Elementos de Álgebra

Cristián Reyes

2019

Índice general

Capítulo 1

Preliminares

En este capítulo recordaremos algunas propiedades y construcciones elementales en los enteros, junto un poco de notación que usaremos a lo largo del resto del texto. Tomaremos como dadas la existencia de $\mathbb{N}$ y las propiedades algebraicas básicas de la suma y multiplicación de números naturales. Una buena referencia para ello es el libro de Halmos [Hal60]. A lo largo del texto escribiremos $[n] = \{1, 2, \dots, n\}$ para $n \in \mathbb{N}$ y δ_{nm} la función que vale 1 si $n = m \in \mathbb{N}$ y 0 si $n \neq m$.

1.1. Estructuras algebraicas

Primero que nada, necesitamos recordar y fijar algunas definiciones básicas: para nosotros, una estructura algebraica es un conjunto A junto con una colección de operaciones finitarias sobre A (es decir, funciones a valores en A cuyo dominio es A^n para algún $n \in \mathbb{N}$).

Una operación binaria $\cdot$ se dice

- *asociativa* si para cada x, y, z en A, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- *conmutativa* si para cada x, y en A, $x \cdot y = y \cdot x$.

Un elemento fijo a en A (o una operación 0-aria) se dice

- *neutro* para $\cdot$ si $a \cdot x = x = x \cdot a$ para cada x en A. Si a sólo verifica la primera (segunda) de estas igualdades, se dice que a es neutro por la izquierda (derecha).
- *absorbente* para $\cdot$ si $a \cdot x = a = x \cdot a$ para cada x en A. Si a sólo verifica la primera (segunda) de estas igualdades, se dice que a es absorbente por la izquierda (derecha).
- *idempotente* si $a \cdot a = a$.
- *cancelable* para $\cdot$ si para cada b, c en A, la ecuación $ab = ac$ implica que $b = c$ y la ecuación $ba = ca$ implica que $b = c$. Si a sólo verifica la primera (segunda) de estas igualdades, se dice que a es cancelable por la izquierda (derecha).

Es fácil ver que una operación binaria tiene a lo más un elemento absorbente y a lo más un neutro.

Si A tiene un neutro para $\cdot$, dado a en A decimos que b en B es su *inverso* para $\cdot$ si $ba = e = ab$. Si b sólo verifica la primera (segunda) de estas igualdades, se dice que b es inverso por la izquierda (derecha)

de a. Es directo que si $\cdot$ es asociativa y tiene neutro, cada elemento tiene a lo más un inverso y si a, b son inversos izquierdos y derechos de un mismo elemento c, entonces necesariamente $a = b$.

Dadas dos operaciones binarias $\cdot$ y $\star$ sobre A, diremos que $\star$ distribuye sobre $\cdot$ si para cada x, y, z en A se tiene que

- $x \star (y \cdot z) = (x \star y) \cdot (x \star z)$.
- $(y \cdot z) \star x = (y \star x) \cdot (z \star x)$.

Si sólo se tiene la primera (segunda) ecuación, decimos que $\star$ distribuye por la izquierda (derecha) sobre $\cdot$.

Si $(A, \cdot)$ y $(B, \star)$ son dos estructuras y $\cdot$, $\star$ son operaciones binarias, entonces una función $f : A \to B$ se dice *homomorfismo* (o *morfismo*) si $f(a \cdot b) = f(a) \star f(b)$ para cada $a, b \in A$. Un homomorfismo f se dice

- *monomorfismo* si es inyectivo.
- *epimorfismo* si es sobreyectivo.
- *isomorfismo* si es biyectivo.
- *endomorfismo* si es A y B son la misma estructura.
- *automorfismo* si es endomorfismo y biyectivo.

Se verifica directamente que la composición de homomorfismos es un homomorfismo (y ocurre lo mismo para cualquiera de las clases de funciones anteriores), y que cuando $f : A \to B$ es epimorfismo, B hereda la asociatividad, conmutatividad y existencia de neutros e inversos a partir de estas propiedades en A. Los homomorfismos son los mapeos que respetan la estructura natural de un objeto algebraico, y a veces le pediremos más a un morfismo que sólo preservar las operaciones para ser considerado como tal (por ejemplo, al hablar de morfismos de anillos unitarios y no unitarios en el capítulo 3, o al hablar de morfismos de módulos en el capítulo 4).

1.2. Construcción de $\mathbb{Z}$ y $\mathbb{Q}$

Para empezar, construiremos $\mathbb{Z}$ y $\mathbb{Q}$ a partir de $\mathbb{N}$ para introducir ideas que luego generalizaremos al ver grupos y anillos más adelante.

Consideremos en $\mathbb{N} \times \mathbb{N}$ la relación de equivalencia $\sim$ definida por $(a, b) \sim (c, d)$ ssi $a + d = c + b$, y sea $\mathbb{Z} \doteq \mathbb{N} \times \mathbb{N}/\sim$ (es decir, $\mathbb{Z}$ es el conjunto de rectas de pendiente 1 en $\mathbb{N} \times \mathbb{N}$ y podemos pensar que la clase $[(a, b)]$ representa el entero $a - b$). La relación $\sim$ efectivamente es de equivalencia: es claro que $\sim$ es refleja y simétrica, y si tenemos que $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$, entonces $a + d = c + b$ y $c + f = e + d$. Luego

$$a + f + d = (a + d) + f = c + b + f = b + (c + f) = b + e + d,$$

y como cada elemento en $\mathbb{N}$ es cancelable para la suma obtenemos que $a + f = e + b$, es decir $(a, b) \sim (e, f)$. Luego $\sim$ es transitiva y por lo tanto es de equivalencia.

Definamos la suma y la multiplicación en $\mathbb{Z}$ como $[(a, b)] + [(c, d)] = [(a + c, b + d)]$ y $[(a, b)][(c, d)] = [(ac + bd, ad + bc)]$. Debemos verificar que están bien definidas (es decir, que el resultado de ambas operaciones no depende de la elección de los representantes de las clases): en efecto, si $(a, b) \sim (a', b')$ y $(c, d) \sim (c', d')$, tendremos que

$$a + b' = b + a' \text{ y } c + d' = d + c'. \tag{1.1}$$

Sumando ambas ecuaciones obtenemos la igualdad $(a+c)+(b'+d')=(a'+c')+(b+d)$, que es equivalente a $(a+c,b+d)\sim(a'+c',b'+d')$ y por lo tanto la suma está bien definida. Por otro lado, notemos que multiplicando la primera ecuación en 1.1 por c y d separadamente, y la segunda ecuación en 1.1 por a' y b' separadamente, obtenemos las igualdades

$$\begin{aligned} ac+b'c &= bc+a'c \\ bd+a'd &= ad+b'd \\ a'd'+a'c &= a'c'+a'd \\ b'c'+b'd &= b'c+b'd' \end{aligned}$$

y sumando todo sigue que

$$ac+bd+a'd'+b'c'+b'c+a'd+a'c+b'd = a'c'+b'd'+ad+bc+a'd+a'c+b'c,$$

o $ac+bd+a'd'+b'c' = a'c'+b'd'+ad+bc$. Concluimos que $[(ac+bd,ad+bc)]=[(a'c'+b'd',a'd'+b'c')]$ y que la multiplicación en $\mathbb{Z}$ también está bien definida.

Notemos que la inclusión $\iota:\mathbb{N}\to\mathbb{Z}$ definida por $\iota(n)=(0,n)$ es inyectiva y es morfismo entre $(\mathbb{N},+,\cdot)$ y $(\mathbb{Z},+,\cdot)$. Entonces podemos hablar de una copia de $\mathbb{N}$ dentro de $\mathbb{Z}$. Por último, es fácil ver que la nueva suma y multiplicación en $\mathbb{Z}$ son conmutativas y asociativas, que $\iota(0)$ e $\iota(1)$ son neutros para la suma y la multiplicación respectivamente, y que todo elemento $[(m,n)]$ posee un inverso aditivo $[(n,m)]$. Como cada elemento en $\mathbb{N}$ es cancelable para la suma y el producto, lo mismo ocurre para $\mathbb{Z}$.

Ahora veamos los racionales: consideremos $\mathbb{Q}\doteq\mathbb{Z}\times\mathbb{Z}^\times=\{(a,b);a,b\in\mathbb{Z},b\neq 0\}$ y la relación $\sim'$ de equivalencia sobre $\mathbb{Q}$ definida por $(a,b)\sim'(c,d)$ ssi $ad=cb$ (entonces la clase $[(a,b)]$ representa el racional $\frac{a}{b}$). $\sim'$ es efectivamente de equivalencia: nuevamente es claro que es refleja y simétrica, y si tenemos que $(a,b)\sim'(c,d)$ y $(c,d)\sim'(e,f)$, entonces $ad=cb$ y $cf=ed$. Luego

$$afd=(ad)f=cbf=b(cf)=bed,$$

y como cada elemento es cancelable para la multiplicación en $\mathbb{Z}$ concluimos que $af=eb$, es decir $(a,b)\sim'(e,f)$. Por lo tanto $\sim'$ es transitiva y sigue que también es de equivalencia.

Definimos la suma y la multiplicación de la manera natural, es decir $[(a,b)]+[(c,d)]=[(ad+bc,bd)]$ y $[(a,b)][(c,d)]=[(ab,cd)]$. La definición es consistente: si $(a,b)\sim'(a',b')$ y $(c,d)\sim'(c',d')$ tenemos las igualdades $ab'=a'b$ y $cd'=c'd$, de manera que

$$bd(a'd'+b'c')=dd'a'b+bb'c'd=dd'ab'+bb'cd'=b'd'(ad+bc)$$

y entonces $(ad+bc,bd)\sim'(a'd'+b'c',b'd')$. Por otro lado, vemos que

$$acb'd'=(ab')(cd')=(a'b)(c'd)=a'c'bd$$

y luego $(ac,bd)\sim'(a'c',b'd')$, es decir, ambas operaciones están bien definidas.

Nuevamente, la función $\iota' : \mathbb{Z} \to \mathbb{Q}$ definida por $\iota'(m) = [(m,1)]$ es monomorfismo entre $(\mathbb{Z},+,\cdot)$ y $(\mathbb{Q},+,\cdot)$. La conmutatividad y asociatividad de la suma y de la multiplicación son un poco más tediosas de verificar que antes, pero todo se reduce a estas propiedades en $\mathbb{Z}$. El neutro aditivo y multiplicativo son $\iota'(0)$ e $\iota'(1)$ respectivamente, y cada elemento $[(a,b)]$ admite un inverso aditivo $[(-a,b)]$ y (si $a \neq 0$) un inverso multiplicativo $[(b,a)]$.

El ejercicio 1.7 esboza una construcción puramente algebraica de $\mathbb{R}$.

1.3. Recuerdo de aritmética elemental

Ahora recordaremos algunos teoremas básicos de aritmética que serán generalizados al discutir factorización en anillos conmutativos en el capítulo 3. Si n, m son enteros, diremos que n divide a m o que m es múltiplo de n (escrito $n \mid m$) si existe un entero k tal que $m = kn$. También diremos que $n \neq 1, -1$ es primo si sus únicos divisores (salvo el signo) son 1 y sí mismo, y que n y m son primos entre sí cuando no comparten divisores. Si $n, m \in \mathbb{Z}$ son tales que al menos uno de ellos es no nulo, el máximo común divisor de n y m (escrito $\mathrm{mcd}(n,m)$) es el divisor positivo común a n y m de mayor módulo, y el mínimo común múltiplo (escrito $\mathrm{mcm}(n,m)$) es el múltiplo común de n y m de menor módulo. El mcd de dos enteros existe porque hay una cantidad finita de divisores de cada entero, y el mcm existe por el principio de buen orden en $\mathbb{N}$.

Teorema 1.1 (Algoritmo de la división)**.** *Para cada par $a, b \in \mathbb{Z}$ con $b \neq 0$, existen únicos $q, r \in \mathbb{Z}$ tales que $a = qb + r$ y $0 \leq r < |b|$.*

Demostración. Sin pérdida de generalidad podemos tomar $b > 0$ cambiando el signo de q. Además, si $a < 0$ y $b > 0$, podemos reescribir la ecuación $a = qb + r$ como $a' = b'q' + r'$ donde $a' = -a$, $q' = -q - 1$ y $r' = b - r$, de manera que $0 \leq r' < b$. Finalmente, el teorema se verifica directamente si $a = 0$, pues podemos tomar $q, r = 0$.

Luego podemos suponer a, b positivos. Si b divide a a estamos listos. Si no, consideremos la sucesión $a, a-b, a-2b, \ldots$ y sea q el primer natural tal que $a-(q+1)b < 0$. Definamos $r = a - qb \geq 0$ (por la minimalidad de q) y notemos que $r < b$ y $a = qb + r$ por definición.

Los enteros q, r son únicos, pues si $a = qb + r = q'b + r'$, entonces $r - r' = (q' - q)b$ y $|q' - q||b| = |r - r'| < |b|$ pues $0 \leq r, r' < |b|$. Luego $|q' - q| < 1$ y como q, q' son enteros, concluimos que $q = q'$ y por lo tanto $r = r'$. □

Teorema 1.2 (Algoritmo de Euclides)**.** *Considere el siguiente procedimiento: dados $a, b \in \mathbb{Z}$ con $b \neq 0$, sean r_0 y q_0 el resto de dividir a por b, y escribamos $r_{-1} = b$. Para $i \in \mathbb{N}$, definamos los enteros r_i, q_i inductivamente: si r_{i-1} y r_{i-2} ya están definidos y $r_{i-1} \neq 0$, entonces definamos r_i y q_i como el resto y el cociente, respectivamente, de dividir r_{i-2} por r_{i-1} (es decir, los enteros tal que $r_{i-2} = q_i r_{i-1} + r_i$). Si $r_{i-1} = 0$, entonces paramos. El algoritmo termina, y el último r no nulo es el* $\mathrm{mcd}(a,b)$.

Demostración. El algoritmo termina pues los r_i son una sucesión estrictamente decreciente de naturales. Sea $n \in \mathbb{N}$ tal que $r_{n+1} = 0$. Probemos que se cumplen las igualdades

$$\mathrm{mcd}(0, r_n) = r_n,\ \mathrm{mcd}(r_{i+1}, r_i) = \mathrm{mcd}(r_{i+2}, r_{i+1}) \tag{1.2}$$

para $i \in [n-1]$, de donde se deduce que $\mathrm{mcd}(a,b) = r_n$. Notemos que la ecuación $r_i = q_{i+2}r_{i+1} + r_{i+2}$ muestra que $\mathrm{mcd}(r_{i+1}, r_i)$ también divide a r_{i+2}, de manera que $\mathrm{mcd}(r_{i+1}, r_i) \leq \mathrm{mcd}(r_{i+2}, r_{i+1})$. Análogamente, la misma ecuación prueba que $\mathrm{mcd}(r_{i+2}, r_{i+1})$ divide a r_{i+1} y por lo tanto es menor o igual a $\mathrm{mcd}(r_{i+1}, r_i)$. Luego se cumple la segunda igualdad en 1.2. La primera es por definición. □

El algoritmo de Euclides también sirve para mostrar la infinitud de los primos: definamos los números de Euclides recursivamente por $e_n = e_1 e_2 \dots e_{n-1} + 1$ para $n \geq 1$ (donde el producto vacío es 1). El algoritmo anterior nos dice que cuando $n > m$ tenemos que $\mathrm{mcd}(e_n, e_m) = \mathrm{mcd}(e_m, 1) = \mathrm{mcd}(1, 0) = 1$, y entonces la sucesión q_n de los factores mínimos de e_n es una secuencia infinita de primos distintos entre sí.

Teorema 1.3 (Lema de Bézout)**.** *Para cada par $a, b \in \mathbb{Z}$, existen $s, t, \in \mathbb{Z}$ tales que* $\mathrm{mcd}(a,b) = as + bt$.

Demostración. Recordemos que $\mathrm{mcd}(a,b) = r_n$, el n-ésimo resto del algoritmo de Euclides y veamos que cada resto r_j admite una escritura del tipo $r_j = as_j + bt_j$: el caso base es $r_1 = a - bq_0$, y si $r_j = as_j + bt_j$ para $j \leq k < n$, entonces $r_{k+1} = -r_k q_k + r_{k-1} = -q_k(as_k + bt_k) + as_{k-1} + bt_{k-1} = as_{k+1} + bt_{k+1}$. □

Otra manera (no algorítmica) de probar el lema anterior es definir

$$l = \min\{as + bt;\ s, t \in \mathbb{Z} \text{ y } as + bt > 0\}$$

y verificar que $l = \mathrm{mcd}(a,b)$.

