para ver si quedaba fijo, pues el cuerpo era finito. Ahora tenemos una extensión de cuerpos infinitos. ¿Cómo determinaremos qué elementos quedan fijos bajo un automorfismo individual, o subgrupos de automorfismos?

La respuesta es usar la estructura de espacio vectorial de la torre aplanada. Como es una extensión de grado 8 de los racionales, las primeras 8 potencias

de un elemento primitivo `c` forman una base cuando el cuerpo se ve como un espacio vectorial con los racionales como escalares. Es suficiente saber como cada automorfismo de cuerpos actúa en esta base para completamente especificar la definición del automorfismo. Esto es,

$$\begin{aligned}
\tau(x) &= \tau\left(\sum_{i=0}^{7} q_i c^i\right) && q_i \in \mathbb{Q} \\
&= \sum_{i=0}^{7} \tau(q_i)\tau(c^i) && \tau \text{ es un automorfismo de cuerpos} \\
&= \sum_{i=0}^{7} q_i \tau(c^i) && \text{los racionales quedan fijos}
\end{aligned}$$

Así podemos calcular el valor de un automorfismo de cuerpos en cualquier combinación lineal de potencias del elemento primitivo como combinación lineal de los valores del automorfismo de cuerpos solo en las potencias del elemento primitivo. Esta se conoce como "base de potencias", lo que podemos obtener simplemente con el método `.power_basis()`. Empezaremos con un ejemplo de como usar esta base. Ilustraremos con el cuarto automorfismo del grupo de Galois. Note que el método `.vector()` es conveniente en tanto transforma una combinación lineal de potencias de `c` en un vector que solo retiene los coeficientes. (Note además que τ está completamente definido por el valor de $\tau(c)$, pues como es un automorfismo de cuerpos $\tau(c^k) = (\tau(c))^k$. Sin embargo, igual debemos trabajar con la base de potencias completa para aprovechar la estructura de espacio vectorial.)

```
basis = L.power_basis(); basis
```

```
[1, c, c^2, c^3, c^4, c^5, c^6, c^7]
```

```
tau = G[3]
z = 4 + 5*c+ 6*c^3-7*c^6
tz = tau(4 + 5*c+ 6*c^3-7*c^6); tz
```

```
11/250*c^7 - 98/25*c^6 + 1/12*c^5 + 779/125*c^3 +
6006/25*c^2 - 11/6*c + 4
```

```
tz.vector()
```

```
(4, -11/6, 6006/25, 779/125, 0, 1/12, -98/25, 11/250)
```

```
tau_matrix = column_matrix([tau(be).vector() for be in
    basis])
tau_matrix
```

```
[  1        0        0         0  -28        0         0
    0]
[  0  -11/30        0         0    0  779/15         0
    0]
[  0        0  -14/25         0    0        0  -858/25
    0]
[  0        0        0  779/750    0        0         0
    -4031/375]
[  0        0        0         0   -1        0         0
    0]
```

```
[  0    1/60       0         0    0   11/30         0
    0]
[  0       0   -1/50         0    0        0    14/25
    0]
[  0       0       0  11/1500    0        0         0
    -779/750]
```

```
tau_matrix*z.vector()
```

```
(4, -11/6, 6006/25, 779/125, 0, 1/12, -98/25, 11/250)
```

```
tau_matrix*(z.vector()) == (tau(z)).vector()
```

```
True
```

La última línea expresa el hecho de que `tau_matrix` es una representación matricial del automorfismo de cuerpos, visto como transformación lineal en la estructura de espacio vectorial. En la representación de un homomorfismo de cuerpos invertible, la matriz es invertible. Para una permutación de orden 2 de las raíces, la inversa de la matriz es ella misma. Pero estos hechos son solo verificaciones de que tenemos lo que queremos, estamos interesados en otras propiedades.

Para construir cuerpos fijos, queremos encontrar los elementos que quedan fijos por automorfismos. Continuando con `tau` de arriba, buscamos elementos `z` (escritos como vectores) tales que `tau_matrix*z=z`. Estos vectores propios para el valor propio 1, o elementos del espacio nulo de `(tau_matrix - I)` (espacios nulos obtenidos con `.right_kernel()` en Sage).

```
K = (tau_matrix-identity_matrix(8)).right_kernel(); K
```

```
Vector space of degree 8 and dimension 4 over Rational Field
Basis matrix:
[    1     0     0     0     0     0     0     0]
[    0     1     0     0     0  1/38     0     0]
[    0     0     1     0     0     0 -1/22     0]
[    0     0     0     1     0     0     0 1/278]
```

Cada fila de la matriz de base es un vector que representa un elemento del cuerpo, esspecíficamente `1`, `c + (1/38)*c^5`, `c^2 - (1/22)*c^6`, `c^3 + (1/278)*c^7`. Examinemos en mayor detalle estos elementos fijos, en términos que reconozcamos.

```
fromL(1)
```

```
1
```

```
fromL(c + (1/38)*c^5)
```

```
60/19*b
```

```
fromL(c^2 - (1/22)*c^6)
```

```
150/11*a^2
```

```
fromL(c^3 + (1/278)*c^7)
```

```
1500/139*a^2*b
```

Cualquier elemento fijo por `tau` es una combinación lineal de estos cuatro elementos. Podemos ignorar los múltiplos racionales, el primer elemento está diciendo simplemente que los racionales quedan fijos, y que el último elemento es simplemente el producto de los dos del medio. Así fundamentalmente `tau` fija los racionales, `b` (que es $\sqrt[4]{2}i$) y `a^2` (que es $\sqrt{2}$). Más aún, `b^2 = -a^2` (la verificación viene a continuación), de manera que podemos crear cualquier elemento fijo por `tau` simplemente adjuntando `b`$=\sqrt[4]{2}i$ a los racionales. Así los elementos fijos por `tau` son $\mathbb{Q}(\sqrt[4]{2}i)$.

```
a^2 + b^2
```

```
0
```

Correspondencia de Galois

La estructura completa de subcuerpos de nuestro cuerpo de descomposición está determinada por la estrcutura de subgrupos del grupo de Galois (Teorema 23.22), que es isomorfo a un grupo que conocemos bien. ¿Cuáles son los subgrupos de nuestro grupo de Galois, expresados como grupos de permutaciones? (Para ser breves, solo listamos los *generadores* de cada subgrupo.)

```
sg = P.subgroups();
[H.gens() for H in sg]
```

```
[[()],
 [(2,3)],
 [(1,4)],
 [(1,4)(2,3)],
 [(1,2)(3,4)],
 [(1,3)(2,4)],
 [(2,3), (1,4)],
 [(1,2)(3,4), (1,4)(2,3)],
 [(1,3,4,2), (1,4)(2,3)],
 [(2,3), (1,2)(3,4), (1,4)]]
```

```
[H.order() for H in sg]
```

```
[1, 2, 2, 2, 2, 2, 4, 4, 4, 8]
```

`tau` arriba, es el cuarto elemento del grupo de automorfismos, y la cuarta permutación en `elements` es la permutación `(2,3)`, el generador (de orden 2) para el segundo subgrupo. Como es el único elemento no trivial de este subgrupo, sabemos que el cuerpo fijo correspondiente es $\mathbb{Q}(\sqrt[4]{2}i)$.

Analicemos otro subgrupo de orden 2, si toda la explicación, y comenzando con el subgrupo. El sexto subgrupo está generado por el quinto automorfismo, así es que determinemos los elementos que quedan fijos.

```
tau = G[4]
tau_matrix = column_matrix([tau(be).vector() for be in
    basis])
(tau_matrix-identity_matrix(8)).right_kernel()
```

```
Vector space of degree 8 and dimension 4 over Rational Field
Basis matrix:
[     1      0      0      0      0      0      0      0]
[     0      1      0      0      0  1/158      0      0]
[     0      0      1      0      0      0   1/78      0]
[     0      0      0      1      0      0      0 13/614]
```

```
fromL(tau(1))
```

```
1
```

```
fromL(tau(c+(1/158)*c^5))
```

```
120/79*b - 120/79*a
```

```
fromL(tau(c^2+(1/78)*c^6))
```

```
-200/39*a*b
```

```
fromL(tau(c^3+(13/614)*c^7))
```

```
3000/307*a^2*b + 3000/307*a^3
```

El primer elemento indica que los racionales quedan fijos (lo sabíamos). Escalando el segundo elemento nos da `b - a` como elemento fijo. Escalando el tercer y cuarto elementos fijos, reconocemos que puedens ser obtenidos a partir de potencias de `b - a`.

```
(b-a)^2
```

```
-2*a*b
```

```
(b-a)^3
```

```
2*a^2*b + 2*a^3
```

Así el cuerpo fijo de este subgrupo puede ser formado adjuntando `b - a` a los racionales, lo que en notación matemática es $\sqrt[4]{2}i - \sqrt[4]{2} = (1-i)\sqrt[4]{2}$, así el cuerpo fijo es $\mathbb{Q}(\sqrt[4]{2}i - \sqrt[4]{2}) = \mathbb{Q}((1-i)\sqrt[4]{2})$.