La próxima proposición permite probar fácilmente el teorema fundamental de la aritmética, y también entrega una caracterización de los primos en $\mathbb{Z}$ que justificará la definición de elemento primo en un anillo conmutativo en el capítulo 3.

Proposición 1.1 (Lema de Euclides)**.** *Sean $a, b, c \in \mathbb{Z}$. Si a divide a bc y además a, b son primos relativos, entonces a divide a c.*

Demostración. Tomando r, s enteros tales que $ra + sb = 1$ y multiplicando esta ecuación por c, obtenemos que $cra + sbc = c$. Luego a divide al lado izquierdo por hipótesis y entonces a divide a c. □

Teorema 1.4 (Teorema fundamental de la aritmética)**.** *Si $n \in \mathbb{N}$, $n > 1$, existen únicos $p_1, \dots, p_k$ primos y $\alpha_1, \dots, \alpha_k$ naturales positivos tales que $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$.*

Demostración. Para ver la existencia, hagamos inducción en n: para $n = 2$ el resultado es claramente cierto, y si lo hemos probado para todos los naturales hasta n, entonces $n+1$ tiene dos posibilidades: es primo (en cuyo caso él mismo es la descomposición requerida) o tiene un divisor $k < n+1$, en cuyo caso $(n+1)/k \leq n$ y podemos concluir aplicando la hipótesis inductiva sobre $(n+1)/k$ y k.

La unicidad también sigue de un argumento inductivo: si $n = q_1 \dots q_r = p_1 \dots p_l$ son dos factorizaciones primas, el lema de Euclides nos dice que q_1 divide a algún p_k y entonces $q_1 = p_k$. Cancelando q_1 de ambas factorizaciones nos remite al caso inductivo. □

En particular, el teorema anterior implica que para $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ y $m = p_1^{\beta_1} \dots p_k^{\beta_k}$ podemos escribir el mcm(n,m) y el mcd(n,m) como $p_1^{\text{máx}(\alpha_1,\beta_1)} \dots p_k^{\text{máx}(\alpha_k,\beta_k)}$ y $p_1^{\text{mín}(\alpha_1,\beta_1)} \dots p_k^{\text{mín}(\alpha_k,\beta_k)}$ respectivamente. Si n y m son grandes resulta más conveniente encontrar el mcd(n,m) vía el algoritmo de Euclides (ver ejercicio 1.4) y usar la identidad $nm = \text{mcd}(n,m)\,\text{mcm}(n,m)$ en vez de calcular la descomposición prima de n y m. Notemos que el lema de Bézout también entrega una manera eficiente de calcular los coeficientes s,t tales que $as + bt = \text{mcd}(a,b)$.

1.4. Aritmética modular

Sea $m \in \mathbb{N}\backslash\{0\}$ fijo y consideremos la relación de equivalencia en $\mathbb{Z}$ definida por $a \sim b$ ssi m divide a $b-a$. En tal caso diremos que a es congruente a b módulo m y escribiremos $a \equiv b \mod m$. Notemos que cuando $a \in \mathbb{Z}$ tenemos que existen q y r enteros tales que $a = mq + r$, con $0 \leq r < m$, y entonces $r \equiv b \mod m$. Es decir, todo número entero es congruente módulo m a un número natural menor que m. Además, si $0 \leq r < r' < m$, entonces $0 < r' - r < m$, y por lo tanto m no divide a $r'-r$, o $r \not\equiv r' \mod m$. Luego este número natural menor que m es único para cada n y $\mathbb{Z}_m = \mathbb{Z}/\sim = \{[0],[1],[2],\dots,[m-1]\}$ es el conjunto de las clases de equivalencia para esta relación.

Definamos una suma en $\mathbb{Z}_m$ por $[a]+[b]=[a+b]$. Mostremos que está bien definida: que $a' \in [a]$ y $b' \in [b]$ es equivalente a decir que existen $r,s \in \mathbb{Z}$ tal que $a' = a + mr$ y $b' = b + ms$ y por lo tanto

$$a' + b' = a + mr + b + ms = a + b + m(r+s) \in [a+b].$$

De aquí sigue que $[a'+b'] = [a+b]$. Esta suma de clases está estrechamente relacionada con la suma de $\mathbb{Z}$: es asociativa y conmutativa, la clase $[0]$ es el neutro aditivo y cada elemento $[a]$ tiene inverso $[m-a]$.

De la misma manera como definimos la suma, podemos definir la multiplicación como $[a][b] = [ab]$. Al igual que antes, veamos que esta multiplicación está bien definida: decir que $a' \in [a]$ y $b' \in [b]$ es lo mismo que decir que $a' = a + mk$ para cierto $k \in \mathbb{Z}$ y que $b' = b + mt$ para cierto $t \in \mathbb{Z}$. Por lo tanto,

$$a'b' = (a+mk)(b+mt) = ab + m(at + kb + mkt) \in [ab],$$

es decir, $[a'b'] = [ab]$. La multiplicación en $\mathbb{Z}_m$ hereda la asociatividad y la conmutatividad de $\mathbb{Z}$ y la existencia de un elemento neutro $[1]$. Sin embargo, pueden haber elementos sin inversos. Como ejemplo, la figura 1.1 muestra la tabla de la suma y de la multiplicación de $\mathbb{Z}_6 = \{[0],[1],[2],[3],[4],[5]\}$.

Notamos que $[2],[3]$, y $[4]$ no tienen inversos multiplicativos. Los únicos elementos invertibles son $[1]$ y $[5]$, y de hecho cada uno de ellos es su propio inverso. Por otro lado, la ecuación $x^2 + x = 0$ tiene como solución en $\mathbb{Z}_6$ a $[3],[2]$ y $[5]$.

Más generalmente, si $m = pq$ con $p > 1$ y $q > 1$, entonces, $p < m$ y $q < m$. Es decir, $[p] \neq [0] \neq [q]$ y sin embargo $[p][q] = [m] = 0$. Si $[p]$ tuviera inverso multiplicativo en $\mathbb{Z}_m$, existirían r y k enteros tales que $pr = 1 + km$, o $p(r-kq) = 1$. Pero no existe ningún número entero mayor que 1 que divida a 1. Por lo tanto tales r y k no existen, y entonces $[p]$ no tiene inverso multiplicativo en $\mathbb{Z}_m$. En cambio, si n y m son tales que $1 \leq n < m$ y mcd$(m,n) = 1$, entonces existen s y t enteros tales que $sm + tn = 1$, es decir, $[t]$ es el

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

×	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Figura 1.1: Operaciones en $\mathbb{Z}_6$.

inverso multiplicativo de $[n]$ en $\mathbb{Z}_m$. En resumen, un elemento no nulo en $\mathbb{Z}_m$ tiene inverso multiplicativo si y solo si es coprimo con n. El conjunto de tales elementos se denota $\mathbb{Z}_m^\times$.

1.5. Ejercicios

Ejercicio 1.1. Muestre que $m \in \mathbb{N}$ es un cuadrado perfecto en los enteros si y solo si $\sqrt{m}$ es racional.

Ejercicio 1.2. Verifique que la multiplicidad de p primo en la factorización prima de $n!$ (esto es, el mayor m tal que p^m divide a $n!$) es

$$\sum_{k\geq 1}\left\lfloor \frac{n!}{p^k} \right\rfloor.$$

Ejercicio 1.3. Definamos $\varphi : \mathbb{N} \to \mathbb{N}$ como $\varphi(n) = |\{a \leq n; \text{mcd}(a,n) = 1\}| = |\mathbb{Z}_n^\times|$. La función φ se conoce comúnmente como la *función indicatriz de Euler*.

a) Muestre directamente que $\lim_{n\to\infty} \varphi(n) = \infty$.
b) Muestre que φ es multiplicativa (es decir, si a, b son naturales primos entre sí entonces $\varphi(ab) = \varphi(a)\varphi(b)$) y que para cada p primo y a natural se tiene la igualdad $\varphi(p^a) = p^{a-1}(p-1)$.
c) Obtenga una expresión para $\varphi(n)$ en función de los factores primos de n y concluya que $\varphi(d)$ divide a $\varphi(n)$ donde d es un divisor cualquiera de n.

Ejercicio 1.4. Muestre que el algoritmo de Euclides aplicado a un par (a, b) con $a > b$ termina en $O(\log(a))$ divisiones.

Ejercicio 1.5. Sea $n = \sum_{k=0}^{m} c_k 10^k$ un entero positivo. Muestre que:

a) n es divisible por 3 ssi $\sum_k c_k$ es divisible por 3.
b) n es divisible por 9 ssi $\sum_k c_k$ es divisible por 9.
c) n es divisible por 11 ssi $\sum_k (-1)^k c_k$ es divisible por 11.

Generalice lo anterior a bases distintas de 10.

Ejercicio 1.6. Sea V un espacio vectorial no trivial sobre F cuerpo.

a) Muestre que V tiene una base.
b) Muestre que cada subconjunto linealmente independiente de V se puede extender a una base y concluya que cada subespacio W de V es un sumando directo (es decir, existe un subespacio U de V tal que $V = W \bigoplus U$).
c) Muestre que todo subconjunto generador de V contiene una base de V.

¿Es necesaria la conmutatividad de la multiplicación de F?

Ejercicio 1.7. En 1872 Dedekind publicó una construcción de los números reales a partir de los racionales distinta de la enfoque desde las secuencias de Cauchy de racionales debida a Cantor. Una ventaja de esta ruta es que el axioma del supremo se verifica directamente y que no requiere ideas de análisis. Este ejercicio sigue el esquema esbozado en el libro de Rudin [Rud64] para realizar la construcción.

Un *corte* S es un subconjunto de $\mathbb{Q}$ tal que

1. S es no vacío y no es todo $\mathbb{Q}$.
2. si $a \in S$ y $b < a$, entonces $b \in S$.
3. si $a \in S$, entonces existe algún $c \in S$ tal que $a < c$.

Definimos $\mathbb{R}$ como el conjunto de todos los cortes. Queremos ver que $\mathbb{R}$ es un cuerpo ordenado arquimediano (el ejercicio 5.3 prueba que es el único), y que la función $\iota : \mathbb{Q} \to \mathbb{R}$ definida por $\iota(q) = \{s \in \mathbb{Q}; s < q\}$ es una inyección que preserva el orden y las operaciones algebraicas (estas nociones las definiremos a lo largo del ejercicio).

a) Defina $S < L$ para $S, L \in \mathbb{R}$ como $S \subsetneq L$. Verifique que el orden inducido es total, y que cada conjunto acotado superiormente posee un supremo.
b) Para $S, L \in \mathbb{R}$ defina $S \oplus L = \{s + l; s \in S, l \in L\}$. Muestre que $S \oplus L$ es un corte y que $\oplus$ es conmutativa y asociativa.
c) Defina $\bar{0} = \iota(0)$ y dado $S \in \mathbb{R}$ defina $-S = \{p \in \mathbb{Q}; \exists\, r \in \mathbb{Q} \text{ tal que } -p - r \notin S\}$. Muestre que $\bar{0}$ es neutro para $\oplus$ y que $-S$ es el inverso aditivo de S.
Indicación: para la inclusión $\bar{0} \subset (-S) \oplus S$, tome $p \in \bar{0}$ y considere la descomposición $p = -np/2 + (n+2)p/2$ para algún $n \in \mathbb{N}$.
d) Dados $S, L > 0$, defina $S \odot L = \{p \in \mathbb{Q};\ p \leq sl \text{ para algún } s \in S,\, l \in L\}$ y extienda la definición a

$$S \odot L = \begin{cases} -(-S) \odot L & \text{si } S < \bar{0},\ L > \bar{0} \\ -S \odot (-L) & \text{si } S > \bar{0},\ L < \bar{0} \\ (-S) \odot (-L) & \text{si } S < \bar{0},\ L < \bar{0}. \end{cases}$$

Pruebe que $\odot$ es asociativa, conmutativa, tiene neutro $\bar{1} = \iota(1)$ y cada elemento tiene inverso.
Indicación: primero trate el caso $S, L > \bar{0}$ y luego use la identidad $-(-S) = S$.
e) Pruebe que $<$ es compatible con $\oplus$ y $\odot$, es decir, $S \oplus L < S \oplus P$ implica que $L < P$ y $S \odot L < S \odot P$ implica que $L < P$ siempre que $S > \bar{0}$.
f) Pruebe que $\odot$ distribuye sobre $\oplus$.
g) Muestre que para cada ι es isótona (es decir, $q < r$ ssi $\iota(q) < \iota(r)$) y realiza un monomorfismo de $(\mathbb{Q}, +, \cdot)$ en $(\mathbb{R}, \oplus, \odot)$.

¿Dónde usó que $\mathbb{Q}$ es arquimediano?

Capítulo 2

Grupos

2.1. Definiciones y ejemplos básicos

En esta sección daremos las definiciones básicas de teoría de grupos y los primeros resultados. También acordaremos algunas notaciones que no son del todo universales.

Un *grupo* es un conjunto no vacío G provisto de una operación binaria $\cdot$ (que también anotaremos por yuxtaposición) tales que:

1. $\cdot$ es asociativa.
2. G contiene un elemento neutro (usualmente llamado e o 1).
3. cada elemento g tiene inverso para $\cdot$ (usualmente escrito g^{-1}).

Si $(G,\cdot)$ sólo satisface 1 diremos que G es un *semigrupo*, y si satisface 1 y 2 diremos que G es un *monoide*. Un grupo *abeliano* es un grupo tal que $\cdot$ es conmutativa. Al tratar con estos grupos usaremos el símbolo $+$ en vez de $\cdot$, 0 en vez de 1 y $-x$ en vez de x^{-1}. Llamamos *orden* de G al cardinal de G.

La definición anterior permite unificar el tratamiento a estructuras como los enteros módulo k, las simetrías de un objeto geométrico, las curvas elípticas y los "grupos de sustituciones" que aparecen naturalmente en la teoría de Galois y que veremos en el capítulo 5.

Algunos ejemplos ya conocidos de grupos abelianos son $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ y $\mathbb{Z}_m$ (para cualquier $m \in \mathbb{N}$) al dotarlos de la suma, y $\mathbb{C}^\times$, $\mathbb{R}^\times$, $\mathbb{Q}^\times$ y $\mathbb{Z}_p^\times$ (para p primo) al dotarlos de la multiplicación. Más adelante veremos ejemplos interesantes de grupos no abelianos. Por otro lado, $\mathbb{N}$ es un ejemplo natural de monoide, y $\mathbb{N}\backslash\{0\}$ lo es de semigrupo. Dado un conjunto X, el conjunto X^X de funciones $f : X \to X$ también es un semigrupo. La construcción de un grupo a partir de un semigrupo abeliano donde cada elemento es cancelable estará implícita al ver cuerpos de cocientes en el capítulo 3.

Observación 2.1. Si x es un elemento de un grupo G tal que $xx = x$, entonces $x = xxx^{-1} = xx^{-1} = 1$. Es decir, en un grupo el 1 es el único elemento idempotente. En particular, tanto $M_2(\mathbb{R})$ como $\mathbb{Z}_6$ no son grupos con la multiplicación pues $[3]$ es idempotente en $\mathbb{Z}_6$ y $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ lo es en $M_2(\mathbb{R})$.

Si H es un conjunto no vacío contenido en un grupo G tal que bajo la operación de G es un grupo, diremos que es un *subgrupo* de G y escribiremos $H \leq G$. Los subgrupos triviales de G son G y $\{1\}$. Si $H \leq G$ y $H \neq G$, entonces diremos que H es un subgrupo propio de G y a veces escribiremos $H < G$.

Observación 2.2. Sea H un conjunto no vacío en un grupo G. Si H es cerrado bajo la operación de G, entonces la asociatividad de los elementos de H se hereda de G. Luego si H es un subconjunto de G que contiene al 1 de G, es cerrado bajo la multiplicación y tiene los inversos multiplicativos de todos sus elementos, tenemos que $H \leq G$. Es directo verificar que una condición equivalente a $H \leq G$ es que $hk^{-1} \in H$ para cada $h, k \in H$.

Ejemplo 2.1. Sea H un subgrupo no trivial de $\mathbb{Z}$, luego H contiene un menor elemento positivo a (ya que $H \neq \{0\}$). Dado $b \in H$ cualquiera, el algoritmo de la división en $\mathbb{Z}$ nos entrega m y r enteros tales que $b = ma + r$, con $0 \leq r < a$. Pero como tanto b y a están en H se tiene que $r = b + (-m)a \in H$. Si r es positivo contradecimos la minimalidad de a y por lo tanto $r = 0$. Luego para cada $b \in H$ existe un $m \in \mathbb{Z}$ tal que $b = ma$, es decir, si H es un subgrupo no trivial de $\mathbb{Z}$, entonces H es el conjunto de los múltiplos de un entero fijo. Como $\mathbb{Z}$ son los múltiplos de 1 y $\{0\}$ son los múltiplos de 0, tenemos que todo subgrupo de $\mathbb{Z}$ es de la forma $a\mathbb{Z} = \{ak;\ k \in \mathbb{Z}\}$ para algún $a \in \mathbb{Z}$.

Es directo de la definición ver que la intersección de subgrupos de un grupo G también es subgrupo de G, luego para $S \subset G$ definimos el *subgrupo generado por* S como

$$\langle S \rangle \doteq \bigcap_{S \subseteq H \leq G} H = \{x_1 \dots x_n;\ n \in \mathbb{N}, x_i \in S\}. \tag{2.1}$$

La segunda igualdad se verifica viendo que el lado derecho es efectivamente el menor subgrupo que contiene a S.

En particular, si $S = \{g\}$ entonces $\langle S \rangle$ se llama el *subgrupo cíclico generado por* g, y lo denotamos por $\langle g \rangle$ y al orden de $\langle g \rangle$ le llamamos el orden de g y lo escribimos $\mathrm{ord}(g)$. Si existe $g \in G$ tal que $G = \langle g \rangle$, entonces decimos que G es un grupo *cíclico*.

Dado $g \in G$, definimos $g^0 = 1$, e inductivamente $g^n = g\,g^{n-1}$ y $g^{-n} = (g^n)^{-1}$ para $n \in \mathbb{N}$. Una inducción directa pero engorrosa prueba que $g^n g^m = g^{n+m}$ y $(g^n)^m = g^{nm}$ cuando $n, m \in \mathbb{Z}$, y entonces de 2.1 resulta que $\langle g \rangle = \{g^n;\ n \in \mathbb{Z}\}$. En particular, $\langle g \rangle = \langle g^{-1} \rangle$.

Si g tiene orden finito, sea n el menor natural tal que $g^n = 1$ (existe pues podemos encontrar $k, k' \in \mathbb{N}$ distintos tales que $g^k = g^{k'}$). Luego $K = \{1, g, g^2, \dots, g^{n-1}\}$ es grupo: $1 \in K$, $(g^k)^{-1} = g^{n-k}$ y cuando $0 \leq k, k' < n$ entonces $g^k g^{k'} \in K$ si $k + k' < n$, y si $k + k' \geq n$ tenemos que $0 \leq k + k' - n < n$ y por lo tanto $g^k g^{k'} = g^{k+k'-n} \in K$. Como $K \subset \langle g \rangle$, obtenemos que $K = \langle g \rangle$ y $n = \mathrm{ord}(g)$.

Ejemplo 2.2.

- Si (X, d) es un espacio métrico denotamos $\mathrm{Isom}(X)$ al subgrupo de Σ_X compuesto por isometrías de X en sí mismo. Si $Y \neq \emptyset$ es un subespacio de X, definimos el *grupo de simetría de* Y como $S_X(Y) = \{\psi \in \mathrm{Isom}(X);\ \psi(Y) = Y\}$. Definamos $\mathrm{Tr}(\mathbb{R}^2)$ como el grupo de traslaciones de $\mathbb{R}^2$, $\mathrm{Rot}(\mathbb{R}^2, s)$ como el grupo de rotaciones en torno a un punto $s \in \mathbb{R}^2$ y $H = \mathrm{Tr}(\mathbb{R}^2) \cup \bigcup_{s \in \mathbb{R}^2} \mathrm{Rot}(\mathbb{R}^2, s)$. Es un

resultado de geometría que $G = H \cup \epsilon H$ donde ϵ es una reflexión cualquiera de $\mathbb{R}^2$. Además, todos los subgrupos $\mathrm{Rot}(\mathbb{R}^2, s)$ son conjugados entre sí.

- Para $n \in \mathbb{N}$ definimos D_{2n}, el *grupo diedral de orden* $2n$, como el grupo de simetrías de un n-ágono regular P_n. El orden de D_{2n} es efectivamente $2n$, pues éste está compuesto por n rotaciones en $0, 2\pi/n, 4\pi/n, \ldots, 2(n-1)\pi/2$ radianes junto con n rotaciones en torno a las líneas de simetría de P_n (si n es impar, cada línea de simetría pasa por un vértice y el punto medio del lado opuesto a éste; si n es par, entonces hay $n/2$ líneas de simetría que unen vértices opuestos y $n/2$ que bisectan lados opuestos). Podemos ver que éstas son las únicas simetrías de P_n notando que una simetría queda determinada por su acción sobre un vértice fijo y su vecino izquierdo. Si ρ es la rotación en $2\pi/n$ radianes y ϵ es una reflexión en torno a alguna de las líneas de simetría de P_n, entonces es directo verificar que $|\rho| = n$, $|\epsilon| = 2$, $\epsilon\rho = \rho^{-1}\epsilon$ y $D_{2n} = \{1, \rho, \rho^2, \ldots, \rho^{n-1}, \epsilon, \epsilon\rho, \epsilon\rho^2, \ldots, \epsilon\rho^{n-1}\}$.

Cuando $H \leq G$ tenemos que la relación $g \sim k \iff k^{-1}g \in H$ es una relación de equivalencia en G: $\sim$ es refleja pues $gg^{-1} = 1 \in H$ para cada $g \in G$. Por otra parte $g \sim k$ es equivalente a $k^{-1}g \in H$ y como H es subgrupo de G, se tiene que $g^{-1}k = (k^{-1}g)^{-1} \in H$, es decir $k \sim g$ y vemos que $\sim$ es simétrica. Además, si $g \sim k$ y $k \sim t$, como H es subgrupo de G se tiene que $(t^{-1}k)(k^{-1}g) = t^{-1}(kk^{-1})g = t^{-1}g \in H$ y entonces $g \sim t$. Luego $\sim$ es transitiva. Por lo tanto $\sim$ efectivamente es una relación de equivalencia, y reescribir las implicancias anteriores en reversa muestra que $\sim$ es relación de equivalencia ssi $H \leq G$.

Al cardinal del conjunto cociente G/H se le llama *índice* de H en G y lo denotamos por $|G : H|$ o $[G : H]$. La clase de $g \in G$ es la *traslación derecha por* H dada por $gH = \{gh;\ h \in H\}$, y notando que la función $\phi : H \to gH$ definida por $\phi(h) = gh$, es inyectiva (pues G es grupo) y epiyectiva (por definición), obtenemos que $|H| = |gH|$. Luego hemos probado el siguiente resultado.

Teorema 2.1 (Teorema de Lagrange)**.** *Si G es grupo y H es subgrupo de G, entonces $|G| = |H|[G : H]$. En particular, el orden de un subgrupo de un grupo finito divide al orden del grupo.*

Observación 2.3. Si $K \leq H \leq G$, entonces

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \times \frac{|H|}{|K|} = [G : H] \times [H : K]$$

Si G es infinito el resultado sigue siendo cierto al considerarlo como una igualdad de cardinales.

Observación 2.4. El teorema de Lagrange muestra que cuando G es finito y $g \in G$, entonces $\mathrm{ord}(g)$ divide a $|G|$. En particular, $g^{|G|} = 1$ y si $|G| = p$ es primo, entonces cualquier elemento $g \neq 1$ genera G. Luego todos los grupos de orden primo son cíclicos.

Por otro lado, si $g \neq 1$ y $g^p = 1$ con p primo, necesariamente $\mathrm{ord}(g) = p$.

Ejemplo 2.3. Dado $m \in \mathbb{N}$ definimos (como en el ejercicio 1.3) la función $\varphi(n) = |\mathbb{Z}_m^\times|$. Por la observación anterior, para cada $[x] \in \mathbb{Z}_m^\times$ se tiene que $x^{\varphi(m)} \equiv 1 \mod m$. Si p es primo, lo anterior se reduce a que si $x \in \mathbb{Z}$ y p no divide a x entonces $x^{p-1} \equiv 1 \mod p$. Este resultado se conoce como el pequeño teorema de Fermat.

Ejemplo 2.4. Sea G un grupo tal que cada elemento verifica $x^2 = 1$. Entonces si $x, y \in G$ se tiene que $(xy)^2 = 1 = x^2y^2$, de modo que multiplicando por x por la izquierda y por y por la derecha concluimos que $yx = xy$. Luego G es abeliano.

En particular, consideremos G un grupo de orden 4. Si en G hay un elemento x de orden 4 entonces $G = \langle x \rangle$. Si G no tiene elementos de orden 4 entonces todos sus elementos distintos del neutro tienen orden 2 y concluimos que G es abeliano. Es decir, todo grupo de orden 4 es abeliano (y es isomorfo a $\mathbb{Z}_4$ o el grupo de Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$).

Ahora queremos dotar a los cocientes G/H de una estructura de grupo de manera que la proyección canónica $\pi\colon g \mapsto gH$ sea morfismo. La única forma de hacerlo es definir $(gH)(kH) = (gk)H$, pero un problema que surge es que esta asignación puede no estar bien definida. Una condición necesaria y suficiente para que lo esté es que $gH = Hg$, o $gHg^{-1} = H$ para cada $g \in G$. Notando que g^{-1} recorre todo G si g lo hace, lo anterior es equivalente a que $gHg^{-1} \subseteq H$ para todo $g \in G$.

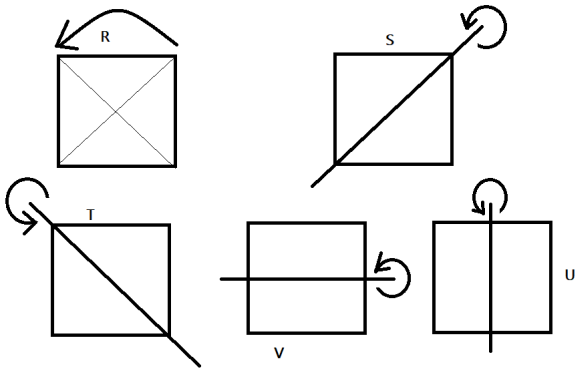
Decimos entonces que un subgrupo H de G es *normal* o *distinguido* en G si esta última condición se cumple, y en tal caso escribimos $H \lhd G$. Claramente todo subgrupo de un grupo abeliano es normal, pero un subgrupo abeliano de un grupo cualquiera no necesariamente lo es, como lo muestra el ejemplo 2.5. Si G es un grupo que no tiene subgrupos normales salvo $\{1\}$ y G, se dice que G es *simple*.

En el caso en que H es normal en G se verifica de manera inmediata que el *grupo cociente* G/H es efectivamente un grupo, con neutro H e inversos $g^{-1}H$ para cada $gH \in G/H$.

Observación 2.5.

- Si $H \leq G$ tiene índice 2 en G entonces es normal, pues cuando $g \notin H$ tenemos que $gH = Hg = G \setminus H$ y cuando $g \in H$ se tiene directamente que $gH = H = Hg$.
- De la misma manera que definimos en un grupo G las traslaciones derechas por un subgrupo H, podemos definir las *traslaciones izquierdas* como el conjunto $H\backslash G$ de clases de equivalencia de la relación $\sim'=\sim^{-1}$ dada por $g \sim' k$ ssi $kg^{-1} \in H$. Las clases de equivalencia resultantes son de la forma Hg con $g \in G$. Una condición suficiente para que $G/H = H\backslash G$ es que H sea normal en G, y es un ejercicio ver que esta condición también es necesaria.

Ejemplo 2.5. Si G es un grupo y N es un subgrupo normal de G y H un subgrupo de G que contiene a N, entonces N es normal en H. Sin embargo, la cadena de afirmaciones $K \lhd H \lhd G$ no necesariamente implica que $K \lhd G$: consideremos el grupo de simetrías del cuadrado $D_4 = \{\mathrm{id} = 1, R, R^2, R^3, S, T, U, V\}$ donde R es la rotación en un ángulo recto y como centro la intersección de las diagonales del cuadrado. La rotación en un ángulo extendido es R^2 y la rotación en un ángulo de $3\pi/2$ es R^3. La reflexión respecto a una de las diagonales es S y la reflexión respecto a la otra diagonal es T. Las reflexiones respecto a la recta que pasa por los puntos medios de lados paralelos las denotamos por U y V. Es claro que $S^2 = T^2 = U^2 = V^2 = (R^2)^2 = 1$.



Numeremos las esquinas del cuadrado en sentido contrarreloj, de manera que a cada una de las simetrás del cuadrado la podemos ver como una permutación de $\{1,2,3,4\}$. Así R transforma $1 \to 2$, $2 \to 3$, $3 \to 4$ y $4 \to 1$. Es decir, R visto en Σ_4 es (1234). Del mismo modo R^2 visto en Σ_4 es (13)(24) y R^3 es (1432). En este mismo sentido, S es (24), T corresponde a (13), U a (12)(34) y V a (14)(23). Por tanto podemos pensar D_4, llamado el grupo diedral de orden 8, como subgrupo de Σ_4.

El conjunto $V_4 = \{1,(13)(24),(12)(34),(14)(23)\}$ es un subgrupo de D_4 llamado el grupo de Klein (que es isomorfo al grupo de simetrías del rectángulo no cuadrado). Como el índice de V_4 en D_4 es 2, entonces $V_4 \lhd D_4$ Además $H = \{1,(12)(34)\}$ es un subgrupo de V_4. Nuevamente $H \lhd V_4$ pues $[V_4 : H] = 2$. Pero $(1234)(12)(34)(1234)^{-1} = (1234)(12)(34)(1432) = (14)(23) \notin H$. Es decir, H no es normal en D_4 pese a que $H \lhd V_4 \lhd D_4$

Ejemplo 2.6. Si X es un conjunto cualquiera, el conjunto de todas las biyecciones de X en si mismo con la operación composición es un grupo, llamado el *grupo de permutaciones* de X, cuyo neutro es la función id_X. A tal grupo lo denotaremos por Σ_X. Si existe una biyección $\phi : X \to Y$ entonces para cada $\sigma \in \Sigma_X$ la función $\Phi(\sigma) = \phi \circ \sigma \circ \phi^{-1}$ es un elemento de Σ_Y y define un isomorfismo entre Σ_X y Σ_Y. Es decir, el grupo de permutaciones solo depende de la cardinalidad de X y no de sus elementos, en particular, si $|X| = n$, entonces Σ_X lo denotamos por Σ_n y sin restricción podemos pensar que $X = \{1,2,3,4,\ldots,n\}$. El orden de Σ_n es $n!$.

Si $X = \{1,2,3,\ldots,n\}$ y $\sigma \in \Sigma_n$, entonces escribiremos

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}.$$

Los seis elementos de Σ_3 son:

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Si $\sigma \in \Sigma_n$ es tal que $\sigma(k_1) = k_2$, $\sigma(k_2) = k_3$, $\sigma(k_3) = k_4, \ldots \sigma(k_r) = k_1$, y σ funciona como la identidad en el resto de elementos de $\{1, 2, 3, \ldots n\}$ entonces también escribiremos σ como $(k_1 k_2 k_3 k_4 \ldots k_r)$ y lo llamaremos un ciclo de largo r. Según esta notación (y escribiendo la identidad como 1), tenemos que $\Sigma_3 = \{(1), (12), (13), (23), (123), (132)\}$. Notamos que $\{1, (12)\}$, $\{1, (13)\}$ y $\{1, (23)\}$ son los únicos subgrupos de orden 2 y $H = \{1, (123), (132)\}$ es el único subgrupo de orden 3. Como el índice de H en G es 2, necesariamente $H \lhd G$.

Además notemos que $(12)(13) = (132)$ y en cambio $(13)(12) = (123)$, por lo tanto Σ_3 no es conmutativo. Más aún, si $n \geq 3$ consideremos los ciclos de largo 2 (12) y (13) en Σ_n, entonces $(12)(13) \neq (13)(12)$. Es decir, Σ_n no es abeliano para $n \geq 3$. Además $\Sigma_2 = \{1, (12)\}$ y $\Sigma_1 = \{1\}$, ambos claramente abelianos. Concluimos que Σ_n es conmutativo si y solo si $n = 1$ o $n = 2$.

Si H y K son subgrupos de un grupo G, el conjunto $KH = \{kh;\ k \in K,\ h \in H\}$ no es necesariamente un subgrupo de G. Por ejemplo, $H = \{1, (12)\}$ y $K = \{1, (23)\}$ son subgrupos de Σ_3 y $KH = \{1, (23), (12), (132)\}$ no lo es. El siguiente resultado da condiciones necesarias y suficientes para que KH sea un subgrupo de G.