Podemos crear este cuerpo fijo, aunque como lo hacemos acá no es estrictamente un subcuerpo de `L`. Usaremos una expresión para `b - a` que es una combinación lineal de potencias de `c`.

```
subinfo = L.subfield((79/120)*(c+(1/158)*c^5)); subinfo
```

```
(Number Field in c0 with defining polynomial x^4 + 8, Ring
    morphism:
  From: Number Field in c0 with defining polynomial x^4 + 8
  To:   Number Field in c with defining polynomial x^8 +
      28*x^4 + 2500
  Defn: c0 |--> 1/240*c^5 + 79/120*c)
```

El método `.subfield()` entrega un par. El primer ítem es un nuevo cuerpo de números, isomorfo a un subcuerpo de `L`. El segundo ítem es una función inyectiva desde el nuevo cuerpo de números a `L`. En este caso, la imagen del elemento primitivo `c0` es el elemento que hemos especificado como generador del subcuerpo. El elemento primitivo del nuevo cuerpo satisface el polinomio $x^4 + 8$ — puede verificar que $(1-i)\sqrt[4]{2}$ es de hecho una raíz del polinomio $x^4 + 8$.

Existen cuatro subgrupos de orden 2, hemos encontrado cuerpos fijos para dos de ellos. Los otros tres son similares, y sería un buen ejercicio obtenerlos. Nuestro grupo de automorfismos tiene tres subgrupos de orden 4, y al menos uno de cada tipo posible (cíclico versus no cíclico). Cuerpos fijos de subgrupos de mayor tamaño requieren encontrar elementos del cuerpo que queden fijos

por todos los automorfismos en el subgrupo. (Convenientemente ignoramos el automorfismo identidad arriba.) Esto va a requerir myores cálculos, pero restringirá las posibilidades (cuerpos menores) al punto de que será más fácil determinar un elemento primitivo para cada uno de los cuerpos.

El séptimo subgrupo es generado por dos elementos de orden 2 y se compone completamente de elementos de orden 2 (exceptuando la identidad), así que es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Las permutaciones corresponden a los automorfismos número 0, 1, 3, y 6. Para determinar el elemento fijo por *los cuatro* automorfismos, construiremos el núcleo de cada uno y a medida que avanzamos, formamos la *intersección* de los cuatro núcleos. Usaremos un bucle sobre los cuatro automorfismos.

```
V = QQ^8
for tau in [G[0], G[1], G[3], G[6]]:
  tau_matrix = column_matrix([tau(be).vector() for be in
      basis])
  K = (tau_matrix-identity_matrix(8)).right_kernel()
  V = V.intersection(K)
V
```

```
Vector space of degree 8 and dimension 2 over Rational Field
Basis matrix:
[    1     0     0     0     0     0     0     0]
[    0     0     1     0     0     0 -1/22     0]
```

Fuera de los racionales, hay un único elemento fijo.

```
fromL(tau(c^2 - (1/22)*c^6))
```

```
150/11*a^2
```

Removiendo un múltiplo escalar, nuestro elemento primitivo es `a^2`, que matemáticamente es $\sqrt{2}$, así el cuerpo fijo es $\mathbb{Q}(\sqrt{2})$. Nuevamente, podemos construir este cuerpo fijo, pero ignorando la función.

```
F, mapping = L.subfield((11/150)*(c^2 - (1/22)*c^6))
F
```

```
Number Field in c0 with defining polynomial x^2 - 2
```

Un subgrupo más. El penúltimo subgrupo tiene una permutación de orden 4 como generador, así es que es un grupo cíclico de orden 4. Las permutaciones individuales del subgrupo corresponden a automorfismos de 0, 1, 2, 7.

```
V = QQ^8
for tau in [G[0], G[1], G[2], G[7]]:
  tau_matrix = column_matrix([tau(be).vector() for be in
      basis])
  K = (tau_matrix-identity_matrix(8)).right_kernel()
  V = V.intersection(K)
V
```

```
Vector space of degree 8 and dimension 2 over Rational Field
Basis matrix:
[1 0 0 0 0 0 0 0]
[0 0 0 0 1 0 0 0]
```

Así podemos calcular el elemento primitivo.

```
fromL(tau(c^4))
```

```
-24*a^3*b - 14
```

Como los racionales quedan fijos, podemos sacar el -14 y el múltiplo y tomar `a^3*b` como el elemento primitivo. Matemáticamente, esto es $2i$, así que podemos usar simplemente i como elemento primitivo y el cuerpo fijo es $\mathbb{Q}(i)$. Podemos entonces construir el cuerpo fijo (e ignorar la función que obtuvimos además).

```
F, mapping = L.subfield((c^4+14)/-48)
F
```

```
Number Field in c0 with defining polynomial x^2 + 1
```

Hay un subgrupo más de orden 4, cuyo análisi dejaremos como ejercicio. Hay además dos subgrupos triviales (la identidad y el grupo completo) que no son muy interesantes ni sorprendentes.

Si lo de arriba le parece mucho trabajo, puede siempre dejar que Sage lo haga todo con el método `.subfields()`.

```
L.subfields()
```

```
[
(Number Field in c0 with defining polynomial x,
 Ring morphism:
   From: Number Field in c0 with defining polynomial x
   To:   Number Field in c with defining polynomial x^8 +
       28*x^4 + 2500
   Defn: 0 |--> 0,
 None),
(Number Field in c1 with defining polynomial x^2 + 112*x +
    40000,
 Ring morphism:
   From: Number Field in c1 with defining polynomial x^2 +
       112*x + 40000
   To:   Number Field in c with defining polynomial x^8 +
       28*x^4 + 2500
   Defn: c1 |--> 4*c^4,
 None),
(Number Field in c2 with defining polynomial x^2 + 512,
 Ring morphism:
   From: Number Field in c2 with defining polynomial x^2 + 512
   To:   Number Field in c with defining polynomial x^8 +
       28*x^4 + 2500
   Defn: c2 |--> 1/25*c^6 + 78/25*c^2,
 None),
(Number Field in c3 with defining polynomial x^2 - 288,
 Ring morphism:
   From: Number Field in c3 with defining polynomial x^2 - 288
   To:   Number Field in c with defining polynomial x^8 +
       28*x^4 + 2500
   Defn: c3 |--> -1/25*c^6 + 22/25*c^2,
 None),
(Number Field in c4 with defining polynomial x^4 + 112*x^2 +
    40000,
 Ring morphism:
   From: Number Field in c4 with defining polynomial x^4 +
       112*x^2 + 40000
   To:   Number Field in c with defining polynomial x^8 +
       28*x^4 + 2500
   Defn: c4 |--> 2*c^2,
```

```
 None),
(Number Field in c5 with defining polynomial x^4 + 648,
 Ring morphism:
   From: Number Field in c5 with defining polynomial x^4 + 648
   To:   Number Field in c with defining polynomial x^8 +
       28*x^4 + 2500
   Defn: c5 |--> 1/80*c^5 + 79/40*c,
 None),
(Number Field in c6 with defining polynomial x^4 + 8,
Ring morphism:
  From: Number Field in c6 with defining polynomial x^4 + 8
  To:   Number Field in c with defining polynomial x^8 +
      28*x^4 + 2500
  Defn: c6 |--> -1/80*c^5 + 1/40*c,
  None),
(Number Field in c7 with defining polynomial x^4 - 512,
 Ring morphism:
   From: Number Field in c7 with defining polynomial x^4 - 512
   To:   Number Field in c with defining polynomial x^8 +
       28*x^4 + 2500
   Defn: c7 |--> -1/60*c^5 + 41/30*c,
 None),
(Number Field in c8 with defining polynomial x^4 - 32,
 Ring morphism:
   From: Number Field in c8 with defining polynomial x^4 - 32
   To:   Number Field in c with defining polynomial x^8 +
       28*x^4 + 2500
   Defn: c8 |--> 1/60*c^5 + 19/30*c,
 None),
(Number Field in c9 with defining polynomial x^8 + 28*x^4 +
    2500,
 Ring morphism:
   From: Number Field in c9 with defining polynomial x^8 +
       28*x^4 + 2500
   To:   Number Field in c with defining polynomial x^8 +
       28*x^4 + 2500
   Defn: c9 |--> c,
 Ring morphism:
   From: Number Field in c with defining polynomial x^8 +
       28*x^4 + 2500
   To:   Number Field in c9 with defining polynomial x^8 +
       28*x^4 + 2500
   Defn: c |--> c9)
]
```

Se describen diez subcuerpos, que es lo que esperábamos, dados los 10 subgrupos del grupo de Galois. Cada uno empieza con un cuerpo de número que es un subcuerpo. Técnicamente, cada uno no es un subconjunto de `L`, pero el segundo ítem devuelto para cada subcuerpo es un homomorfismo inyectivo, también conocido como una "incrustación." Cada incrustación describe cómo un elemento primitivo del subcuerpo se traduce a un elemento de `L`. Algunos de estos elementos primitivos podrían ser manipulados (como hicimos arriba) para darnos polinomios minimales más simples, pero los resultados son bastante impresionantes de todas formas. Cada ítem en la lista tiene una tercera componente, que es casi siempre `None`, excepto cuando el subcuerpo es el cuerpo completo, y ahí la tercera componente es un homomorfismo inyectivo "en la otra dirección."