Proposición 2.1. *Si H y K son subgrupos de G, entonces KH es subgrupo de G si y solamente si $KH = HK$.*

Demostración. Supongamos que $KH \leq G$ y sean $k \in K$ y $h \in H$. Luego $k^{-1}h^{-1} \in KH$ y como KH es un grupo, se tiene que $hk = (k^{-1}h^{-1})^{-1} \in KH$ luego $HK \subseteq KH$. Por otro lado, tomemos $z \in KH$ y sea $w = z^{-1} \in KH$ (ya que $KH \leq G$). Como $w = kh$ para ciertos $k' \in K$ y $h' \in H$, entonces $z = w^{-1} = (k'h')^{-1} = h'^{-1}k'^{-1} \in HK$. Concluimos que $HK = KH$.

Ahora supongamos que $KH = HK$. Como H y K contienen a 1, entonces $1 \in HK$. Sean ahora $k, k' \in K$ y $h, h' \in H$, luego $kh(k'h')^{-1} = khh'^{-1}k' = kk''h'' \in KH$ para ciertos $k'' \in K$, $h'' \in H$, pues $hh'^{-1}k' \in HK = KH$. Luego $KH \leq G$. □

Corolario 2.1. *Si G es un grupo, $H \leq G$ y $N \lhd G$, entonces $NH \leq G$.*

Demostración. Como N es normal, para cada $g \in H$ se tiene que $gN = Ng$, y por ende $HN = NH$. El resultado anterior prueba que que $NH \leq G$. □

Proposición 2.2. *Si H, K son subgrupos finitos de un grupo G, entonces $|HK||N \cap K| = |N||H|$.*

Demostración. Notemos que $A = H \cap K$ es un subgrupo de K de índice $n \doteq |K|/|H \cap K|$. Luego podemos escribir K como la unión disjunta $K = \bigcup_{i \in [n]} k_i A$ para ciertos $k_i \in K$, y como $AH = H$, obtenemos que $HK = \bigcup_{i \in [n]} k_i H$, de manera que $|HK| = n|H| = |H||K|/|H \cap K|$. □

Si G es un grupo, el conjunto de los elementos que conmutan con todos los elementos de G se llama el *centro* de G y se anota por $Z(G)$ (o simplemente Z si el grupo está subentendido), esto es, $Z(G) = \{x \in G;\ xg = gx\ \ \forall g \in G\}$. Definimos también el *centralizador* de $g \in G$ por $C_G(g)$ (o $C(g)$) como el conjunto de elementos de G que conmutan con g, o $C_G(g') = \{g \in G;\ gg' = g'g\}$. Se verifica que ambos conjuntos son subgrupos de G, el centro de G es normal en éste y se tiene que $Z(G) = \bigcap_{g \in G} C_G(g)$.

Sean G, G' grupos. Una función $f: G \to G'$ se dice *morfismo de grupos* si se cumple la condición enunciada en la sección 1.1, es decir $f(gh) = f(g)f(h)$ para cada $g,h \in G$. Es inmediato ver que $f(1)$ es idempotente en G', y entonces la observación 2.1 muestra que $f(1)$ es el neutro de G'. Por otro lado, $f(g)f(g^{-1}) = f(1)$ implica que $f(g)^{-1} = f(g^{-1})$ para todo $g \in G$.

El conjunto $\ker(f) \doteq \{g \in G / \ f(g) = 1'\} = f^{-1}(\{1'\})$, llamado *kernel* de f, es un subgrupo de G pues $1 \in \ker(f)$ y para $x, y \in \ker(f)$, $f(xy^{-1}) = f(x)f(y)^{-1} = 1'$. Además es normal en G ya que $f(gxg^{-1}) = f(g)1'f(g)^{-1} = 1'$ cuando $x \in \ker(f)$, $g \in G$ (y el mismo razonamiento muestra que la preimagen de subgrupos normales es también subgrupo normal). Como veremos ahora, los únicos subgrupos normales son de este tipo.

Proposición 2.3. *Todo subgrupo normal es el kernel de algún morfismo.*

Demostración. Sea $H \lhd G$ y consideremos el grupo cuociente G/H. Para concluir basta notar que la proyección canónica $\pi: G \to G/H$ definida por $\pi(g) = gH$ es un morfismo cuyo kernel es H. □

Cuando $\ker(f) \neq \{1\}$, f no puede ser inyectiva y recíprocamente, si $\ker(f) = \{1\}$, entonces para cada $x, y \in G$ la igualdad $f(x) = f(y)$ implica que $xy^{-1} \in \ker(f)$ y por lo tanto $xy^{-1} = 1$, o $x = y$. Luego f es inyectiva ssi $\ker(f) = \{1\}$.

Si $f : G \to G'$ es morfismo de grupos, el conjunto $\mathrm{im}(f) = \{f(g);\ g \in G\} = f(G)$ también es un subgrupo de G ya que $1' = f(1) \in \mathrm{im}(f)$ y si $x, y \in \mathrm{im}(f)$, podemos encontrar $g,h \in G$ tales que $f(g) = x$ y $f(h) = y$. Luego $xy^{-1} = f(gh^{-1}) \in \mathrm{im}(f)$. Similarmente, la imagen de cualquier subgrupo de G también es un subgrupo de G' y si $H \lhd K \leq G$, entonces $f(H) \lhd f(K) \leq G$. Sin embargo, $\mathrm{im}(f)$ no necesariamente es normal en G'.

Ejemplo 2.7. Si $G = \langle g \rangle$ es un grupo cíclico infinito, definamos el epimorfismo $\phi: \mathbb{Z} \to G$ por $\phi(n) = g^n$. Esta función también es inyectiva, pues si existe $n \in \ker(\phi)$ entonces $g^n = 1$ y $n = 0$ ya que g tiene orden infinito. Luego salvo isomorfismo, $\mathbb{Z}$ es el único grupo cíclico infinito.

Dado un grupos G, el conjunto de sus automorfismos $\mathrm{Aut}(G)$ es un grupo al dotarlo de la composición de funciones. Para cada $g \in G$, la función (llamada *conjugación por* g) $f_g: G \to G$ definida por $f_g(x) = gxg^{-1}$ es un automorfismo con inversa $f_{g^{-1}}$. Si definimos $\Psi: G \to \mathrm{Aut}(G)$ por $\Psi(g) = f_g$, entonces cuando $g, g', x \in G$ tenemos que $\Psi(g) \circ \Psi(g')(x) = g(g'xg'^{-1})g^{-1} = (gg')x(gg')^{-1} = \Psi(gg')(x)$. Luego Ψ es morfismo. La imagen de G por Ψ se conoce como el grupo de *automorfismos interiores* de G y se escribe $\mathrm{Inn}(G)$. Cuando $\alpha \in \mathrm{Aut}(G)$, la igualdad $\alpha \circ f_g \circ \alpha^{-1} = f_{\alpha(g)}$ muestra que $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

Un subgrupo H de un grupo G que es $\mathrm{Aut}(G)$-invariante, esto es, $\sigma(H) \subseteq H$ para cada $\sigma \in \mathrm{Aut}(G)$, se dice *característico*. Notemos que si H es finito, entonces lo anterior es equivalente a $\sigma(H) = H$, y si H es el único subgrupo de orden $|H|$ en G, necesariamente H es característico.

Proposición 2.4. *Si $H \lhd G$ y K es característico en H, entonces K es normal en G.*

Demostración. Sea f_g un automorfismo interior de G cualquiera. Como H es normal, f_g define un automorfismo de H por restricción. Sea $\tau \in \mathrm{Aut}(H)$ esa restricción y notemos que como K es característico en H se tiene que $\tau(K) \subseteq K$ o $gKg^{-1} \subseteq K$. □

2.2. Teoremas de isomorfismo

Ahora veremos resultados que permiten probar que ciertos grupos son isomorfos a otros y que además entregan isomorfismos canónicos en esos casos. Mostraremos teoremas idénticos a éstos para otras estructuras algebraicas en los capítulos 3 y 4, y en éste último daremos una demostración alternativa del primer y tercer teorema de isomorfismo.

Teorema 2.2 (Teorema del factor)**.** *Si $f : G \to H$ es morfismo, $N \lhd G$ y $N \subseteq \ker(f)$, la función $\bar{f} : G/N \to H$ dada por $aN \mapsto f(a)$ está bien definida y es morfismo. La ecuación $\bar{f} \circ \pi = f$ caracteriza únicamente a $\bar{f}$. Además,* $\mathrm{im}(\bar{f}) = \mathrm{im}(f)$ *y* $\ker(\bar{f}) = \ker(f)/N$.

Demostración. Notemos que $\bar{f} \circ \pi = f$ implica que $\bar{f}(aN) = f(a)$, luego $\bar{f}$ es única con esta propiedad. Veamos que es función: si $b \in aN$, entonces $b = an$ con $n \in N \leq \ker(f)$ y luego $f(b) = f(a)f(n) = f(a)$, de modo que $\bar{f}$ está bien definida. Como

$$\bar{f}(aN\,bN) = \bar{f}(abN) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN),$$

$\bar{f}$ también es morfismo. Es claro que $\mathrm{im}(\bar{f}) = \mathrm{im}(f)$, y

$$aN \in \ker(\bar{f}) \iff \bar{f}(aN) = f(a) = e \iff a \in \ker(f)$$

muestra que $\ker(\bar{f}) = \ker(f)/N$. □

Podríamos aplicar el teorema del factor para probar la próxima proposición de forma inmediata, pero preferimos dar una demostración que explicite el isomorfismo requerido.

Teorema 2.3 (Primer teorema de isomorfismo)**.** *Si $\tau : G \to G'$ es un morfismo de grupos, entonces $G/\ker(\tau)$ es isomorfo a* $\mathrm{im}(\tau)$.

Demostración. Denotemos por $K = \ker(\tau)$ y definamos $\tilde{\tau} : G/K \to \mathrm{im}(\tau)$ por $\tilde{\tau}(gK) = \tau(g)$, que está bien definida ya que cuando $gK = g'K$, existe $k \in \ker(\tau)$ tal que $g' = gk$ y por lo tanto

$$\tilde{\tau}(g'K) = \tau(g') = \tau(gk) = \tau(g)\tau(k) = \tau(g) = \tilde{\tau}(gK)$$

pues $\tau(k) = 1$. Luego $\tilde{\tau}$ es efectivamente una función, que por la definición de $\mathrm{im}(\tau)$ es epiyectiva. Es directo verificar que $\tilde{\tau}$ es morfismo, y si tomamos $gK \in \ker(\tilde{\tau})$, entonces $\tau(g) = 1$ y $gK = K$. Luego $K = Ker(\tilde{\tau})$ de modo que $\tilde{\tau}$ es inyectiva. Concluimos que $\tilde{\tau}$ es isomorfismo. □

Ejemplo 2.8. En la sección anterior definimos $\Psi : G \to \mathrm{Aut}(G)$ por $\psi(g) = f_g$ donde f_g es la conjugación por g, y vimos que es un morfismo de grupos y además $\mathrm{im}(\Phi) = \mathrm{Inn}(G)$. Por otra parte, las igualdades

$$\ker(\Psi) = \{g \in G;\ f_g = \mathrm{id}_G\} = \{g \in G;\ f_g(x) = x\ \forall x \in G\} = \{g \in G/\ gx = xg\ \forall x \in G\} = Z(G)$$

y el primer teorema de isomorfismo muestran que $G/Z(G) \cong \mathrm{Inn}(G)$.

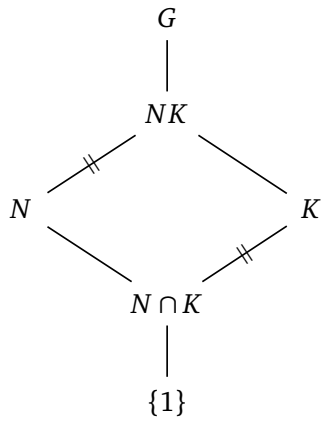


Figura 2.1: Diagrama de Hasse de los subgrupos involucrados en el segundo teorema de isomorfismo. Los cocientes de los grupos en cada extremo de las líneas marcadas son isomorfos.

Ejemplo 2.9. Sea $G = \langle g \rangle$ un grupo cíclico finito. Como en el ejemplo 2.7 definamos $\phi(n) = g^n$ de $\mathbb{Z}$ en G. Además sabemos que ϕ no es inyectivo y por lo tanto existe m entero positivo tal que $m\mathbb{Z} = \ker(\phi)$. Por el primer teorema del isomorfismo se tiene que $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} \cong G$. Como $\mathbb{Z}_m \cong \mathbb{Z}_n$ ssi $n = m$, obtenemos que para cada $m \in \mathbb{N}$ existe un único grupo cíclico, salvo isomorfismos, de orden m.

Los dos siguientes teoremas son corolarios del primer teorema de isomorfismo. El diagrama de Hasse de un grupo es una manera de visualizar la estructura de subgrupos de éste. La figura 2.1 muestra el diagrama asociado a los grupos involucrados en el segundo teorema de isomorfismo.

Teorema 2.4 (Segundo teorema de isomorfismo)**.** *Sean K y N subgrupos de G, con N normal en G. Entonces NK es un subgrupo de G, $N \cap K$ es normal en K y además $K/(N \cap K)$ es isomorfo a NK/N.*

Demostración. Como N es normal en G, entonces $NK \leq G$ por el corolario 2.1. Además, la igualdad $NK = KN$ implica que cada clase $nkN \in NK/N$ se puede escribir como $k'N$ con $k' \in K$. Luego la función $\rho : K \to NK/N$ definida por $\rho(k) = kN$ es una sobreyección y dado que N es normal,

$$\rho(kk') = kk'N = (kN)(k'N) = \rho(k)\rho(k')$$

muestra que es ρ es morfismo. Por otra parte

$$\ker(\rho) = \{k \in K;\, kN = N\} = N \cap K$$

implica que $N \cap K \lhd K$, y el primer teorema de isomorfismo permite concluir que $K/(N \cap K) \cong NK/N$. □

Teorema 2.5 (Tercer teorema de isomorfismo)**.** *Sean K y H subgrupos normales de G tales que $K \leq H$. Entonces H/K es un subgrupo normal de G/K y además $(G/K)/(H/K)$ es isomorfo a G/H.*

Demostración. Primero que nada, notemos que $gK = g'K$ es equivalente a decir que existe $k \in K \subseteq H$ tal que $g' = gk$ y por lo tanto $gH = g'H$. Luego la función $\eta\colon G/K \to G/H$ definida por $\eta(gK) = gH$ está bien definida y es epiyectiva por definición. Por otro lado,

$$\eta((gK)(g'K)) = \eta(gg'K) = gg'H = gHg'H = \eta(gK)\eta(g'K)$$

de modo que η también morfismo. Finalmente,

$$\ker(\eta) = \{gK \in G/K;\ gH = H\} = \{gK \in G/K;\ g \in H\} = H/K$$

implica que H/K es normal en G/K y el primer teorema del isomorfismo muestra que $(G/K)/(H/K) \cong G/H$. □

Notemos que en la demostración anterior, el subgrupo $\ker(\eta)$ resultó ser K/H, donde η era un morfismo de G/H en otro grupo y $H \leq K \leq G$. La pregunta natural que surge es si todos los subgrupos de G/H tienen esa forma, y la respuesta es afirmativa.

Teorema 2.6 (Teorema de correspondencia)**.** *Si $H \lhd G$, los subgrupos de G/H son exactamente los grupos de la forma K/H donde $K \leq H$. Es decir, la proyección canónica $\pi\colon G \to G/H$ se extiende a la biyección de grupos $\bar{\pi}\colon \{K; H \leq K \leq G\} \to \{Q; Q \leq G/H\}$. Además, para cada $A,B \leq G$ con $N \leq A,B$, se tiene que $\bar{\pi}$ verifica:*

1. *$A \leq B$ ssi $\bar{\pi}(A) \leq \bar{\pi}(B)$.*
2. *si $A \leq B$, entonces $[B : A] = [\bar{\pi}(B) : \bar{\pi}(A)]$.*
3. *$\bar{\pi}(\langle A,B\rangle) = \langle \bar{\phi}(A), \bar{\pi}(B)\rangle$.*
4. *$\bar{\pi}(A \cap B) = \bar{\pi}(A) \cap \bar{\pi}(B)$.*
5. *$A \lhd G$ ssi $\bar{\pi}(A) \lhd G/N$.*

Demostración. Como π es morfismo obtenemos que $\pi(K) \leq G/H$ cuando $H \leq K \leq G$, y si $Q \leq G/H$ entonces $\pi^{-1}(Q) \leq G$ y además $H = \pi^{-1}(\{H\}) \leq \pi^{-1}(Q)$. Luego $\bar{\pi}$ está bien definida. La sobreyectividad de π asegura que $\pi(\pi^{-1}(Q)) = Q$ para cada $Q \leq G/H$. Por otro lado, siempre se cumple que $\pi^{-1}(\pi(K)) \supseteq K$ cuando $K \subseteq G$. Veamos que si $H \leq K \leq G$ se tiene la otra inclusión $\pi^{-1}(\pi(K)) \subseteq K$: si $s \in G$ es tal que $\pi(s) \in \pi(K)$, entonces existe un $k \in K$ tal que $\pi(s) = \pi(k)$, es decir $s \in kH$. Ahora bien, la afirmación $H \leq K$ muestra que $s \in K$, y podemos concluir que $\pi^{-1}(\pi(K)) = K$. Luego $\bar{\pi}$ es biyección.