Exensiones Normales

Considere el tercer subgrupo en la lista arriba, generado por la permutación `(1,4)`. Como subgrupo de orden 2, tiene solo un elemento no trivial, que acá corresponde con el séptimo automorfismo. Determinamos los elementos fijos como antes.

```
tau = G[6]
tau_matrix = column_matrix([tau(be).vector() for be in
    basis])
(tau_matrix-identity_matrix(8)).right_kernel()
```

```
Vector space of degree 8 and dimension 4 over Rational Field
Basis matrix:
[    1     0     0     0     0     0     0     0]
[    0     1     0     0     0 -1/82     0     0]
[    0     0     1     0     0     0 -1/22     0]
[    0     0     0     1     0     0     0 11/58]
```

```
fromL(tau(1))
```

```
1
```

```
fromL(tau(c+(-1/82)*c^5))
```

```
-120/41*a
```

```
fromL(tau(c^2+(-1/22)*c^6))
```

```
150/11*a^2
```

```
fromL(tau(c^3+(11/58)*c^7))
```

```
3000/29*a^3
```

Como siempre, ignorando múltiplos racionales, vemos potencias de `a` y reconocemos que `a` es un elemento primitivo para el cuerpo fijo, que es por lo tanto $\mathbb{Q}(\sqrt[4]{2})$. Reconozcamos que `a` era nuestra primera raíz de $x^4 - 2$, y fue usada para crear la primera parte de nuestra torre original, `N`. Así `N` es tanto $\mathbb{Q}(\sqrt[4]{2})$ como el cuerpo fijo de $H = \langle (1,4) \rangle$.

$\mathbb{Q}(\sqrt[4]{2})$ contiene al menos una raíz del polinomio irreducible $x^4 - 2$, pero no todas las raíces (atestigua la factorización de arriba) y por lo tanto no califica como extensión normal. Por la parte (4) del Teorema 23.22 el grupo de automorfismos de la extensión no es normal en el grupo de Galois completo.

```
sg[2].is_normal(P)
```

```
False
```

Como se esperaba.

23.7 Ejercicios en Sage

1. En el análisis del Ejemplo 23.24 con Sage, hubo dos subgrupos de orden 2 y un subgrupo de orden 4 que no fueron analizados. Determine los cuerpos fijos de estos tres subgrupos.

2. Construya el cuerpo de descomposición de $p(x) = x^3-6x^2+12x-10$ y determine el grupo de Galois de $p(x)$ como un grupo concreto de permutaciones explícitas. Construya el reticulado de subgrupos del grupo de Galois, nuevamente usando las mismas permutacione explícitas. Use el Teorema Fundamental de la Teoría de Galois, construya los subcuerpos del cuerpo de descomposición. Incluya la documentación de respaldo necesaria en su entrega. Además, entregue una componente escrita de esta tarea que contenga un despliegue completo de los subgrupos y subcuerpos, escritos enteramente con notación matemática y sin comando Sage, diseñado para ilustrar la correspondencia entre los dos. Todo lo que necesita acá es el despliegue gráfico, apropiadamente etiquetado — el trabajo hecho en Sage constituye el respaldo de su trabajo.

3. El polinomio $x^5 - x - 1$ tiene todo el grupo simétrico S_5 como su grupo de Galois. Como S_5 es no soluble, sabemos que este polinomio es un ejemplo de un polinomio quíntico que no es soluble por radicales. Desafortunadamente, pedirle a Sage que calcule este grupo de Galois toma demasiado tiempo. Así este ejercicio simulará esa experiencia con un ejemplo ligeramente más pequeño. Considere el polinomio $p(x) = x^4 + x + 1$.

(a) Construya el cuerpo de descomposición de $p(x)$ una raíz a la vez. Cree una extensión, fatorice allí, descarte factores lineales, use los restantes factores irreducibles para extender una vez más. Repita hasta que $p(x)$ se factorice completamente. Asegúrese de hacer una extensión final usando solo un factor lineal. Esto es un poco tonto, y Sage parecerá ignorar el último generador (de manera que querrá determinar a qué equivale en términos de los generadores previos). Las direcciones que siguen dependen de tomar este paso adicional.

(b) Factorice el polinomio original sobre la extensión final en la torre. ¿Qué es aburrido de esta factorización en relación a otros ejemplos que hemos hecho?

(c) Construya la torre completa como un cuerpo de números absoluto sobre $\mathbb{Q}$. Del grado de esta extensión y del grado del polinomio original, infiera el grupo de Galois de este polinomio.

(d) Usando las funciones que permiten taducir entre la torre y el cuerpo de números absoluto (obtenido del método `.structure()`), elija una de las raíces (cualquiera) y exprésela en términos del único generador del cuerpo absoluto. Después invierta el procedimiento y exprese el generador del cuerpo absoluto en términos de las raíces en la torre.

(e) Calcule el grupo de automorfismos del cuerpo absoluto (sin mostrar el grupo en lo que entregue). Tome las cuatro raíces (incluyendo la tonta del último paso de la construcción de la torre) y aplique cada automorfismo de cuerpos a las cuatro raíces (formando la permutaciones garantizadas de las raíces). Comente sobre lo que observa.

(f) Hay un automorfismo no trivial que tiene una forma especialmente simple (es el segundo para mí) cuando es aplicado al generador del cuerpo absoluto. ¿Qué le hace este automorfismo a las raíces de $p(x)$?

(g) Considere la extensión de $\mathbb{Q}$ formada al adjuntar una sola de las raíces. Este es un subcuerpo del cuerpo de descomposición del polinomio, de manera que es el cuerpo fijo por un subgrupo del grupo de Galois. Dé una descripción simple del subgrupo correspondientesusando el lenguaje que típicamente solo aplicamos a grupos de permutaciones.

4. Vuelva al cuerpo de descomposición de la quíntica discutida en la introcucción al problema anterior (x^5-x-1). Cree los primeros dos cuerpos intermedios

adjuntando dos raíces (de a una). Pero en lugar de factorizar en cada paso para obtener un nuevo polinomio irreducible, *divida* por el factor lineal que *sabe* que es un factor. En general, el cociente puede que se siga factorizando, pero en este ejercicio presuponga que no es así. En otras palabras, haga como si el cociente por el factor lineal fuera irreducible. Si no lo fuera, el comando `NumberField()` debiera reclamar (lo que no hará).
Después de adjuntar las dos raíces, cree una extensión produciendo una tercera raíz, y haga la división. Ahora debiera tener un factor cuadrático. Suponiendo que este polinomio cuadrático es irreducible (lo es) argumente que tiene suficiente evidencia para determinar el orden del grupo de Galois, y por ende puede determinar *exactamente* qué grupo es.
Puede intentar usar este factor cuadrático para crear un paso más en las extensiones, y llegará al cuerpo de descomposición, como se ver por lógica o por división. Sin embargo, esto puede tomarle un tiempo largo a Sage (¡guarde su trabajo antes!). Puede intentar con el argumento opcional `check=False` en el comando `NumberField()`— esto evitará la verificación de irreducibilidad.

5. Cree el cuerpo finito de orden 3^6, dejando que Sage entregue el polinomio por defecto para su construcción. El polinomio $x^6 + x^2 + 2x + 1$ es irreducible sobre el cuerpo de 3 elementos. Verifique que este polinomio se descompone en el cuerpo finito construido, y use el método `.roots()` para recolectar sus raíces. Obtenga el grupo de automorfismos del cuerpo con el comando `End()`.
Con esto tiene todas las piezas para asociar a cada automorfismo de cuerpos con una permutación de las raíces. De esto, identifique el grupo de Galois y todos sus subgrupos. Para cada subgrupo, determine el cuerpo que queda fijo. Puede encontrar que es más fácil trabajar con las raíces si usa el método `.log()` para identificarlas como potencias del generador multiplicativo del cuerpo.
Su grupo de Galois en este ejemplo será abeliano. Por ello todo subgrupo es normal, y por lo tanto toda extensión también es normal. ¿Puede extender este ejemplo escogiendo un cuerpo intermedio con un polinomio no trivial irreducible que tenga todas sus raíces en el cuerpo intermedio y con un polinomio no trivial irreducible que no tenga raíces en el cuerpo intermedio?
Sus resultados acá son "típicos" en el sentido de que el cuerpo o el polinomio irreducible particular no hacen gran diferencia en la naturaleza cualitativa de los resultados.

6. El cuerpo de descomposición del polinomio irreducible $p(x) = x^7 - 7x + 3$ tiene grado 168 (de manera que este es el orden de su grupo de Galois). Este polinomio se deriva de una "curva trinomial de Elkies," una curva hiperelíptica (abajo) que produce polinomios con grupos de Galois interesantes:

$$y^2 = x(81x^5 + 396x^4 + 738x^3 + 660x^2 + 269x + 48)$$

Para $p(x)$ el grupo de Galois resultante es $PSL(2, 7)$, un grupo simple. Si $SL(2, 7)$ consiste de todas las matrices de 2×2 sobre $\mathbb{Z}_7$ con determinante 1, entonces $PSL(2, 7)$ es el cociente por el subgrupo $\{I_2, -I_2\}$. Es el segundo grupo simple no abeliano (después de A_5).
Vea qué tan lejos puede llegar con Sage construyendo este cuerpo de descomposición. Una extensión de grado 7 entregará un factor lineal, y una extensión siguiente de grado 6 entregará dos factores lineales más, dejando un factor de grado cuatro. Es en este punto donde los cálculo empiezan a hacerse lentos. Si aceptamos que el cuerpo de descomposición tiene grado 168, entonces sabemos que agregando una raíz de este factor de grado cuatro nos llevará hasta el cuerpo de descomposición. Crear esta extensión puede que sea posible computacionalmente, pero verificar que el polinomio cuártico se descompone en factores lineales acá, parace ser impracticable.

7. Volvamos al Ejemplo 23.24, y la lista completa de subcuerpo obtenible del método `.subfields()` aplicado a la torre aplanada. Como mencionamos, estos no son técnicamente subcuerpos, pero tienen incrustaciones a la torre. Dados dos subcuerpos, sus respectivos elementos primitivos son incrustados en la torre, con una imagen que es combinación lineal de potencias del elemento primitivo para la torre.
Si uno de lus subcuerpos está contenido en otro, entonces la imagen del elemento primitivo para el cuerpo menor debería ser combinación lneal de potencias (apropiadas) de la imagen del elemento primitivo para el cuepo mayor. Este es un cálculo de álgebra lineal que debiese ser posible en la torre, relativo a la base de potencias de la torre completa.
Escriba un procedimiento para determinar si dos subcuerpos están relacionados por inclusión, es decir si uno es subconjunto del otro. Use este procedimiento para crear el reticulado de subcuerpos. El objetivo final sería una imagen gráfica del reticulado, usando los procedimientos gráficos disponibles para reticulados, similar a la mitad superior de la Figura 23.25. Este es un ejercicio "desafiante", lo que quiere decir que "es especulativo y no ha sido probado."

A

GNU Free Documentation License

Version 1.3, 3 November 2008

0. PREAMBLE The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or

authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers

may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You

may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties — for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS A compilation of the Document or its derivatives with other separate and independent

documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If

the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING "Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright (C)  YEAR  YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with... Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

B

Pistas y Soluciones a Ejercicios Seleccionados

1.3 Ejercicios

1. (a) $A \cap B = \{2\}$; (b) $B \cap C = \{5\}$.

2. (a) $A \times B = \{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3),(c,1),(c,2),(c,3)\}$; (d) $A \times D = \emptyset$.

6. Si $x \in A \cup (B \cap C)$, entonces ya sea $x \in A$ o $x \in B \cap C$. Luego, $x \in A \cup B$ y $A \cup C$. Así, $x \in (A \cup B) \cap (A \cup C)$. Por lo tanto, $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$. Recíprocamente, si $x \in (A \cup B) \cap (A \cup C)$, entonces $x \in A \cup B$ y $A \cup C$. Luego, $x \in A$ o x está tanto en B como en C. Así $x \in A \cup (B \cap C)$ y por lo tanto $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$. Luego, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

10. $(A \cap B) \cup (A \setminus B) \cup (B \setminus A) = (A \cap B) \cup (A \cap B') \cup (B \cap A') = [A \cap (B \cup B')] \cup (B \cap A') = A \cup (B \cap A') = (A \cup B) \cap (A \cup A') = A \cup B$.

14. $A \setminus (B \cup C) = A \cap (B \cup C)' = (A \cap A) \cap (B' \cap C') = (A \cap B') \cap (A \cap C') = (A \setminus B) \cap (A \setminus C)$.

17. (a) No es función pues $f(2/3)$ no está definido; (b) es una función; (c) no es función, pues $f(1/2) = 3/4$ pero $f(2/4) = 3/8$; (d) es una función.

18. (a) f es 1-1 pero no es sobre. $f(\mathbb{R}) = \{x \in \mathbb{R} : x > 0\}$. (c) f no es 1-1 ni es sobre. $f(\mathbb{R}) = \{x : -1 \leq x \leq 1\}$.

20. (a) $f(n) = n + 1$.

22. (a) Sean $x, y \in A$. Entonces $g(f(x)) = (g \circ f)(x) = (g \circ f)(y) = g(f(y))$. Luego, $f(x) = f(y)$ y $x = y$, so $g \circ f$ es 1-1. (b) Sea $c \in C$, entonces $c = (g \circ f)(x) = g(f(x))$ para algún $x \in A$. Como $f(x) \in B$, g es sobre.

23. $f^{-1}(x) = (x+1)/(x-1)$.

24. (a) Sea $y \in f(A_1 \cup A_2)$. Entonces existe $x \in A_1 \cup A_2$ tal que $f(x) = y$. Luego, $y \in f(A_1)$ o $f(A_2)$. Por lo tanto, $y \in f(A_1) \cup f(A_2)$. Así, $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$. Recíprocamente, si $y \in f(A_1) \cup f(A_2)$, entonces $y \in f(A_1)$ o $f(A_2)$. Luego, existe x en A_1 o A_2 tal que $f(x) = y$. Entonces existe $x \in A_1 \cup A_2$ tal que $f(x) = y$. Por lo tanto, $f(A_1) \cup f(A_2) \subset f(A_1 \cup A_2)$, y $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

25. (a) La relación no es simétrica. (b) La erlación no es refleja, pues 0 no es equivalente a si mismo. (c) La relación no es transitiva.

28. Sea $X = \mathbb{N} \cup \{\sqrt{2}\}$ y defina $x \sim y$ si $x + y \in \mathbb{N}$.

2.3 Ejercicios

1. El caso base, $S(1) : [1(1+1)(2(1)+1)]/6 = 1 = 1^2$ es verdadero. Supongamos que $S(k) : 1^2+2^2+\cdots+k^2 = [k(k+1)(2k+1)]/6$ es verdadero. Entonces

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= [k(k+1)(2k+1)]/6 + (k+1)^2 \\ &= [(k+1)((k+1)+1)(2(k+1)+1)]/6, \end{aligned}$$

y así $S(k+1)$ es verdadero. Luego, $S(n)$ es verdadero para todos los enteros positivos n.

3. El caso base, $S(4) : 4! = 24 > 16 = 2^4$ es verdadero. Supongamos que $S(k) : k! > 2^k$ es verdadero. Entonces $(k+1)! = k!(k+1) > 2^k \cdot 2 = 2^{k+1}$, así $S(k+1)$ es verdadero. Luego, $S(n)$ es verdadero para todos los enteros positivos n.

8. Siga la demostración el Ejemplo 2.4.

11. El caso base, $S(0) : (1+x)^0 - 1 = 0 \geq 0 = 0 \cdot x$ es verdadero. Supongamos que $S(k) : (1+x)^k - 1 \geq kx$ es verdadero. Entonces

$$\begin{aligned} (1+x)^{k+1} - 1 &= (1+x)(1+x)^k - 1 \\ &= (1+x)^k + x(1+x)^k - 1 \\ &\geq kx + x(1+x)^k \\ &\geq kx + x \\ &= (k+1)x, \end{aligned}$$

así $S(k+1)$ es verdadero. Por lo tanto, $S(n)$ es verdadero para todos los enteros positivos n.

17. Para (a) y (b) use inducción. (c) Muestre que $f_1 = 1$, $f_2 = 1$, y $f_{n+2} = f_{n+1} + f_n$. (d) Use la parte (c). (e) Use la parte (b) y el Ejercicio 2.3.16.

19. Use el Teorema Fundamental de la Aritmética.

23. Use el Principio del Buen-Orden y el algoritmo de división.

27. Como $\text{mcd}(a, b) = 1$, existen enteros r y s tales que $ar + bs = 1$. Luego, $acr + bcs = c$.

29. Todo primo es de la forma 2, 3, $6n+1$, o $6n+5$. Suponga que solo hay un número finito de primos de la forma $6k+5$.

3.4 Ejercicios

1. (a) $3 + 7\mathbb{Z} = \{\ldots, -4, 3, 10, \ldots\}$; (c) $18 + 26\mathbb{Z}$; (e) $5 + 6\mathbb{Z}$.

2. (a) No es un grupo; (c) es un grupo.

6.

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

8. Elija dos matrices. Casi cualquier par sirve.

15. Hay un grupo no abeliano con seis elementos.

16. Considere el grupo de simetrías de un triángulo equilátero o de un cuadrado.

17. Hay cinco grupos diferentes de orden 8.

18. Sea

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

en S_n. Todos los a_i deben ser distintos. Hay n forman de elegir a_1, $n-1$ formas de elegir a_2, ..., 2 formas de elegir a_{n-1}, y solo una forma de elegir a_n. Por lo tanto, podemos formar σ de $n(n-1)\cdots 2\cdot 1 = n!$ maneras.

25.

$$\begin{aligned}(aba^{-1})^n &= (aba^{-1})(aba^{-1})\cdots(aba^{-1}) \\ &= ab(aa^{-1})b(aa^{-1})b\cdots b(aa^{-1})ba^{-1} \\ &= ab^n a^{-1}.\end{aligned}$$

31. Como $abab = (ab)^2 = e = a^2b^2 = aabb$, sabemos que $ba = ab$.

35. $H_1 = \{\mathrm{id}\}$, $H_2 = \{\mathrm{id}, \rho_1, \rho_2\}$, $H_3 = \{\mathrm{id}, \mu_1\}$, $H_4 = \{\mathrm{id}, \mu_2\}$, $H_5 = \{\mathrm{id}, \mu_3\}$, S_3.