Las afirmaciones 1–5 son el ejercicio 2.1. □

Ejemplo 2.10. Notemos que si $n, m \in \mathbb{Z}$, el segundo teorema de isomorfismo nos dice que $n\mathbb{Z} + m\mathbb{Z}/m\mathbb{Z} \cong n\mathbb{Z}/n\mathbb{Z} \cap m\mathbb{Z}$. El lema de Bézout implica que $n\mathbb{Z} + m\mathbb{Z} = \operatorname{mcd}(n,m)\mathbb{Z}$ y la definición de mcm muestra que $n\mathbb{Z} \cap m\mathbb{Z} = \operatorname{mcm}(n,m)\mathbb{Z}$. Luego $\operatorname{mcd}(n,m)\mathbb{Z}/m\mathbb{Z} \cong n\mathbb{Z}/\operatorname{mcm}(n,m)\mathbb{Z}$. En el próximo capítulo veremos que también son isomorfos como anillos.

Por otro lado, el teorema de correspondencia prueba que todos los subgrupos de $\mathbb{Z}_n$ son de la forma $m\mathbb{Z}/n\mathbb{Z}$ donde $n\mathbb{Z} \subseteq m\mathbb{Z}$ o equivalentemente donde m divide a n. Entonces el tercer teorema de isomorfismo prueba que $\mathbb{Z}_n/(m\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$. Por lo tanto, todos los subgrupos de un subgrupo cíclico también son cíclicos.

2.3. Acción de grupos

Sea X un conjunto y G un grupo. A una función $G \times X \to X$, denotada por yuxtaposición, se llama una *acción* de G en X si se tiene las siguientes condiciones:

1. $1x = x$ para cada $x \in X$.
2. $g'(gx) = (g'g)x$ para cada $g, g' \in G$ y $x \in X$.

También diremos que X es un *G-conjunto* en tal caso. Esta noción precisa la intuición de que muchos grupos nacen como transformaciones biyectivas de ciertos conjuntos. Los ejemplos naturales son los grupos diedrales D_{2n} y los grupos de permutaciones Σ_n, quienes actúan sobre los vértices (o las aristas, o las diagonales) de un n-ágono regular y sobre $[n]$ respectivamente. Un cuerpo $\mathbb{K}$ actúa sobre un $\mathbb{K}$-espacio vectorial y sobre el conjunto de sus subespacios vectoriales a través de la ponderación.

Una definición equivalente de una acción es un morfismo $\psi\colon G \to \Sigma_X$, ya que a partir de éste podemos definir la acción $G \times X \to X$ por $(g, x) \mapsto \psi(g)(x)$. Como ψ es morfismo, tenemos que $g'(gx) = \psi(g') \circ \psi(g)(x) = \psi(g'g)(x) = (g'g)x$ y también $\psi(1)(x) = \mathrm{id}_X(x) = x$. Luego la función que definimos es efectivamente una acción. Recíprocamente, dada una acción de G en X podemos definir un morfismo $\psi\colon G \to \Sigma_X$ vía $\psi(g)(x) = gx$. Las igualdades anteriores muestran que ψ es efectivamente un morfismo y además tenemos que ψ está bien definido, ya que $\psi(g)$ tiene inversa $\psi(g^{-1})$. Un tal ψ se dice *representación por permutaciones* de G.

El kernel de ψ se llama el *kernel de la acción*, y ésta se dice *fiel* si su kernel es la identidad. Notemos que $\ker(\psi)$ es normal. Si para $x \in X$ definimos el *estabilizador* de x o el *grupo de isotropía* de x como $\mathrm{Stab}(x) \doteq \{g \in G;\ gx = x\}$, entonces éste resulta ser subgrupo de G: $1x = x$ muestra que $1 \in \mathrm{Stab}(x)$ y además si $g, g' \in \mathrm{Stab}(x)$, entonces $(gg'^{-1})x = g(g'^{-1}x) = gx = x$, (ya que $x = (g'^{-1}g')x = g'^{-1}x$). Luego $\mathrm{Stab}(x) \leq G$. Las definiciones involucradas implican inmediatamente que $\ker(\psi) = \bigcap_{x \in X} \mathrm{Stab}(x)$.

Ejemplo 2.11. Sea G un grupo finito y H un subgrupo de índice p donde p es el menor primo que divide a G. Entonces H es normal en G.

Demostración. Sea Ω el conjunto de todas las clases laterales izquierdas de H en G, de modo que $|\Omega| = p$. Hagamos actuar G en Ω por multiplicación izquierda, es decir definimos para cada $g' \in G$ definimos $\tau_{g'}$ de Ω en si mismo por $\tau_{g'}(gH) = g'(gH) = (g'g)H$. Luego $\phi\colon G \to \Sigma_\Omega$ dada por $g' \mapsto \tau_{g'}$ es morfismo. Notemos que el kernel de esta acción es $\ker(\phi) = K = \{x \in G;\ xgH = gH\ \forall g \in G\}$ y está contenido en H pues si $x \in K$, en particular $xH = H$, y además K es normal en G dado que es el kernel de un homomorfismo. El primer teorema de isomorfismo muestra que G/K es isomorfo a un subgrupo de Σ_p y luego $[G : K]$, que es un divisor de $|G|$, también divide a $p!$.

Ahora $[G : K] = [G : H][H : K] = pq$ donde $q = [H : K]$. Como $[G : K]$ es un divisor de $p!$, tenemos que q es un divisor de $(p-1)!$. Entonces si r es un divisor primo de q, necesariamente $r < p$, pero esto contradice la minimalidad de p pues r divide a $[H : K]$ y $[H : K]$ divide a $|G|$. Por lo tanto tal r no existe y $q = 1$, es decir $[H : K] = 1$. Luego $H = K$ y H es normal en G. □

Teorema 2.7 (Teorema de Cayley)**.** *Todo grupo G es isomorfo a un subgrupo de $\Sigma_{|G|}$.*

Demostración. Consideremos la acción de G sobre sí mismo por multiplicación izquierda, es decir definimos $\Psi\colon G \to \Sigma_G$ por $\Psi(g)(x) = gx$ cuando $g, x \in G$. Por definición Ψ es morfismo, y la acción es fiel pues $\Psi(g) = \Psi(g')$ implica que en particular $g = \Psi(g)(1) = \Psi(g')(1) = g'$. Luego $G \leq \Sigma_G \cong \Sigma_{|G|}$. □

Si G actúa en X, esta acción define una relación de equivalencia en X, a saber $x \sim x'$ ssi existe $g \in G$ tal que $x' = gx$. La clase de equivalencia de $x \in X$, llamada la *órbita* de x, es $\mathrm{Orb}(x) \doteq Gx = \{gx;\ g \in G\}$ y el conjunto cociente bajo esta relación se escribe X/G. Una acción se dice *transitiva* si $\mathrm{Orb}(x) = X$, es decir, si para cada $x, y \in X$ existe un $g \in G$ tal que $x = gy$.

Proposición 2.5. *La órbita de $x \in X$ tiene tantos elementos como clases laterales de* $\mathrm{Stab}(x)$ *en G. En particular, si G es finito entonces la órbita de x también lo es y* $|\mathrm{Orb}(x)| = |G|/|\mathrm{Stab}(x)|$.

Demostración. Denotemos por Y al conjunto de todas las clases laterales izquierdas de $\mathrm{Stab}(x)$ en G (recordemos que $|Y| = [G : \mathrm{Stab}(x)]$) y sea $H = \mathrm{Stab}(x)$.

Definamos $\mu : \mathrm{Orb}(x) \to Y$ por $\mu(gx) = gH$. La función μ está bien definida, pues si $gx = g'x$, entonces $g'^{-1}gx = 1x = x$, y $g'^{-1}g \in H = \mathrm{Stab}(x)$, que es equivalente a decir que $gH = gH$. Además la definición de μ implica que ésta es epiyectiva. Por otro lado, si $\mu(gx) = \mu(g'x)$ tenemos que $gH = g'H$, es decir, existe $h \in H = \mathrm{Stab}(x)$ tal que $g' = gh$ y entonces $g'x = (gh)x = g(hx) = gx$. Por lo tanto μ es biyectiva y $|\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)]$. □

Sea G un grupo y hagamos actuar G en si mismo por conjugación, es decir $(g, g') \to gg'g^{-1}$. El estabilizador de g' es exactamente $C(g')$. Notando que la órbita de g' tiene un solo elemento ssi $g' \in Z$ y que las órbitas son disjuntas obtenemos el siguiente resultado.

Teorema 2.8 (Fórmula de clases)**.** *Sea G un grupo y $\mathscr{G}$ un conjunto de representantes de las órbitas de G tales que ningún representante está en el centro de G. Luego*

$$|G| = |Z(G)| + \sum_{g' \in \mathscr{G}} |G : C(g')|.$$

Los siguientes tres resultados son una aplicación directa de la igualdad anterior.

Proposición 2.6. *Todo grupo cuyo orden es una potencia positiva de un primo tiene centro no trivial.*

Demostración. Sea G de orden p^n, con $n \in \mathbb{N}$ positivo y supongamos que $|Z(G)| = 1$. La definición de centro implica que para cualquier $x \neq 1$ se tiene que $C(x) \neq G$ y entonces $[G : C(x)]$ es una potencia positiva de p. Luego la fórmula de clases muestra que $|G| = 1 + kp$ para cierto $k \in \mathbb{N}$, pero p divide a $|G|$ y llegamos a una contradicción, de modo que $|Z(G)| > 1$. □

Proposición 2.7. *Si $G/Z(G)$ es cíclico, entonces G es abeliano.*

Demostración. Sea $G/Z = \langle gH \rangle$ de modo que cualquier elemento de G se puede escribir en la forma $g^k z$ con $g \in G$ fijo, $k \in \mathbb{Z}$ y $z \in Z$. Luego si $x = g^k z$ e $y = g^l z'$ se tiene que

$$xy = g^k z g^l z' = z g^k g^l z' = z g^l g^k z' = z g^l z' g^k = g^l z' g^k z = yx.$$

□

Corolario 2.2. *Si p es primo entonces todo grupo de orden p^2 es abeliano.*

Ahora bien consideremos un grupo G y $\mathscr{S}$ el conjunto de todos los subgrupos de G, y hagamos actuar G en $\mathscr{S}$ vía conjugación, esto es $(g,H) \to gHg^{-1}$. Ésta es efectivamente una acción, pues gHg^{-1} es un grupo y también se tiene que $1H1^{-1} = H$ y $g(g'Hg^{-1}1)g^{-1} = (gg')H(gg')^{-1}$. Al estabilizador de H bajo esta acción particular se le llama el normalizador de H en G y se anota $N_G(H)$ o simplemente $N(H)$ y es el subgrupo más grande en G en el cual H es normal pues

$$N_G(H) = N(H) = \{g \in G / \ gHg^{-1} = H\}.$$

Luego $H \lhd G$ ssi $N(H) = G$.

Sea G un grupo actuando en un conjunto X. Denotemos por $\mathrm{Fix}_X(G)$ al conjunto de elementos de X que son fijos por todos los elementos de G, de manera que $\mathrm{Fix}_X(G) = \{x \in X; gx = x \ \forall g \in G\}$. Equivalentemente, son aquellos elementos cuya órbita está compuesta por un solo elemento, o aquellos cuyo estabilizador es todo G.

Lema 2.1. *Si G es un grupo finito cuyo orden es una potencia de un primo p y G actúa en un conjunto finito X, entonces* $|\mathrm{Fix}_X(G)| \equiv |X| \mod p$.

Demostración. Consideremos $\{X_1, X_2, X_3, \ldots, X_n\}$ el conjunto de todas las órbitas de G en X y escojamos $x_i \in X_i$ un representante de cada órbita. Ordenemos los X_i para que exista $1 \leq k \leq n$ tal que $x_i \in \mathrm{Fix}(G)$ si y solo si $i \leq k$. Entonces $|X_i| = 1$ para cada $i \leq k$. Por otra parte, como X es la unión disjunta de las órbitas se tiene que

$$|X| = \sum_{i=1}^{n} |X_i| = \sum_{i=1}^{k} |X_i| + \sum_{i=k+1}^{n} |X_i| = |\mathrm{Fix}(G)| + \sum_{i=k+1}^{n} [G : \mathrm{Stab}(x_i)].$$

Pero si $i > k$ entonces $x_i \notin \mathrm{Fix}(G)$, es decir $\mathrm{Stab}(x)$ es un subgrupo propio de G. El teorema de Lagrange implica que cada $\mathrm{Stab}(x_i)$ tiene orden una potencia de p, luego p divide a $\sum_{i=k+1}^{n} [G : \mathrm{Stab}(x_i)]$ y por lo tanto $|X| \equiv |\mathrm{Fix}(G)| \mod p$. □

Lema 2.2. *Si H es un subgrupo de orden una potencia de un primo p de un grupo finito G, y además p divide a $[G : H]$, entonces p divide a $[N(H) : H]$.*

Demostración. Hagamos actuar H en el conjunto X de las clases laterales izquierdas de H en G por multiplicación izquierda. Esto es, $H \times X \to X$ definida por $(h, gH) \longmapsto (hg)H$. Por el resultado anterior se tiene que $|\mathrm{Fix}(H)| \equiv [G : H] \mod p$, pero

$$\mathrm{Fix}(H) = \{gH; \ hgH = gH \ \forall h \in H\} = \{gH; \ g^{-1}hg \in H \ \forall h \in H\} = \{gH; \ g \in N(H)\}.$$

Es decir, $\mathrm{Fix}(H)$ es el conjunto de las clases laterales de H en $N(H)$ y por lo tanto

$$[N(H) : H] \equiv [G : H] \equiv 0 \mod p$$

pues p divide a $[G : H]$. □

Un corolario evidente es el siguiente.

Corolario 2.3. *En un grupo de orden una potencia de un primo p, todo subgrupo propio es un subgrupo propio de su normalizador. En particular, si G tiene orden p^m, todo subgrupo de orden p^{m-1} es normal en G.*

Teorema 2.9 (Teorema de Cauchy)**.** *Si G es un grupo finito y p es un primo que divide el orden de G, entonces existe un elemento en G que tiene orden p.*

Demostración. Consideremos $\mathscr{S} = \{(a_1, a_2, a_3, \ldots, a_n) \in G^p / \ a_1a_2a_3\cdots a_p = 1\}$ el conjunto de las p-tuplas de elementos de G que multiplicados dan 1, y la permutación cíclica de orden p dada por $\sigma = (123\cdots p-1) \in \Sigma_p$.

Hagamos actuar el grupo cíclico $\langle\sigma\rangle$ en $\mathscr{S}$ por

$$(\sigma^i, (a_1, a_2, a_3, \ldots, a_p)) \longmapsto (a_{\sigma^i(1)}, a_{\sigma^i(2)}, a_{\sigma^i(3)}, \ldots, a_{\sigma^i(p)}).$$

Recordemos que $xy = 1$ implica que $yx = 1$ en un grupo, y por lo tanto para $\mathbf{a} = (a_1, a_2, a_3, \ldots, a_p) \in \mathscr{S}$ se tiene que $a_2a_3\cdots a_pa_1 = 1$. Luego

$$(\sigma, \mathbf{a}) = (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}, \ldots, a_{\sigma(p)}) \in \mathscr{S}$$

e inductivamente se verifica que $(\sigma^i, \mathbf{a}) \in \mathscr{S}$. Además, $(1, \mathbf{a}) = \mathbf{a}$ y $(\sigma^i\sigma^j, \mathbf{a}) = (\sigma^{i+j}, \mathbf{a}) = (\sigma^i, (\sigma^j, \mathbf{a}))$. Por lo tanto, la función definida arriba es efectivamente una acción de $\langle\sigma\rangle$ en $\mathscr{S}$.