41. La identidad de G es $1 = 1+0\sqrt{2}$. Como $(a+b\sqrt{2}\,)(c+d\sqrt{2}\,) = (ac+2bd)+(ad+bc)\sqrt{2}$, G es cerrado bajo multiplicación. Finalmente, $(a+b\sqrt{2}\,)^{-1} = a/(a^2-2b^2) - b\sqrt{2}/(a^2-2b^2)$.

46. Considere S_3.

49. $ba = a^4b = a^3ab = ab$

4.4 Ejercicios

1. (a) Falso; (c) falso; (e) verdadero.

2. (a) 12; (c) infinito; (e) 10.

3. (a) $7\mathbb{Z} = \{\ldots, -7, 0, 7, 14, \ldots\}$; (b) $\{0, 3, 6, 9, 12, 15, 18, 21\}$; (c) $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10\}$; (g) $\{1, 3, 7, 9\}$; (j) $\{1, -1, i, -i\}$.

4. (a)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(c)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

10. (a) 0; (b) $1, -1$.

11. 1, 2, 3, 4, 6, 8, 12, 24.

15. (a) $-3+3i$; (c) $43-18i$; (e) i

16. (a) $\sqrt{3}+i$; (c) -3.

17. (a) $\sqrt{2}\,\mathrm{cis}(7\pi/4)$; (c) $2\sqrt{2}\,\mathrm{cis}(\pi/4)$; (e) $3\,\mathrm{cis}(3\pi/2)$.

18. (a) $(1-i)/2$; (c) $16(i-\sqrt{3}\,)$; (e) $-1/4$.

22. (a) 292; (c) 1523.

27. $|\langle g\rangle \cap \langle h\rangle| = 1$.

31. El elemento identidad en cualquier grupo tiene orden finito. Si $g, h \in G$ tienen orden m y n, respectivamente, como $(g^{-1})^m = e$ y $(gh)^{mn} = e$, se cumple que los elementos de orden finito en G forman un subgrupo de G.

37. Si g es un elemento distinto de la identidad en G, entonces g debe generar todo G; de lo contrario, $\langle g\rangle$ sería un subgrupo propio no trivial de G.

5.3 Ejercicios

1. (a) (12453); (c) (13)(25).

2. (a) (135)(24); (c) (14)(23); (e) (1324); (g) (134)(25); (n) (17352).

3. (a) (16)(15)(13)(14); (c) (16)(14)(12).

4. $(a_1, a_2, \ldots, a_n)^{-1} = (a_1, a_n, a_{n-1}, \ldots, a_2)$

5. (a) $\{(13), (13)(24), (132), (134), (1324), (1342)\}$ no es un subgrupo.

8. (12345)(678).

11. Permutaciones de la forma

$$(1), (a_1, a_2)(a_3, a_4), (a_1, a_2, a_3), (a_1, a_2, a_3, a_4, a_5)$$

son posibles en A_5.

17. Calcule (123)(12) y (12)(123).

25. Considere los casos $(ab)(bc)$ y $(ab)(cd)$.

30. Para la parte (a), muestre que $\sigma\tau\sigma^{-1}(\sigma(a_i)) = \sigma(a_{i+1})$.

6.4 Ejercicios

1. El orden de g y el orden de h deben ambos dividir el orden de G.

2. Los órdenes posibles deben ser divisores de 60.

3. Esto es verdadero para todo subgrupo propio no trivial.

4. Falso.

5. (a) $\langle 8\rangle$, $1 + \langle 8\rangle$, $2 + \langle 8\rangle$, $3 + \langle 8\rangle$, $4 + \langle 8\rangle$, $5 + \langle 8\rangle$, $6 + \langle 8\rangle$, and $7 + \langle 8\rangle$; (c) $3\mathbb{Z}$, $1 + 3\mathbb{Z}$, and $2 + 3\mathbb{Z}$.

7. $4^{\phi(15)} \equiv 4^8 \equiv 1 \pmod{15}$.

12. Sea $g_1 \in gH$. Muestre que $g_1 \in Hg$ y por lo tanto $gH \subset Hg$.

19. Muestre que $g(H \cap K) = gH \cap gK$.

22. Si $\text{mcd}(m, n) = 1$, entonces $\phi(mn) = \phi(m)\phi(n)$ (Ejercicio 2.3.26 en el Capítulo 2).

7.3 Ejercicios

1. `LAORYHAPDWK`

3. Hint: `V = E`, `E = X` (also used for spaces and punctuation), `K = R`.

4. $26! - 1$

7. (a) 2791; (c) 112135 25032 442.

9. (a) 31; (c) 14.

10. (a) $n = 11 \cdot 41$; (c) $n = 8779 \cdot 4327$.

8.5 Ejercicios

2. No puede ser un código de gruops pues $(0000) \notin C$.

3. (a) 2; (c) 2.

4. (a) 3; (c) 4.

6. (a) $d_{\min} = 2$; (c) $d_{\min} = 1$.

7.

(a) $(00000), (00101), (10011), (10110)$

$$G = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$$

(b) $(000000), (010111), (101101), (111010)$

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$$

9. Multiples errores ocurren en una de las palabras recibidas.

11. (a) Es matriz verificadora canónica con matriz generadora estándar

$$G = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

(c) Es matriz verificadora canónica con matriz generadora estándar

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

12. (a) Ocurren todos los posibles síndromes.

15. (a) C, $(10000) + C$, $(01000) + C$, $(00100) + C$, $(00010) + C$, $(11000) + C$, $(01100) + C$, $(01010) + C$. No hay tabla de decodificación para C pues este es solo un código detector de un error.

19. Sea $\mathbf{x} \in C$ una palabra de peso impar y defina una función y defina una función del conjunto de todas las palabras de peso impar al conjunto de las palabras de peso par como $\mathbf{y} \mapsto \mathbf{x} + \mathbf{y}$. Muestre que esta función es una biyección.

23. Para 20 posiciones de información, se requieren al menor 6 bits de verificación para permitir un código de corrección de un error.

9.3 Ejercicios

1. Todo grupo cíclico infinito es isomorfo a $\mathbb{Z}$ por el Teorema 9.7.

2. Defina $\phi : \mathbb{C}^* \to GL_2(\mathbb{R})$ como

$$\phi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

3. Falso.

6. Defina una función de $\mathbb{Z}_n$ en el grupo de raíces n-ésimas de la unidad como $k \mapsto \text{cis}(2k\pi/n)$.

8. Suponga que $\mathbb{Q}$ es cíclico e intente encontrar un generador.

11. Hay dos grupos no abelianos y tres grupos abelianos que no son isomorfos.

16. (a) 12; (c) 5.

19. Haga el dibujo.

20. Verdadero.

25. Verdadero.

27. Sea a un generador de G. Si $\phi : G \to H$ es un isomorfismo, muestre que $\phi(a)$ es un generador de H.

38. Cualquier automorfismo de $\mathbb{Z}_6$ debe enviar al 1 en otro generador de $\mathbb{Z}_6$.

45. Para mostrar que ϕ es 1-1, sean $g_1 = h_1k_1$ y $g_2 = h_2k_2$ y considere $\phi(g_1) = \phi(g_2)$.

10.3 Ejercicios

1. (a)

	A_4	$(12)A_4$
A_4	A_4	$(12)A_4$
$(12)A_4$	$(12)A_4$	A_4

(c) D_4 no es normal en S_4.

8. Si $a \in G$ es un generador para G, entonces aH es un generador para G/H.

11. Para cualquier $g \in G$, muestre que la función $i_g : G \to G$ definida como $i_g : x \mapsto gxg^{-1}$ es un isomorfismo de G en si mismo. Luego considere $i_g(H)$.

12. Supongamos que $\langle g \rangle$ es normal en G y sea y un elemento arbitrario de G. Si $x \in C(g)$, debemos mostrar que yxy^{-1} también está en $C(g)$. Muestre que $(yxy^{-1})g = g(yxy^{-1})$.

14. (a) Sean $g \in G$ y $h \in G'$. Si $h = aba^{-1}b^{-1}$, entonces

$$\begin{aligned} ghg^{-1} &= gaba^{-1}b^{-1}g^{-1} \\ &= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \\ &= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}. \end{aligned}$$

También debemos demostrar que si $h = h_1 \cdots h_n$ with $h_i = a_ib_ia_i^{-1}b_i^{-1}$, entonces ghg^{-1} es un producto de elementos del mismo tipo. Pero, $ghg^{-1} = gh_1 \cdots h_ng^{-1} = (gh_1g^{-1})(gh_2g^{-1}) \cdots (gh_ng^{-1})$.

11.3 Ejercicios

2. (a) es un homomorfismo con núcleo $\{1\}$; (c) no es un homomorfismo.

4. Como $\phi(m+n) = 7(m+n) = 7m+7n = \phi(m)+\phi(n)$, ϕ es un homomorfismo.

5. Para cualquier homomorfismo $\phi : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$, el núcleo de ϕ es un subgrupo de $\mathbb{Z}_{24}$ y la imagen de ϕ es un subgrupo de $\mathbb{Z}_{18}$. Ahora usea el hecho de que la imagen de un generador es un generador.

9. Sean $a, b \in G$. Entonces $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$.

17. Encuentre un contraejemplo.

12.3 Ejercicios

1.

$$\begin{aligned}\frac{1}{2}\left[\|\mathbf{x}+\mathbf{y}\|^2+\|\mathbf{x}\|^2-\|\mathbf{y}\|^2\right] &= \frac{1}{2}\left[\langle x+y, x+y\rangle - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2\right] \\ &= \frac{1}{2}\left[\|\mathbf{x}\|^2 + 2\langle x, y\rangle + \|\mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2\right] \\ &= \langle \mathbf{x}, \mathbf{y}\rangle.\end{aligned}$$

3. (a) está en $SO(2)$; (c) no está en $O(3)$.

5. (a) $\langle \mathbf{x}, \mathbf{y}\rangle = \langle \mathbf{y}, \mathbf{x}\rangle$.

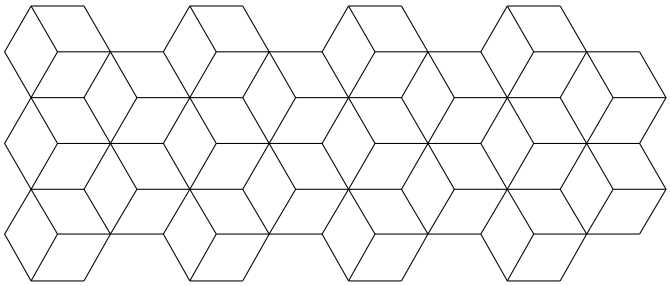
7. Use la matriz unimodular

$$\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}.$$

10. Muestre que el núcleo de la función $\det : O(n) \to \mathbb{R}^*$ es $SO(n)$.

13. True.

17. $p6m$



13.3 Ejercicios

1. Hay tres grupos posibles de orden 40.

4. (a) $\{0\} \subset \langle 6\rangle \subset \langle 3\rangle \subset \mathbb{Z}_{12}$; (e) $\{(1)\} \times \{0\} \subset \{(1), (123), (132)\} \times \{0\} \subset S_3 \times \{0\} \subset S_3 \times \langle 2\rangle \subset S_3 \times \mathbb{Z}_4$.

7. Use el Teorema Fundamental de los Grupos Abelianos Finitamente Generados.

12. Si N y G/N son solubles, entonces tienen series solubles

$$\begin{aligned} N = N_n \supset N_{n-1} \supset \cdots \supset N_1 \supset N_0 = \{e\} \\ G/N = G_n/N \supset G_{n-1}/N \supset \cdots G_1/N \supset G_0/N = \{N\}. \end{aligned}$$

16. Use el hecho de que D_n tiene un subgrupo cíclico de índice 2.

21. G/G' es abeliano.

14.4 Exercises

1. Example 14.1: 0, $\mathbb{R}^2 \setminus \{0\}$. Example 14.2: $X = \{1, 2, 3, 4\}$.

2. (a) $X_{(1)} = \{1, 2, 3\}$, $X_{(12)} = \{3\}$, $X_{(13)} = \{2\}$, $X_{(23)} = \{1\}$, $X_{(123)} = X_{(132)} = \emptyset$. $G_1 = \{(1), (23)\}$, $G_2 = \{(1), (13)\}$, $G_3 = \{(1), (12)\}$.

3. (a) $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$.

6. The conjugacy classes for S_4 are

$$\begin{aligned}\mathcal{O}_{(1)} &= \{(1)\},\\ \mathcal{O}_{(12)} &= \{(12),(13),(14),(23),(24),(34)\},\\ \mathcal{O}_{(12)(34)} &= \{(12)(34),(13)(24),(14)(23)\},\\ \mathcal{O}_{(123)} &= \{(123),(132),(124),(142),(134),(143),(234),(243)\},\\ \mathcal{O}_{(1234)} &= \{(1234),(1243),(1324),(1342),(1423),(1432)\}.\end{aligned}$$

The class equation is $1+3+6+6+8=24$.

8. $(3^4+3^1+3^2+3^1+3^2+3^2+3^3+3^3)/8 = 21$.

11. The group of rigid motions of the cube can be described by the allowable permutations of the six faces and is isomorphic to S_4. There are the identity cycle, 6 permutations with the structure $(abcd)$ that correspond to the quarter turns, 3 permutations with the structure $(ab)(cd)$ that correspond to the half turns, 6 permutations with the structure $(ab)(cd)(ef)$ that correspond to rotating the cube about the centers of opposite edges, and 8 permutations with the structure $(abc)(def)$ that correspond to rotating the cube about opposite vertices.

15. $(1\cdot 2^6 + 3\cdot 2^4 + 4\cdot 2^3 + 2\cdot 2^2 + 2\cdot 2^1)/12 = 13$.

17. $(1\cdot 2^8 + 3\cdot 2^6 + 2\cdot 2^4)/6 = 80$.

22. Use the fact that $x \in gC(a)g^{-1}$ if and only if $g^{-1}xg \in C(a)$.

15.3 Exercises

1. If $|G| = 18 = 2\cdot 3^2$, then the order of a Sylow 2-subgroup is 2, and the order of a Sylow 3-subgroup is 9.

2. The four Sylow 3-subgroups of S_4 are $P_1 = \{(1),(123),(132)\}$, $P_2 = \{(1),(124),(142)\}$, $P_3 = \{(1),(134),(143)\}$, $P_4 = \{(1),(234),(243)\}$.

5. Since $|G| = 96 = 2^5\cdot 3$, G has either one or three Sylow 2-subgroups by the Third Sylow Theorem. If there is only one subgroup, we are done. If there are three Sylow 2-subgroups, let H and K be two of them. Therefore, $|H\cap K| \geq 16$; otherwise, HK would have $(32\cdot 32)/8 = 128$ elements, which is impossible. Thus, $H\cap K$ is normal in both H and K since it has index 2 in both groups.

8. Show that G has a normal Sylow p-subgroup of order p^2 and a normal Sylow q-subgroup of order q^2.

10. False.

17. If G is abelian, then G is cyclic, since $|G| = 3\cdot 5\cdot 17$. Now look at Example 15.14.

23. Define a mapping between the right cosets of $N(H)$ in G and the conjugates of H in G by $N(H)g \mapsto g^{-1}Hg$. Prove that this map is a bijection.

26. Let $aG', bG' \in G/G'$. Then $(aG')(bG') = abG' = ab(b^{-1}a^{-1}ba)G' = (abb^{-1}a^{-1})baG' = baG'$.

16.6 Exercises

1. (a) $7\mathbb{Z}$ is a ring but not a field; (c) $\mathbb{Q}(\sqrt{2}\,)$ is a field; (f) R is not a ring.

3. (a) $\{1,3,7,9\}$; (c) $\{1,2,3,4,5,6\}$; (e)

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \right\}.$$

4. (a) $\{0\}$, $\{0,9\}$, $\{0,6,12\}$, $\{0,3,6,9,12,15\}$, $\{0,2,4,6,8,10,12,14,16\}$; (c) there are no nontrivial ideals.

7. Assume there is an isomorphism $\phi : \mathbb{C} \to \mathbb{R}$ with $\phi(i) = a$.

8. False. Assume there is an isomorphism $\phi : \mathbb{Q}(\sqrt{2}\,) \to \mathbb{Q}(\sqrt{3}\,)$ such that $\phi(\sqrt{2}\,) = a$.

13. (a) $x \equiv 17 \pmod{55}$; (c) $x \equiv 214 \pmod{2772}$.

16. If $I \neq \{0\}$, show that $1 \in I$.

18. (a) $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$.

26. Let $a \in R$ with $a \neq 0$. Then the principal ideal generated by a is R. Thus, there exists a $b \in R$ such that $ab = 1$.

28. Compute $(a+b)^2$ and $(-ab)^2$.

34. Let $a/b, c/d \in \mathbb{Z}_{(p)}$. Then $a/b + c/d = (ad+bc)/bd$ and $(a/b)\cdot(c/d) = (ac)/(bd)$ are both in $\mathbb{Z}_{(p)}$, since $\gcd(bd, p) = 1$.

38. Suppose that $x^2 = x$ and $x \neq 0$. Since R is an integral domain, $x = 1$. To find a nontrivial idempotent, look in $\mathbb{M}_2(\mathbb{R})$.

17.4 Exercises

2. (a) $9x^2 + 2x + 5$; (b) $8x^4 + 7x^3 + 2x^2 + 7x$.

3. (a) $5x^3 + 6x^2 - 3x + 4 = (5x^2 + 2x + 1)(x-2) + 6$; (c) $4x^5 - x^3 + x^2 + 4 = (4x^2+4)(x^3+3) + 4x^2 + 2$.

5. (a) No zeros in $\mathbb{Z}_{12}$; (c) 3, 4.

7. Look at $(2x+1)$.

8. (a) Reducible; (c) irreducible.

10. One factorization is $x^2 + x + 8 = (x+2)(x+9)$.

13. The integers $\mathbb{Z}$ do not form a field.

14. False.

16. Let $\phi : R \to S$ be an isomorphism. Define $\overline{\phi} : R[x] \to S[x]$ by $\overline{\phi}(a_0 + a_1x + \cdots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$.

20. The polynomial

$$\Phi_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1$$

is called the ***cyclotomic polynomial.*** Show that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$ for any prime p.