Notemos que para determinar $(a_1, a_2, a_3, \ldots, a_p) \in \mathscr{S}$ los primeros $p-1$ elementos son cualquiera en G y $a_p = \left(\prod_{i=1}^{p-1} a_i\right)^{-1}$, luego $|\mathscr{S}| = |G|^{p-1}$ y entonces p divide a $|\mathscr{S}|$. El lema 2.1 permite concluir que $0 \equiv |\mathscr{S}| \equiv |\mathrm{Fix}\,\langle\sigma\rangle| \mod p$.

Como $\mathbf{1} = (1, 1, 1, \ldots, 1) \in \mathrm{Fix}(\langle\sigma\rangle)$ y p divide a $|\mathrm{Fix}(\langle\sigma\rangle)|$, necesariamente existe un $\mathbf{x} \neq \mathbf{1}$ en $\mathrm{Fix}(\langle\sigma\rangle)$. Pero $\mathrm{Fix}(\langle\sigma\rangle) = \{\mathbf{a} \in \mathscr{S} / \ a_1 = a_2 = a_3 = \cdots = a_p\}$, y entonces podemos encontrar $x \in G$, $x \neq 1$ tal que $(x, x, x, x, \ldots, x) = \mathbf{x} \in \mathrm{Fix}(\langle\sigma\rangle)$. Es decir, $x^p = 1$. Finalmente concluimos que como p es primo y $x \neq 1$, el orden de x es p. □

Observación 2.6. Sea p un número primo. Un grupo en el cual todo elemento tiene orden una potencia de p, se llama un *p-grupo*. El teorema de Cauchy permite asegurar que todo p-grupo finito tiene orden una potencia de p.

Ejemplo 2.12. Si G tiene orden 6, el teorema de Cauchy asegura la existencia de elementos $x, y \in G$ de orden 2 y 3 respectivamente. Notemos que $xy \neq 1$, pues si en tal caso $y = x^{-1} = x$.

Si G es abeliano, entonces $(xy)^2 = x^2y^2 = y^2 \neq 1$ y del mismo modo $(xy)^3 = x^3y^3 = x^3 \neq 1$, luego el teorema de Lagrange muestra que xy tiene orden 6. Por lo tanto G es el grupo cíclico de orden 6. Es decir, existe un único grupo abeliano de orden 6 salvo isomorfismo.

Si G no es abeliano, podemos afirmar que x y y no conmutan y como $\langle y\rangle$ es de índice 2 en G tenemos que $\langle y\rangle$ es normal en G, y por ende $xyx^{-1} = xyx \in \langle y\rangle$. Veamos qué valores puede tomar xyx^{-1}:

- Si $xyx = 1$ entonces $xy = x$ e $y = 1$, lo cual no puede ser.

- Si $xyx = y$ entonces $xy = yx$, pero habíamos asumido que x e y no conmutaban.

Entonces necesariamente $xyx = y^2$, o equivalentemente $xy = y^{-1}x^{-1} = (xy)^{-1}$. Lo anterior también implica que $yx = xy^2 = x^{-1}y^{-1} = (yx)^{-1}$. Entonces podemos afirmar que $xy \neq yx$ y ambos elementos son de orden 2. Además, ambos xy y yx son distintos de x pues y no es 1.

Así tenemos que $G = \{1, x, y, y^2, xy, yx\}$ y además notamos que como $xyx = y^2$, entonces $(xy)y = yx$, y como $xy = y^2x$ entonces $yxy = x$. De la misma manera se obtienen las relaciones $y^2xy = yx$ y $yxy^2 = xy$. Por lo tanto, la tabla de multiplicación de G es

	1	x	y	y^2	xy	yx
1	1	x	y	y^2	xy	yx
x	x	1	yx	xy	y^2	y
y	y	xy	y^2	1	yx	x
y^2	y^2	yx	1	y	x	xy
xy	xy	y	x	yx	1	y^2
yx	yx	y^2	xy	x	y	1

Por lo tanto existe un único grupo de orden 6 no abeliano, salvo isomorfismo. Finalmente obtenemos que salvo isomorfismo $\mathbb{Z}_3$ y Σ_3 son los únicos grupos con 6 elementos.

En el caso particular de Σ_3 tenemos que $x = (12)$ es de orden 2 y $y = (123)$ es de orden 3. Además $xy = (12)(123) = (23)$ y $yx = (123)(12) = (13)$. Es un ejercicio directo verificar que la tabla de multiplicación de Σ_3 es idéntica a la tabla de arriba.

El siguiente resultado es una extensión del teorema de Cauchy y permite estudiar la estructura aritmética de un grupo, finita es decir, las propiedades de éste que resultan de la factorización prima de su cardinal.

Teorema 2.10 (Teoremas de Sylow)**.** *Sea G un grupo finito de orden $p^m r$ donde p es primo que no divide a r.*

(1) Para cada $1 \leq k \leq m$ existe un subgrupo de G de orden p^k. Cada subgrupo de orden p^i es normal en algún subgrupo de orden p^{i+1} para $0 \leq i < m$.

(2) Todos los subgrupos de orden p^m son conjugados entre si.

(3) Si n es la cantidad de subgrupos de orden p^m, entonces $n = [G : N(P)]$ donde P es cualquier subgrupo de orden p^m. Además $n \equiv 1 \mod p$ y n divide a r.

Demostración. Por el teorema de Cauchy existe un elemento g de orden p. Supongamos que H es un subgrupo de orden p^i con $1 \leq i < m$, entonces p divide a $[G : H]$ y por el lema 2.2 p también divide a $[N(H) : H]$. Como H es normal en $N(H)$, se tiene que $N(H)/H$ es un grupo cuyo orden es divisible por p y nuevamente por el teorema de Cauchy muestra la existencia de un elemento $\mathscr{K}$ de orden p en $N(H)/H$. El teorema de correspondencia implica la existencia de un subgrupo K de $N(H)$, tal que $H \lhd K \leq N(H)$ y $\mathscr{K} = K/H$. Luego $[K : H] = p$ y entonces $|K| = p^{i+1}$. Un argumento inductivo termina de demostrar (1).

Sea Q un p-subgrupo de G y sea X el conjunto de todas las clases laterales de P en G. Hagamos actuar Q en X por multiplicación izquierda, esto es definimos $(q, gP) \longmapsto (qg)P$. El lema **??** muestra que

$|\text{Fix}(Q)| \equiv |X| \mod p$. Como $|X| = [G : P]$ entonces p no divide a $|X|$ y $\text{Fix}(Q) \not\equiv 0 \mod p$. Luego existe $yP \in \text{Fix}(Q)$ pero

$$\begin{aligned}\text{Fix}(Q) &= \{gP \in X;\, qgP = gP,\ \forall q \in Q\} = \{gP \in X;\, g^{-1}qgP = P,\ \forall q \in Q\} \\ &= \{gP \in X;\, g^{-1}qg \in P,\ \forall q \in Q\} = \{gP \in X;\, g^{-1}Qg \subseteq P\}.\end{aligned}$$

Concluimos que existe yP en X tal que $y^{-1}Qy \subseteq P$, y tomando $x = y^{-1}$ se tiene que $xQx^{-1} \leq P$. En particular, si $|Q| = p^m$ tenemos que $xQx^{-1} = P$ pues tanto xQx^{-1} como P tienen orden p^m. Esto demuestra (2).

Ahora consideremos un grupo P fijo de orden tamaño p^m. Sea $\mathscr{S}$ la familia de subgrupos de G y consideremos la acción de G en $\mathscr{S}$ por conjugación. Entonces la órbita de P es el conjunto de subgrupos conjugados de P y además $\text{Orb}(P) = [G : \text{Stab}(P)]$, pero $\text{Stab}(P) = N(P)$ y por ende si n denota la cantidad de subgrupos de orden p^m en G se tiene que $n = [G : N(P)]$. Además

$$p^m r = [G : N(P)][N(P) : P]|P| = [G : N(P)][N(P) : P]p^m$$

implica que $r = n[N(P) : P]$, y entonces n divide a r.

Finalmente consideremos $\mathscr{P}$ la familia de subgrupos de orden p^m en G y hagamos actuar H en $\mathscr{P}$ por conjugación. Nuevamente el lema **??** entrega que $|\text{Fix}(H)| \equiv n \mod p$. Notemos que $Q \in \text{Fix}(H)$ si y solo si $pQp^{-1} = Q$ para cada $p \in P$, es decir $P \subseteq N(Q)$. Pero $Q \lhd N(Q)$ implica que $xQx^{-1} = Q$ para cada $x \in N(Q)$ y entonces Q es el único subgrupo de orden p^m en $N(Q)$. Es decir, $\text{Fix}(P) = \{P\}$ y por lo tanto $n \equiv 1 \mod p$, que termina por demostrar (3) y el teorema. □

Cuando $|G| = p^m r$ y p no divide a r, a los subgrupos de orden p^m le llamamos p-subgrupos de Sylow. Notemos que la parte (2) del Teorema dice que todos los p-subgrupos de Sylow son conjugados y la demostración de la parte (3) prueba que el único p-subgrupo de Sylow en $N(P)$ es P.

Un corolario evidente es el siguiente

Corolario 2.4. *Un p-subgrupo de Sylow es normal si y solamente si es el único p-subgrupo de Sylow.*

Demostración. Basta notar que $H \lhd G$ si y solo si $1 = [G : N(H)]$. □

Corolario 2.5. *Si P es un p-subgrupo de Sylow, entonces $N(N(P)) = N(P)$.*

Demostración. Es claro que $N(P) \subseteq N(N(P))$, luego basta probar la contención en el otro sentido. Sea $x \in N(N(P))$, entonces $xPx^{-1} \leq xN(P)x^{-1} = N(P)$, de modo que xPx^{-1} es un p-subgrupo de Sylow en $N(P)$. Como P es normal en $N(P)$ se deduce por el corolario anterior que P es el único p-subgrupo de Sylow en $N(P)$ y entonces $xPx^{-1} = P$. Luego $x \in N(P)$ y concluimos que $N(N(P)) \subset N(P)$. □

Ejemplo 2.13. Sea G un grupo de orden 10. Por el teorema de Cauchy existen $x, y \in G$ de orden 2 y 5 respectivamente. Como $x^{-1} = x$, se tiene que $xy \neq 1$, pues en tal caso $y = x^{-1} = x$.

Supongamos que G es abeliano. En tal caso, $(xy)^2 = x^2y^2 = x^2 \neq 1$ y por lo tanto xy no tiene orden 2. Del mismo modo $(xy)^5 = x^5y^5 = y^5 = y \neq 1$, es decir, xy no tiene orden 5 de manera que xy tiene orden 10 y $G = \langle xy \rangle$. Luego hay un único grupo abeliano de orden 10 salvo isomorfismo.

Supongamos ahora que G no es abeliano. Entonces $xy \neq yx$ y el teorema de Sylow muestra la cantidad de subgrupos de orden 5 es un divisor de 2 y es congruente a 1 módulo 5. Por lo tanto, existe un único grupo de orden 5 en G y concluimos que $\langle x \rangle$ es normal en G. Luego $yxy^{-1} = yxy \in \langle x \rangle$. Revisemos qué valores puede tomar yxy^{-1}:

- Si $yxy = 1$ entonces $x = 1$, lo que no puede ser.
- Si $yxy = x$ entonces $yx = xy$, pero ya habíamos asumido que x e y no conmutaban.
- Si $yxy = x^2$ entonces $x^4 = x^2x^2 = (yxy)(yxy) = yx^2y$. Por otra parte $x = y^2xy^2 = y(yxy)y = yx^2y = x^4$ y entonces x tendría orden 3.
- Si $yxy = x^3$, entonces $x^4 = x^9 = (yxy)(yxy)(yxy) = yx^3y$. Por otra parte $x = y^2xy^2 = y(yxy)y = yx^3y = x^4$ y entonces x tendría orden 3.

Luego necesariamente $yxy = x^4 = x^{-1}$, o dicho de otro modo $yx = x^{-1}y$. Entonces $G \cong D_{10}$, donde D_{10} es el grupo de simetrías del pentágono regular.

Ejemplo 2.14. Consideremos un grupo G abeliano finito. Sea $|G| = p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$ la descomposición prima de $|G|$ y sea r un divisor de $|G|$ con $r = p_1^{m_1}p_2^{m_2}\cdots p_s^{m_s}$ donde $s \leq r$ y $m_i \leq n_i$. Por el teorema de Sylow, para cada i existe un subgrupo $|H_i|$ de orden $p_i^{m_i}$ en G, y además cada H_i es normal en G pues éste es abeliano. Consideremos H_1 y H_2, cuyos órdenes son claramente primos relativos. Entonces $H_1 \cap H_2 = \{1\}$ ya que si $x \in H_1 \cap H_2$, entonces el orden de x divide a $p_1^{m_1}$ y a $p_2^{m_2}$. Por lo tanto $H_{12} \doteq H_1H_2$ es subgrupo de G de orden $p_1^{m_1}p_2^{m_2}$ y de hecho es grupo ya que $H_1H_2 = H_2H_1$ al ser G abeliano. Consideremos la función epiyectiva $\tau : H_1 \times H_2 \to H_1H_2$ definida por $\tau(h_1, h_2) = h_1h_2$ y notemos que $h_1h_2 = \tau(h_1, h_2) = \tau(h_1', h_2') = h_1'h_2'$ implica que $h_2h_2'^{-1}$ es el inverso de $h_1'^{-1}h$ y por ende $h_2h_2'^{-1} \in H_1 \cap H_2 = \{1\}$. Luego $h_1 = h_1'$ y $h_2 = h_2'$, lo que muestra que τ es también inyectiva y que $H_{12} = H_1H_2$ es un subgrupo de G de orden $p_1^{m_1}p_2^{m_2}$.

Ahora notemos que H_{12} y H_3 tienen órdenes que son primos relativos, por lo tanto $H_{12} \cap H_3 = \{1\}$ y el mismo argumento que antes muestra que $H_{123} = H_{12}H_3$ es un subgrupo de G de orden $p_1^{m_1}p_2^{m_2}p_3^{m_3}$. Inductivamente se verifica que

$$H_{123\ldots s} = H_1H_2H_3\cdots H_s$$

es un grupo de orden r en G. Es decir, el recíproco del teorema de Lagrange es cierto cuando G es abeliano.

2.4. Σ_n

En esta sección le daremos un vistazo con mayor detalle a Σ_n, el grupo de permutaciones de n elementos. Como el Teorema de Cayley afirma que todo grupo es isomorfo a un subgrupo de de un grupo de permutaciones, esto basta para intentar conocer más personalmente a Σ_n, al menos haberlo saludado de mano. Por otro lado, este grupo tiene aplicaciones interesante a la teoría de grafos y a la teoría de Galois. Por ejemplo, el que no exista una fórmula para las raíces del polinomio general de grado mayor o igual a 5 con coeficientes en $\mathbb{R}$ (u otro cuerpo) que recurra solamente a operaciones algebraicas, radicales y los

coeficientes del polinomio, usa un resultado previo que dice que Σ_n no es soluble para $n \geq 5$. Probaremos esto en el capítulo 5 y en este apartado demostraremos varias propiedades de Σ_n, entre ellas ésta última.

Primero que nada, necesitamos una definición preliminar: un grupo G se dice *soluble* si existe una cadena de subgrupos

$$G_1 = \{1\} \lhd G_2 \lhd G_3 \lhd \cdots G_n = \{G\}$$

tal que cada G_i es normal en G_{i+1} y además cada cuociente G_{i+1}/G_i es abeliano para $i \in [n-1]$.

Ejemplo 2.15. Todo grupo abeliano es soluble, pues basta tomar la serie $\{1\} \lhd G$. Si G es un p-grupo finito de orden p^n con p primo, entonces existe un subgrupo G_{n-1} de G orden p^{n-1}, cuyo índice en G es p, el menor primo que divide a p, y concluimos que $G_{n-1} \lhd G$. Por la misma razón existe un subgrupo normal G_{n-2} en G_{n-1} de índice p. Inductivamente podemos crear una cadena

$$G_0 = \{1\} \lhd G_1 \lhd G_2 \lhd \cdots G_{n-1} \lhd G_n = G$$

donde cada $G_i \lhd G_{i+1}$ y el índice $[G_{i+1} : G_i] = p$ entonces cada factor $G_{i+1}/G_i \cong \mathbb{Z}_p$. Luego todo p-grupo finito es soluble. Es el caso de D_4 que tiene $2^3 = 8$ elementos.

Recordemos que a $\sigma = (i_1 i_2 i_3 \dots i_r) \in \Sigma_n$ le llamamos un ciclo de largo r, y denota a la función de $[n]$ en sí mismo que fija a todo elemento de $[n] \setminus \{i_1, i_2, i_3, \cdots, i_r\}$ y además $\sigma(i_k) = i_{k+1}$ si $k \in [r-1]$ y $\sigma(i_r) = i_1$. Por ejemplo, (1234) es un ciclo de largo 4 en Σ_{2666}. [1] También podemos notar que $\sigma = (i_1 i_2 i_3 \dots, i_r) = (i_1 \sigma(i_1) \sigma^2(i_1) \sigma^3(i_1) \dots \sigma^{r-1}(i_1))$. Por lo tanto $\sigma^t \neq 1$ si $t \in [r-1]$. Pero además $\sigma^r(i_1) = \sigma(i_r) = i_1$ y $\sigma^r(i_j) = (\sigma^{j-1})^r(i_1) = (\sigma^r)^{j-1}(i_1) = \sigma^{j-1}(i_1) = i_j$. Es decir, σ^r es la identidad en $\{i_1, i_2, \dots, i_r\}$ y como σ fija a todo elemento de $[n] \setminus \{i_1, i_2, i_3, \cdots, i_r\}$, entonces $\sigma^r = 1$. Por lo tanto:

Proposición 2.8. *Un ciclo de largo r tiene orden r.*

Ahora notemos que no existe una única manera de escribir un ciclo: por ejemplo, $(123) = (231) = (312)$ y más generalmente $(i_1 i_2 i_3 \dots i_r) = (i_2 i_3 \dots i_r i_1) = (i_3 i_4 \dots i_r i_1 1_2) = \cdots (i_r i_1 \dots i_{r-2} i_{r-1})$ es decir, un ciclo de largo r se puede escribir de r formas distintas. De hecho basta fijar el primer elemento del ciclo para que quede totalmente determinado. Consideremos el elemento τ de Σ_9 definido por

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 2 & 1 & 6 & 5 & 9 & 7 & 8 \end{pmatrix}.$$

Podemos escribir τ como producto de ciclos como $\tau = (1324)(56)(798)$. Notemos que no hay un número de $[9]$ que se repita en un par de ciclos de τ y cada elemento de $[9]$ está en un ciclo de τ. Si por ejemplo, $\rho = (1234)$ en Σ_9 podemos escribirlo como $\rho = (1234)(5)(6)(7)(8)(9)$ y entonces podemos decir que ρ también es un producto de ciclos disjuntos dos a dos tal que cada elemento de $[9]$ está en un ciclo de ρ.

Diremos que dos ciclos $(i_1 i_2 i_3 \cdots i_r)$ y $(j_1 j_2 j_3 \cdots j_s)$ son *disjuntos* en Σ_n si $i_k \neq j_l$ para todo $k \in [r]$ y $l \in [s]$.

[1] Hay una cierta ambigüedad en la notación de ciclos, pues (123) puede ser considerado en Σ_n para cualquier $n \geq 3$ pero cargaremos con esta culpa, y el contexto nos permitirá entender en cuál Σ_n se está.

Observación 2.7. Si $\sigma = (i_1 i_2 \dots i_r)$ y $\tau = (j_1 j_2 j_3 \dots j_s)$ son ciclos disjuntos, esto quiere decir que τ funciona como la identidad en los i_k y σ funciona como la identidad en los j_t. Por lo tanto, si $x \notin \{i_k\}_{k=1}^r \cup \{j_t\}_{k=1}^s$, entonces $\tau\sigma(x) = x = \sigma\tau(x)$. Si $x \in \{i_k\}_{k=1}^r$, entonces $\tau\sigma(x) = \sigma(x) = \sigma\tau(x)$. Finalmente, si $x \in \{j_t\}_{t=1}^s$, entonces $\tau\sigma(x) = \tau(x) = \sigma\tau(x)$. Es decir, dos ciclos disjuntos conmutan.

Teorema 2.11. *Toda permutación se escribe de manera única (salvo el orden) como producto de ciclos disjuntos.*

Demostración. Sea $\sigma \in \Sigma_n$ y consideremos H el grupo cíclico generado por σ en Σ_n. Consideremos también la acción natural $H \times [n] \to [n]$ dada por $(\tau, k) \longmapsto \tau(k)$ y sean $\{X_i\}_{i=1}^r$ las distintas órbitas asociadas. Notemos que $\sigma(X_j) = X_j$, pues σ es biyectiva y $\sigma(X_j) \subset X_j$ por la definición de las órbitas.

Definamos $\sigma_j \in \Sigma_n$ del siguiente modo

$$\sigma_j(x) = \begin{cases} \sigma(x) & \text{si } x \in X_j \\ x & \text{si } x \notin X_j \end{cases}$$

y consideremos el producto $\sigma_1\sigma_2\sigma_3 \cdots \sigma_r \in \Sigma_n$. Cuando $x \in X_j$ tenemos que

$$\sigma_1\sigma_2\sigma_3 \cdots \sigma_r(x) = \sigma_j(x) = \sigma(x)$$

y entonces $\sigma = \sigma_1\sigma_2\sigma_3 \cdots \sigma_r$.

Si $|X_j| = r_j$ y $x_j \in X_j$ entonces

$$X_j = \{x_j, \sigma(x_j), \sigma^2(x_j), \dots, \sigma^{r_j-1}(x_j)\} = \{x_j, \sigma_j(x_j), \sigma_j^2(x_j), \dots, \sigma_j^{r_j-1}(x_j)\},$$

pero además σ_j actúa como la identidad fuera de X_j y por lo tanto σ_j es el ciclo

$$(x_j\, \sigma_j(x_j)\, \sigma_j^2(x_j) \cdots \sigma_j^{r_j-1}(x_j)).$$

Concluimos que σ es un producto de ciclos disjuntos.

La unicidad es directo de ver que cada ciclo τ en una descomposición de σ en ciclos disjuntos es del tipo $(x\, \tau(x) \dots \tau^{r-1}(x))$ donde $r = |\operatorname{Orb}(x)|$. □

Veamos otros generadores de Σ_n. Hasta el momento tenemos que los ciclos generan Σ_n. Consideremos un ciclo cualquiera $(i_1 i_2 \dots i_r)$ de Σ_n y escribámoslo del siguiente modo:

$$(i_1 i_2 \dots i_r) = (i_1 i_r)(i_1 i_{r-1})(i_1 i_{r-2}) \cdots (i_1 i_3)(i_1 i_2)$$

Como toda permutación es producto de ciclos y como todo ciclo es producto de 2-ciclos, obtenemos que los 2-ciclos generan a Σ_n. A los 2-ciclos les llamamos *transposiciones*. Hemos demostrado el siguiente resultado.

Teorema 2.12. *Toda permutación se puede escribir como producto de transposiciones no necesariamente disjuntas.*

Sin embargo, una permutación no tiene una única forma de escribirse como producto de transposiciones. Por ejemplo $(13)(34) = (34)(14)$ y no es solo orden sino que son distintas formas de escribirlas. Además, como una transposición es su propia inversa podemos agregar dos veces una misma transposición y no cambiar a la permutación:

$$(134) = (12)(34)(23)(23)(45)(45)(14)(14)$$

Entonces ni siquiera el "largo" de la escritura vía transposiciones es invariante. Una pregunta que surge es si hay algo invariante en la escritura y una respuesta es la *paridad*. Es decir, si una permutación se escribe como un producto par de transposiciones, cualquier otra escritura también tiene un número par de transposiciones. Esto significa que no hay ninguna transposición que se pueda escribir como un producto de un número par de transposiciones y por otro lado como el producto de un número impar de transposiciones.

En efecto, consideremos $\sigma \in \Sigma_n$ y la base canónica de $\mathbb{R}^n$ $\mathscr{B} = \{e_1, e_2, e_3, \ldots, e_n\} = \{e_{\sigma(1)}, e_{\sigma(2)}, e_{\sigma(3)}, \ldots, e_{\sigma(n)}\}$. Consideremos también la matriz $M_\sigma \in M_n(\mathbb{R})$ cuya i-ésima columna es el vector $e_{\sigma(i)}$. Como el determinante es alternante (esto es, cada vez que se permutan dos columnas el determinante cambia en un signo) y el determinante de la matriz identidad es 1, se tiene que si $\sigma = \tau_1\tau_2\tau_3\cdots\tau_r$, con τ_i transposición, entonces el determinante de M_σ es $(-1)^r$. Luego un la paridad de una permutación está bien definida.

Si una permutación se escribe como un número par de transposiciones se llama una permutación *par* y en caso contrario se dice *impar*. Por ejemplo, (si $n \geq 2$) la identidad es par, pues $1 = (12)(12)$.

Es claro que el producto de dos permutaciones pares es par, el producto de dos impares es par y el producto de una par con una impar es impar. Como el conjunto $\{1, -1\}$ es un grupo con la multiplicación de $\mathbb{R}$, la función $\operatorname{sgn}\colon \Sigma_n \to \{1, -1\}$ definida por $\operatorname{sgn}(\sigma) = 1$ si σ es par y -1 si σ es impar, es un morfismo de grupos llamado *signo*. Si $n \geq 2$ este morfismo es epiyectivo y el kernel de sgn es el subgrupo normal de Σ_n formado por todas las permutaciones pares, llamado el grupo *alternante* en n símbolos y denotado por A_n. Por el primer teorema el isomorfismo se tiene que $\Sigma_n/A_n \cong \{1, -1\} \cong \mathbb{Z}_2$.

Así se tiene que A_n es normal en Σ_n, tiene índice 2 en Σ_n, y que $|A_n| = n!/2$.

Ejemplo 2.16. Examinemos A_n para valores pequeños de n: primero notemos que $A_2 = \{1\}$ y $|A_3| = \dfrac{3!}{2} = 3$. Como Σ_3 tiene un único subgrupo de orden 3 y es $\{1, (123), (132)\}$, entonces $A_3 = \langle(132)\rangle$. De hecho, $(123) = (13)(12)$ y en general $(abc) = (ac)(ab)$.

Para el caso $n = 4$ tenemos que $|A_4| = 4!/2 = 12$, y como A_4 contiene a todos los 3-ciclos y a los productos de 2 transposiciones disjuntas, deducimos que

$$A_4 = \{1, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}.$$

De la descripción anterior sigue que los elementos de A_4 tienen orden 3,2 ó 1. Supongamos ahora que A_4 tiene un subgrupo H de orden 6, luego éste debe ser Σ_3 o $\mathbb{Z}_6$ por el ejemplo 2.12. Como A_4 no tiene elementos de orden seis, entonces $H \cong \Sigma_3$ y H tiene un único grupo de orden 3 generado por (abc). Sea $d \in \{1, 2, 3, 4\} \setminus \{a, b, c\}$, entonces el elemento $(ab)(cd)$ no puede estar en H por que si lo estuviera

obtendríamos que $(abc)(ab)(cd) = (acd) \in H$, pero $(acd) \notin \langle(abc)\rangle$ y (abc) era el único elemento de orden 3 en H. Tampoco puede estar $(ac)(bd)$ pues si lo estuviera entonces $(abc)(ac)(bd) = (bdc) \in H$ pero $(bdc) \notin \langle(abc)\rangle$, y análogamente $(ad)(bc) \notin H$ pues si lo estuviera

$$(abc)(ad)(bc) = (adb) \in H$$

pero $(bdc) \notin < (abc) >$. Pero $(ab)(cd), (ac)(bd)$ y $(ad)(bc)$ son los únicos elementos de orden 2 en A_4 y por lo tanto H no tiene elementos de orden 2, lo que contradice el teorema de Cauchy. Luego A_4 no tiene subgrupos de orden 6 pese a que 6 divide a $|A_4|$, lo que implica que el recíproco del teorema de Lagrange (y la generalización del teorema de Cauchy a divisores no primos) es falso en general.

Observación 2.8. Notemos que el grupo de Klein $V_4 = \{1, (13)(24), (12)(34), (14)(23)\}$ es el único 2-Sylow en A_4 y entonces V_4 es característico (y por ende, normal) en A_4. Además tenemos una cadena de subgrupos normales $\{1\} \lhd \langle(12)\rangle \lhd V_4 \lhd A_4$ tal que los cocientes consecutivos

$$A_4/V_4,\ V_4/\langle(12)(34)\rangle,\ \langle(12)(34)\rangle/1$$

son todos abelianos (más precisamente son todos cíclicos). Luego A_4 es soluble. Σ_3 también lo es: notemos que $\{1\} \lhd \langle(123)\rangle \lhd \Sigma_3$ y además

$$\Sigma_3/\langle(123)\rangle,\ \langle(123)\rangle/1$$

son cíclicos.

En lo que sigue demostraremos que A_n no tiene esa propiedad (una cadena de subgrupos, cada uno normal en el siguiente, partiendo de $\{1\}$ y llegando a al grupo completo, donde cada cuociente es abeliano) si $n \geq 5$. Para ello analizaremos más detenidamente a A_n.

En el ejemplo anterior vimos que todo 3-ciclo es par pues $(abc) = (ac)(ab)$. Recíprocamente, consideremos el producto de dos transposiciones $(ab)(cd)$ y veamos los tres casos posibles: si son la misma transposición, entonces $(ab)(cd) = (ab)(ab) = 1 = (123)(123)(123)$. Si tienen un valor en común, entonces $(ab)(cd) = (ab)(bc) = (abc)$. Si son disjuntas, entonces $(ab)(cd) = (acb)(acd)$. Por lo tanto, como toda permutación par se escribe como un producto de pares de transposiciones, entonces toda permutación par se escribe como producto de 3-ciclos. Hemos probado el lema siguiente.

Lema 2.3. *Si $n \geq 3$, entonces los 3-ciclos generan A_n.*

Fijemos ahora $r \neq s \in [n]$ con $n \geq 3$ y consideremos el conjunto $T = \{(rsk) / \ s \neq k \neq r, k \in [n]\} \subseteq A_n$. Tomemos un 3-ciclo cualquiera (abc) en A_n, entonces

$$(abc) = (rsa)^2(rsc)(rsb)^2(rsa)$$

siempre y cuando $\{r,s\} \cap \{a,b,c\} = \emptyset$. Si $\{r,s\} = \{a,b\}$, entonces $(abc) = (rsc)$ o (rcs). En el primer caso $(rsc) \in T$ y el el segundo $(rcs) = (rsc)(rsc)$. Si $|\{r,s\} \cap \{a,b,c\}| = 1$, entonces sin restricción $(abc) = (rbc)$ de modo que $(rbc) = (rsc)(rsb)^2$. Entonces tenemos que todo 3-ciclo de A_n se puede escribir como producto de elementos de T. Esto refina el lema anterior al resultado a continuación.

Lema 2.4. *Si $n \geq 3$, y $r \neq s$ entonces A_n es generado por $\{(rsk)/\ s \neq k \neq r, k \in [n]\}$.*

Ahora consideremos un subgrupo N normal en A_n con $n \geq 3$ y supongamos que N contiene un 3-ciclo. Si $n = 3$ se tiene que $N = A_3 = \langle(123)\rangle$, pero si $n > 3$ el resultado también es cierto: en efecto, si $(rsc) \in N$ y $k \notin \{r, s, c\}$ entonces $(rsk) = (rs)(ck)(rsc)^2[(rs)(ck)]^{-1} \in N$, pero como $\{(rsk)/\ s \neq k \neq r, k \in [n]\}$ genera a A_n se tiene que $A_n = N$. Concluimos lo siguiente.

Teorema 2.13. *Si $n \geq 3$, $N \lhd A_n$ y N contiene un 3-ciclo, entonces $N = A_n$.*

Si demostramos que todo subgrupo normal N de A_n, tiene un 3-ciclo, habremos demostrado que A_n no tiene subgrupos normales distintos de A_n y de $\{1\}$. Pero ya vimos A_4 tiene un subgrupo normal, a saber V_4 el grupo de Klein. Sin embargo, el resultado es cierto para $n \geq 5$.

Lema 2.5. *Si $n = 3$ o $n \geq 5$ y $\{1\} \neq N \lhd A_n$, entonces N tiene un 3-ciclo.*

Demostración. El caso $n = 3$ es directo. Consideremos $n \geq 5$ y tomemos un elemento $\sigma \in N$ distinto de la identidad y que no sea un 3-ciclo. Clasifiquemos σ de acuerdo al mayor largo de los ciclos en su descomposición cíclica y veamos que en cualquier caso N tiene un 3-ciclo.