26. Find a nontrivial proper ideal in $F[x]$.

18.3 Exercises

1. Note that $z^{-1} = 1/(a + b\sqrt{3}\,i) = (a - b\sqrt{3}\,i)/(a^2 + 3b^2)$ is in $\mathbb{Z}[\sqrt{3}\,i]$ if and only if $a^2 + 3b^2 = 1$. The only integer solutions to the equation are $a = \pm 1, b = 0$.

2. (a) $5 = -i(1+2i)(2+i)$; (c) $6+8i = -i(1+i)^2(2+i)^2$.

4. True.

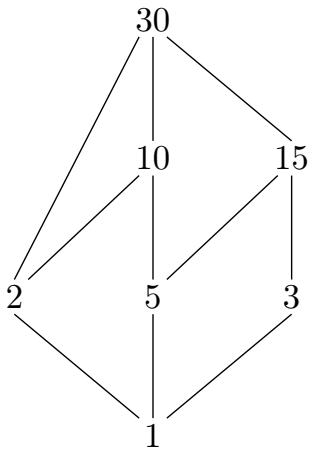
9. Let $z = a+bi$ and $w = c+di \neq 0$ be in $\mathbb{Z}[i]$. Prove that $z/w \in \mathbb{Q}(i)$.

15. Let $a = ub$ with u a unit. Then $\nu(b) \leq \nu(ub) \leq \nu(a)$. Similarly, $\nu(a) \leq \nu(b)$.

16. Show that 21 can be factored in two different ways.

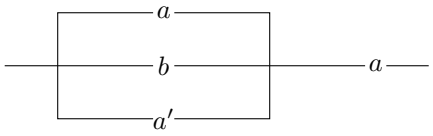
19.4 Exercises

2.

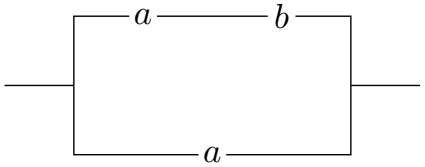


5. False.

6. (a) $(a \vee b \vee a') \wedge a$



(c) $a \vee (a \wedge b)$



8. Not equivalent.

10. (a) $a' \wedge [(a \wedge b') \vee b] = a \wedge (a \vee b)$.

14. Let I, J be ideals in R. We need to show that $I + J = \{r + s : r \in I \text{ and } s \in J\}$ is the smallest ideal in R containing both I and J. If $r_1, r_2 \in I$ and $s_1, s_2 \in J$, then $(r_1 + s_1) + (r_2 + s_2) = (r_1 + r_2) + (s_1 + s_2)$ is in $I + J$. For $a \in R$, $a(r_1 + s_1) = ar_1 + as_1 \in I + J$; hence, $I + J$ is an ideal in R.

18. (a) No.

20. ($\Rightarrow$). $a = b \Rightarrow (a \wedge b') \vee (a' \wedge b) = (a \wedge a') \vee (a' \wedge a) = O \vee O = O$. ($\Leftarrow$). $(a \wedge b') \vee (a' \wedge b) = O \Rightarrow a \vee b = (a \vee a) \vee b = a \vee (a \vee b) = a \vee [I \wedge (a \vee b)] = a \vee [(a \vee a') \wedge (a \vee b)] = [a \vee (a \wedge b')] \vee [a \vee (a' \wedge b)] = a \vee [(a \wedge b') \vee (a' \wedge b)] = a \vee 0 = a$. A symmetric argument shows that $a \vee b = b$.

20.4 Exercises

3. $\mathbb{Q}(\sqrt{2},\sqrt{3}\,)$ has basis $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\,\}$ over $\mathbb{Q}$.

5. The set $\{1,x,x^2,\ldots,x^{n-1}\}$ is a basis for P_n.

7. (a) Subspace of dimension 2 with basis $\{(1,0,-3),(0,1,2)\}$; (d) not a subspace

10. Since $0=\alpha 0=\alpha(-v+v)=\alpha(-v)+\alpha v$, it follows that $-\alpha v=\alpha(-v)$.

12. Let $v_0=0,v_1,\ldots,v_n\in V$ and $\alpha_0\neq 0,\alpha_1,\ldots,\alpha_n\in F$. Then $\alpha_0v_0+\cdots+\alpha_nv_n=0$.

15. (a) Let $u,v\in\ker(T)$ and $\alpha\in F$. Then

$$T(u+v)=T(u)+T(v)=0$$
$$T(\alpha v)=\alpha T(v)=\alpha 0=0.$$

Hence, $u+v,\alpha v\in\ker(T)$, and $\ker(T)$ is a subspace of V.

(c) The statement that $T(u)=T(v)$ is equivalent to $T(u-v)=T(u)-T(v)=0$, which is true if and only if $u-v=0$ or $u=v$.

17. (a) Let $u,u'\in U$ and $v,v'\in V$. Then

$$(u+v)+(u'+v')=(u+u')+(v+v')\in U+V$$
$$\alpha(u+v)=\alpha u+\alpha v\in U+V.$$

21.4 Ejercicios

1. (a) $x^4-(2/3)x^2-62/9$; (c) x^4-2x^2+25.

2. (a) $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\,\}$; (c) $\{1,i,\sqrt{2},\sqrt{2}\,i\}$; (e) $\{1,2^{1/6},2^{1/3},2^{1/2},2^{2/3},2^{5/6}\}$.

3. (a) $\mathbb{Q}(\sqrt{3},\sqrt{7}\,)$.

5. Use el hecho de que los elementos de $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ son 0, 1, α, $1+\alpha$, α^2, $1+\alpha^2$, $\alpha+\alpha^2$, $1+\alpha+\alpha^2$ y el hecho de que $\alpha^3+\alpha+1=0$.

8. False.

14. Supongamos que E es algebraico sobre F y K es algebraico sobre E. Sea $\alpha\in K$. Basta con demostrar que α es algebraico sobre alguna extensión finita de F. Como α es algebraico sobre E, debe ser cero de algún polinomio $p(x)=\beta_0+\beta_1x+\cdots+\beta_nx^n$ en $E[x]$. Por lo tanto α es algebraico sobre $F(\beta_0,\ldots,\beta_n)$.

22. Como $\{1,\sqrt{3},\sqrt{7},\sqrt{21}\,\}$ es una base para $\mathbb{Q}(\sqrt{3},\sqrt{7}\,)$ sobre $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3},\sqrt{7}\,)\supset\mathbb{Q}(\sqrt{3}+\sqrt{7}\,)$. Como $[\mathbb{Q}(\sqrt{3},\sqrt{7}\,):\mathbb{Q}]=4$, $[\mathbb{Q}(\sqrt{3}+\sqrt{7}\,):\mathbb{Q}]=2$ o 4. Como el grado del polinomio minimal de $\sqrt{3}+\sqrt{7}$ es 4, $\mathbb{Q}(\sqrt{3},\sqrt{7}\,)=\mathbb{Q}(\sqrt{3}+\sqrt{7}\,)$.

27. Sea $\beta\in F(\alpha)$ no en F. Entonces $\beta=p(\alpha)/q(\alpha)$, donde p y q son polinomios en α con $q(\alpha)\neq 0$ y coeficientes en F. Si β es algebraico sobre F, entonces hay un polinomio $f(x)\in F[x]$ tal que $f(\beta)=0$. Sea $f(x)=a_0+a_1x+\cdots+a_nx^n$. Entonces

$$0=f(\beta)=f\left(\frac{p(\alpha)}{q(\alpha)}\right)=a_0+a_1\left(\frac{p(\alpha)}{q(\alpha)}\right)+\cdots+a_n\left(\frac{p(\alpha)}{q(\alpha)}\right)^n.$$

Ahora multiplique ambos lados por $q(\alpha)^n$ para demostrar que hay un polinomio en $F[x]$ que se anula en α.

28. Vea el comentario que sigue al Teorema 21.13.

22.3 Ejercicios

1. Asegúrese de tener una extensión de cuerpos.

4. Hay ocho elementos en $\mathbb{Z}_2(\alpha)$. Exhiba dos ceros más de x^3+x^2+1 además de α entre estos ocho elementos.

5. Encuentre un polinomio irreducible $p(x)$ en $\mathbb{Z}_3[x]$ de grado 3 y muestre que $\mathbb{Z}_3[x]/\langle p(x)\rangle$ tiene 27 elementos.

7. (a) $x^5-1=(x+1)(x^4+x^3+x^2+x+1)$; (c) $x^9-1=(x+1)(x^2+x+1)(x^6+x^3+1)$.

8. Verdadero.

11. (a) Use el hechode que $x^7-1=(x+1)(x^3+x+1)(x^3+x^2+1)$.

12. Falso.

17. Si $p(x)\in F[x]$, entonces $p(x)\in E[x]$.

18. Como α es algebraico sobreo F de grado n, podemos escribir cualquier elemento $\beta\in F(\alpha)$ de forma única como $\beta=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}$ with $a_i\in F$. Existen q^n posibles n-tuplas $(a_0,a_1,\ldots,a_{n-1})$.

24. Factorice $x^{p-1}-1$ sobre $\mathbb{Z}_p$.

23.4 Ejercicios

1. (a) $\mathbb{Z}_2$; (c) $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$.

2. (a) Separable sobre $\mathbb{Q}$ pues $x^3+2x^2-x-2=(x-1)(x+1)(x+2)$; (c) no es separable sobre $\mathbb{Z}_3$ pues $x^4+x^2+1=(x+1)^2(x+2)^2$.

3. Si

$$[\mathrm{GF}(729):\mathrm{GF}(9)]=[\mathrm{GF}(729):\mathrm{GF}(3)]/[\mathrm{GF}(9):\mathrm{GF}(3)]=6/2=3,$$

entonces $G(\mathrm{GF}(729)/\mathrm{GF}(9))\cong\mathbb{Z}_3$. Un generador para $G(\mathrm{GF}(729)/\mathrm{GF}(9))$ es σ, deonde $\sigma_{3^6}(\alpha)=\alpha^{3^6}=\alpha^{729}$ para $\alpha\in\mathrm{GF}(729)$.

4. (a) S_5; (c) S_3; (g) Vea el Ejemplo 23.10.

5. (a) $\mathbb{Q}(i)$

7. Sea E el cuerpo de descomposición de un polinomio cúbico en $F[x]$. Muestre que $[E:F]$ es menor o igual a 6 y es divisible por 3. Como $G(E/F)$ es un subgrupo de S_3 cuyo orden es divisible por 3, concluya que este grupo debe ser isomorfo a $\mathbb{Z}_3$ o a S_3.

9. G es un subgrupo de S_n.

16. Verdadero.

20.

(a) Claramente $\omega,\omega^2,\ldots,\omega^{p-1}$ son distintas pues $\omega\neq 1$ ni 0. Para mostrar que ω^i es un cero de Φ_p, calcule $\Phi_p(\omega^i)$.

(b) Los conjugados de ω son $\omega,\omega^2,\ldots,\omega^{p-1}$. Defina una función $\phi_i:\mathbb{Q}(\omega)\to\mathbb{Q}(\omega^i)$ como

$$\phi_i(a_0+a_1\omega+\cdots+a_{p-2}\omega^{p-2})=a_0+a_1\omega^i+\cdots+c_{p-2}(\omega^i)^{p-2},$$

donde $a_i\in\mathbb{Q}$. Demuestre que ϕ_i es un isomorfismo de cuerpos. Muestre que ϕ_2 genera $G(\mathbb{Q}(\omega)/\mathbb{Q})$.

(c) Muestre que $\{\omega,\omega^2,\ldots,\omega^{p-1}\}$ es una base para $\mathbb{Q}(\omega)$ sobre $\mathbb{Q}$, y considere cuáles combinaciones lineales de $\omega,\omega^2,\ldots,\omega^{p-1}$ quedan fijas por todos los elementos de $G(\mathbb{Q}(\omega)/\mathbb{Q})$.

C

Notación

La siguiente tabla deine la notación usada en este libro. Los números de página o referencias se refieren a la primera aparición de cada símbolo.

Symbol	Description	Página
$a \in A$	a está en el conjunto A	3
$\mathbb{N}$	los número naturales	4
$\mathbb{Z}$	los números enteros	4
$\mathbb{Q}$	los números racionales	4
$\mathbb{R}$	los números reales	4
$\mathbb{C}$	los números complejos	4
$A \subset B$	A es un subconjunto de B	4
$\emptyset$	el conjunto vacío	4
$A \cup B$	la unión de los conjuntos A y B	4
$A \cap B$	la intersección de los conjuntos A y B	4
A'	complemento del conjunto A	5
$A \setminus B$	diferencia entre los conjuntos A y B	5
$A \times B$	producto Cartesiano de conjuntos A y B	7
A^n	$A \times \cdots \times A$ (n veces)	7
id	función identidad	10
f^{-1}	inversa de la función f	10
$a \equiv b \pmod{n}$	a es congruente a b módulo n	13
$n!$	n factorial	24
$\binom{n}{k}$	coeficiente binomial $n!/(k!(n-k)!)$	24
$a \mid b$	a divide a b	26
$\text{mcd}(a, b)$	máximo común divisor de a y b	26
$\mathcal{P}(X)$	conjunto potencia de X	30
$\text{mcm}(m, n)$	el mínimo común múltiplo de m y n	32
$\mathbb{Z}_n$	los enteros módulo n	38
$U(n)$	grupo de unidades en $\mathbb{Z}_n$	43
$\mathbb{M}_n(\mathbb{R})$	las matrices de $n \times n$ con entradas en $\mathbb{R}$	44
$\det A$	el determinante de A	44
$GL_n(\mathbb{R})$	el grupo lineal general	44
Q_8	el grupo de cuaterniones	44
$\mathbb{C}^*$	el grupo multiplicativo de los complejos	45
$\lvert G \rvert$	el orden de un grupo	45
$\mathbb{R}^*$	el grupo multiplicativo de los números reales	47

(Continúa en la próxima página)

Symbol	Description	Página
$\mathbb{Q}^*$	el grupo multiplicativo de los números racionales	47
$SL_n(\mathbb{R})$	el grupo lineal especial	47
$Z(G)$	el centro de un grupo	52
$\langle a \rangle$	grupo cíclico generado por a	62
$\lvert a \rvert$	el orden de un elemento a	63
$\operatorname{cis}\theta$	$\cos\theta + i\sin\theta$	66
$\mathbb{T}$	el grupo de la circunferencia	68
S_n	el grupo simétrico en n símbolos	85
$(a_1, a_2, \ldots, a_k)$	ciclo de largo k	87
A_n	el grupo alternante en n símbolos	90
D_n	el grupo the dihedral	92
$[G : H]$	índice de un subgrupo H en un grupo G	108
$\mathcal{L}_H$	el conjunto de clases laterales izquierdas de un subgrupo H en un grupo G	109
$\mathcal{R}_H$	el conjunto de clases laterales derechas de un subgrupo H en un grupo G	109
$d(\mathbf{x}, \mathbf{y})$	distancia de Hamming entre $\mathbf{x}$ e $\mathbf{y}$	138
$d_{\min}$	la distancia mínima de un código	138
$w(\mathbf{x})$	el peso de $\mathbf{x}$	138
$\mathbb{M}_{m\times n}(\mathbf{Z}_2)$	el conjunto de matrices de $m\times n$ con coeficientes en $\mathbb{Z}_2$	142
$\operatorname{Null}(H)$	espacio nulo de una matriz H	142
δ_{ij}	delta de Kronecker	146
$G \cong H$	G es isomorfo a un grupo H	161
$\operatorname{Aut}(G)$	grupo de automorfismos de un grupo G	171
i_g	$i_g(x) = gxg^{-1}$	171
$\operatorname{Inn}(G)$	grupo de automorfismos internos de un grupo G	171
ρ_g	representación regular derecha	171
G/N	grupo cociente de G mód N	179
G'	subgrupo conmutador de G	184
$\ker\phi$	núcleo de ϕ	191
(a_{ij})	matriz	204
$O(n)$	grupo ortogonal	206
$\lVert\mathbf{x}\rVert$	longitud de un vector $\mathbf{x}$	206
$SO(n)$	grupo ortogonal especial	209
$E(n)$	Grupo Euclideano	209
$\mathcal{O}_x$	órbit de x	234
X_g	conjunto de puntos fijos de g	235
G_x	subgrupo de isotropía de x	235
$N(H)$	normalizer of s subgroup H	253
$\mathbb{H}$	el anillo de los cuaterniones	271
$\mathbb{Z}[i]$	los enteros Gaussianos	273
$\operatorname{char} R$	característica de un anillo R	274
$\mathbb{Z}_{(p)}$	ring of integers localized at p	286
$\operatorname{gr} f(x)$	grado de un polinomio	297
$R[x]$	anillo depolinomios sobre un anillo R	298

(Continúa en la próxima página)

Symbol	Description	Página
$R[x_1, x_2, \ldots, x_n]$	anillo de polinomios en n indeterminadas	300
ϕ_α	homomorfismo de evaluación en α	300
$\mathbb{Q}(x)$	cuerpo de funciones racionales sobre $\mathbb{Q}$	322
$\nu(a)$	Valuación Euclideana de a	326
$F(x)$	field of rational functions in x	330
$F(x_1, \ldots, x_n)$	field of rational functions in $x_1, \ldots, x_n$	330
$a \preceq b$	a es menor a b	336
$a \vee b$	supremo de a y b	338
$a \wedge b$	ínfimo de a y b	338
I	elemento mayor en un reticulado	340
O	menor elemento en un reticulado	340
a'	complemento de a en un reticulado	340
$\dim V$	dimension of a vector space V	361
$U \oplus V$	direct sum of vector spaces U and V	363
$\mathrm{Hom}(V, W)$	set of all linear transformations from U into V	363
V^*	dual of a vector space V	363
$F(\alpha_1, \ldots, \alpha_n)$	menor cuerpo que contiene a F y $\alpha_1, \ldots, \alpha_n$	373
$[E : F]$	dimensión de la extensión de cuerpos E sobre F	376
$\mathrm{GF}(p^n)$	Cuerpo de Galois de orden p^n	400
F^*	grupo multiplicativo de un cuerpo F	401
$G(E/F)$	Grupo de Galois de E sobre F	417
$F_{\{\sigma_i\}}$	cuerpo fijo por el automorfismo σ_i	421
F_G	cuerpo fijo por el grupo de automorfismos G	421
Δ^2	discriminante de un polinomio	433

Índice alfabético

This book was authored and produced with PreTeXt.