- Si en la descomposición en ciclos disjuntos de σ hay un elemento de largo mayor o igual a 4 entonces $\sigma = (i_1 i_2 i_3 i_4, ..i_r)\tau$ con τ disjunto con $(i_1 i_2 i_3 i_4, ..i_r)$, de modo que

$$\sigma^{-1}(i_1 i_2 i_3)\sigma(i_1 i_3 i_2) = (i_1 i_2 i_3 i_4, ..i_r)^{-1}(i_1 i_2 i_3)(i_1 i_2 i_3 i_4, ..i_r)(i_1 i_3 i_2) = (i_1 i_3 i_r) \in N$$

  pues $N \lhd A_n$ e $(i_1 i_2 i_3) \in A_n$.
- Si la descomposición en ciclos disjuntos de σ tiene al menos dos elementos de largo 3, digamos $\sigma = (i_1 i_2 i_3)(i_4 i_5 i_6)\tau$ donde τ es disjunto con $(i_1 i_2 i_3)$ y con $(i_4 i_5 i_6)$, entonces consideremos $(i_1 i_2 i_4) \in A_n$. Notemos que

$$\sigma^{-1}(i_1 i_2 i_4)\sigma(i_1 i_4 i_2) = ((i_1 i_2 i_3)(i_4 i_5 i_6))^{-1}(i_1 i_2 i_4)(i_1 i_2 i_3)(i_4 i_5 i_6)(i_1 i_4 i_2) = (i_1 i_4 i_2 i_6 i_3) \in N$$

  y en consecuencia el caso anterior muestra que N tiene un 3-ciclo.
- Si la descomposición en ciclos disjuntos de σ tiene solo un elemento de largo 3 y el resto de largo 2, digamos $\sigma = (i_1 i_2 i_3)\tau$ donde τ es un producto de transposiciones disjuntas entre sí y disjuntas de $(i_1 i_2 i_3)$, entonces $\sigma^2 = (i_1 i_2 i_3)^2\tau^2 = (i_1 i_3 i_2) \in N$.
- Si la descomposición en ciclos disjuntos de σ solo tiene transposiciones, digamos $\sigma = (i_1 i_2)(i_3 i_4)\tau$ donde τ es un producto de transposiciones disjuntas entre sí y disjuntas de $(i_1 i_2)$ y con $(i_3 i_4)$, entonces

$$\sigma^{-1}(i_1 i_2 i_3)\sigma(i_1 i_3 i_2) = (i_1 i_2)(i_3 i_4)(i_1 i_2 i_3)(i_1 i_2)(i_3 i_4)(i_1 i_3 i_2) = (i_1 i_3)(i_2 i_4) \in N.$$

  Como $n > 4$, podemos tomar $j \in [n] \setminus \{i_1, i_2, i_3, i_4\}$ y por ende

$$(i_1 i_3)(i_2 i_4)(i_1 i_3 j)(i_1 i_3)(i_2 i_4)(i_1 j i_3) = (i_1 i_3 j) \in N.$$

□

Los lemas anteriores prueban el próximo teorema.

Teorema 2.14. *Si $n = 3$ o $n \geq 5$, entonces A_n es simple.*

Tomemos $\sigma \in \Sigma_n$ con $n \geq 3$ tal que $\sigma \neq 1$. Supongamos primero que $\sigma(1) = i \neq 1$. Consideremos k con $1 \neq k \neq i$ y definamos $\tau = (ik)$. Entonces $\sigma\tau(1) = \sigma(1) = i$ y en cambio $\tau\sigma(1) = \tau(i) = k \neq i$, es decir $\sigma \notin Z(\Sigma_n)$.

Por otra parte, si $\sigma(1) = 1$ entonces existen $i \neq j$ tal que $\sigma(i) = j$ ya que σ no es la identidad. Definamos $\tau = (1i)$ y notemos que en este caso $\sigma\tau(1) = \sigma(i) = j$ y $\tau\sigma(1) = \tau(1) = i \neq j$. Luego $\sigma \notin Z(\Sigma_n)$. Es decir, hemos demostrado el siguiente resultado.

Teorema 2.15. *Si $n \geq 3$, entonces $Z(\Sigma_n) = \{1\}$.*

Consideremos ahora un ciclo $\sigma = (a_1 a_2 a_3 \dots a_r)$ en Σ_n y conjuguemos σ vía τ una permutación cualquiera de Σ_n. Lo que queremos mostrar es que $\tau\sigma\tau^{-1}$ es también un ciclo de largo r. Para ello notemos que $[n] = \{\tau(1), \tau(2), \dots, \tau(n)\}$, entonces para conocer $\tau\sigma\tau^{-1}$ tenemos que ver cual es su efecto en $\tau(i)$ para cada $i \in [n]$. Empecemos por evaluar los elementos que no están en $\{\tau(a_i)\}_{i=1}^r$: si tomamos $x \notin \{\tau(a_i)\}_{i=1}^r$, entonces $\tau^{-1}(x) \notin \{a_i\}_{i=1}^r$ y por lo tanto $\sigma(\tau^{-1}(x)) = \tau^{-1}(x)$. Por ende $\tau\sigma\tau^{-1}(x) = x$ en y $\tau\sigma\tau^{-1}$ funciona como la identidad fuera de $\{\tau(a_i)\}_{i=1}^r$.

Ahora tomemos $x = \tau(a_1)$, entonces

$$\tau\sigma\tau^{-1}(\tau(x)) = \tau\sigma\tau^{-1}(\tau(a_1)) = \tau\sigma(a_1) = \tau(a_2).$$

Del mismo modo, evaluando en $\tau(a_2)$ se tiene que

$$\tau\sigma\tau^{-1}(\tau(a_2)) = \tau\sigma(a_2) = \tau(a_3)$$

y en general si $i < r$ obtenemos que

$$\tau\sigma\tau^{-1}(\tau(a_i)) = \tau\sigma(a_i) = \tau(a_{i+1})$$

y además

$$\tau\sigma\tau^{-1}(\tau(a_r)) = \tau\sigma(a_r) = \tau(a_1).$$

Es decir,

$$\tau(a_1 a_2 a_3 \dots a_r)\tau^{-1} = (\tau(a_1)\tau(a_2)\tau(a_3)\dots\tau(a_r))$$

Concluimos que el conjugado de un ciclo de largo r es un ciclo de largo r. Más generalmente, si $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ es el producto de ciclos disjuntos y τ una permutación cualquiera, entonces por lo anterior $\rho_i = \tau\sigma_i\tau^{-1}$ es un ciclo del mismo largo que σ_i y además

$$\tau\sigma\tau^{-1} = \tau\sigma_1\sigma_2\sigma_3\cdots\sigma_r\tau^{-1} = \tau\sigma_1\tau^{-1}\tau\sigma_2\tau^{-1}\tau\sigma_3\tau^{-1}\tau\cdots\tau^{-1}\tau\sigma_r\tau^{-1} = \rho_1\rho_2\rho_3\cdots\rho_r.$$

Luego el conjugado de una permutación tiene la misma estructura de ciclos disjuntos que la permutación.

Recíprocamente, si $\gamma = (i_1 i_2 i_3 \dots i_r)$ y $\delta = (k_1 k_2 k_3 \dots k_r)$ son dos ciclos del mismo largo en Σ_n, consideremos $A = [n] \setminus \{i_j\}_{j=1}^r$ y $B = [n] \setminus \{k_j\}_{j=1}^r$ de manera que $|A| = |B| = n - r$. Tomemos una biyección α de A en B y definamos $\sigma \in \Sigma_n$ como sigue: $\sigma(i_j) = k_j$ para $j = [r]$ y $\sigma(x) = \alpha(x)$ si $x \notin \{i_j\}_{j=1}^r$. Por lo tanto

$$\sigma\gamma\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\sigma(i_3)\cdots\sigma(i_r)) = \delta$$

Es decir, dos ciclos del mismo largo son conjugados y por lo tanto dos permutaciones que tienen la misma estructura de ciclos disjuntos son conjugados. Obtenemos el siguiente teorema.

Teorema 2.16. *La clase de conjugación de una permutación es el conjunto de todas las permutaciones que tienen su misma estructura de ciclos.*

Dado $\tau \in \Sigma_n$ escribamos su clase de conjugación como $\mathrm{cl}(\tau)$.

Ejemplo 2.17. Consideremos $\sigma = (1234\dots n) \in \Sigma_n$ de modo que todos los elementos del grupo generado por σ conmutan con σ. La pregunta que queremos responder es si hay elementos fuera de $\langle\sigma\rangle$ que conmutan con $\langle\sigma\rangle$. Hasta el momento tenemos que al menos n elementos lo hacen. Por lo anterior, la $\mathrm{cl}(\sigma)$ tiene tantos elementos como n-ciclos hay en Σ_n, pero esta cantidad es $n!/n = (n-1)!$. Como la clase de conjugación de un elemento es el índice del centralizador del elemento en el grupo, deducimos que

$$(n-1)! = [\Sigma_n : C(\sigma)] = \frac{|\Sigma_n|}{|C(\sigma)|} = \frac{n!}{|C(\sigma)|},$$

y concluimos que $|C(\sigma)| = n$, es decir, $C(\sigma) = \langle\sigma\rangle$.

Ejemplo 2.18. Consideremos $\sigma = (12) \in \Sigma_n$. Por el teorema anterior se tiene que $|\mathrm{cl}(12)|$ es el número de transposiciones en Σ_n y entonces $|\mathrm{cl}(\sigma)| = n(n-1)/2$. Consideremos ahora $\tau = (i_1 j_1)(i_2 j_2)(i_3 j_3)\cdots(i_r j_r)$ un producto de r transposiciones disjuntas, luego

$$|\mathrm{cl}(\tau)| = \frac{n!}{2^r r!(n-2r)!}.$$

En el caso particular en que $n = 6$ y $r = 3$ se tiene que

$$|\mathrm{cl}((12)(34)(56))| = \frac{6!}{2^3 3!} = 15 = \frac{6 \times 5}{2} = |\mathrm{cl}((12))|.$$

Pero éste el único caso que esto ocurre: si $n \geq 2$, $n \neq 6$ y $1 < r \leq \frac{n}{2}$ se cumple que

$$\frac{n!}{2^r r!(n-2r)!} \neq \frac{n(n-1)}{2}.$$

Ahora bien, volvamos a nuestro estudio de los subgrupos normales de Σ_n. Consideremos un subgrupo normal propio N en Σ_n con $n \geq 5$ y tomemos $1 \neq \sigma \in N$. Como $Z(\Sigma_n) = 1$ y las transposiciones generan Σ_n, existe una transposición τen Σ_n que no conmuta con σ y consideremos la permutación $1 \neq \tau\sigma\tau\sigma^{-1} \in N$. Notemos que $\sigma\tau\sigma^{-1}$ es una transposición y entonces

$$1 \neq \tau(\sigma\tau\sigma^{-1}) \in N \cap A_n$$

Pero $\{1\} \neq A_n \cap N \lhd A_n$ implica por la simplicidad de A_n que $A_n \cap N = A_n$,, es decir $A_n \leq N$. Ahora A_n tiene índice 2 en Σ_n y entonces

$$2 = [\Sigma_n : N][N : A_n].$$

Luego $[N : A_n] = 1$ o $[\Sigma_n : N] = 1$, y concluimos que $A_n = N$ o $\Sigma_n = N$.

Teorema 2.17. *Los únicos subgrupos normales de* Σ_n *con* $n = 3$ *o* $n \geq 5$ *son* $\{1\}$, A_n *y* Σ_n.

Notemos ahora que A_3 es abeliano, y que si $n > 3$, entonces

$$(123)(124) = (13)(24) \neq (14)(23) = (124)(123)$$

luego A_n no es abeliano para $n > 3$. Por lo tanto si $n \geq 5$, entonces la única cadena de subgrupos normales que parte en $\{1\}$ y termina en Σ_n es $\{1\} \lhd A_n \lhd \Sigma_n$ pero los cuocientes Σ_n/A_n y $A_n/\{1\}$ no son todos abelianos ya que $A_n/\{1\} \cong A_n$ no lo es. Podemos resumir la discusión anterior de la siguiente manera.

Teorema 2.18. *Si* $n \geq 5$, *entonces* Σ_n *y* A_n *no son solubles.*

Para finalizar este capítulo, demostraremos que el grupo de automorfismos de Σ_n es isomorfo a Σ_n en casi todos los casos. El caso $n = 6$ se trata en el ejercicio 2.22. Primero notemos que $\mathrm{Aut}(\Sigma_1) = \{1\}$ y $\mathrm{Aut}(\Sigma_2) = \{1\}$ también.

Observación 2.9. Sean G un grupo finito, $K = \mathrm{cl}(g)$ la clase de conjugación de algún g en G y ϕ un automorfismo de G. Entonces $\phi(K) = \{\phi(xgx^{-1});\ x \in G\} = \{\phi(x)\phi(g)(\phi(x))^{-1};\ x \in G\}$. Pero si x recorre G entonces $\phi(x)$ también recorre todo G. Luego $\phi(\mathrm{cl}(g)) = \mathrm{cl}(\phi(g))$.

Ahora notemos que si G es un grupo, $g \in G$ es de orden r y ϕ es un automorfismo de G, entonces se cumple que $\phi(g)$ es un elemento de orden r: en efecto, $1 = \phi(1) = \phi(g^r) = (\phi(g))^r$ luego $\mathrm{ord}(\phi(g))$ divide a r. Como $\phi^{-1} \in \mathrm{Aut}(G)$ se cumple que $1 = \phi^{-1}((\phi(g))^{\mathrm{ord}(\phi(g))}) = g^{\mathrm{ord}(\phi(g))}$ y por lo tanto$r$ divide a $\mathrm{ord}(\phi(g))$. Entonces si ϕ es un automorfismo de Σ_n, se tiene que $\phi(\mathrm{cl}((12))) = \mathrm{cl}(\sigma)$, donde σ es una permutación de orden 2.

Observación 2.10. Sea σ de orden 2 y sea $\sigma = \sigma_1\sigma_2\sigma_3\cdots\sigma_r$ su descomposición en ciclos disjuntos tal que cada ciclo tiene largo mayor o igual a 2. Escribamos $\sigma_1 = (i_1 i_2 \ldots i_s)$ con $s \geq 2$. Como $\sigma^2 = 1$ y como los ciclos son disjuntos, entonces $\sigma_1^2\sigma_2^2\sigma_3^2\cdots\sigma_r^2 = 1$. Si $x \in \{i_1, i_2, \ldots, i_s\}$, entonces $\sigma_k^2(x) = \sigma_k(\sigma_k(x)) = \sigma_k(x) = x$ para cualquier $k \neq 1$ pues σ_k y σ_1 son disjuntas. Por lo tanto

$$\sigma_1^2(x) = \sigma_1^2\sigma_2^2\sigma_3^2\cdots\sigma_r^2(x) = \mathrm{id}(x) = x.$$

Por otra parte si $x \notin \{i_1, i_2, \ldots, i_s\}$ entonces

$$\sigma_1^2(x) = \sigma_1(\sigma_1(x)) = \sigma_1(x) = x.$$

Luego $\sigma_1^2 = 1$ y como el largo de un ciclo es el orden del ciclo y σ_1 no es la identidad, se tiene que σ_1 es una transposición. Lo mismo ocurre para σ_k con $1 < k \leq s$. Es decir, si $\sigma \in \Sigma_n$ es de orden 2, entonces σ es el producto de transposiciones disjuntas.

Recapitulando, tenemos que si $\phi \in \mathrm{Aut}(\Sigma_n)$, entonces $\phi(\mathrm{cl}((12))) = \mathrm{cl}(\sigma)$ donde σ es un producto de transposiciones disjuntas. Como ϕ es biyectiva, se tiene que $|\mathrm{cl}((12))| = |\mathrm{cl}(\sigma)|$, pero por el ejemplo 2.18 se tiene que si $n \geq 2$ y $n \neq 6$ y si $1 < r \leq n/2$, entonces

$$|\mathrm{cl}((12))| = \frac{n(n-1)}{2} \neq \frac{n!}{(n-2r)!2^r r!} = |\mathrm{cl}(\sigma)|.$$

Por lo tanto tenemos el siguiente teorema.

Teorema 2.19. *Si $n \geq 2$ y $n \neq 6$, y si ϕ es un automorfismo de Σ_n, entonces $\phi(cl((12))) = cl((12))$.*

Lo que dice el teorema anterior es que $\phi \in \mathrm{Aut}(\Sigma_n)$ induce una biyección entre las transposiciones. Para finalizar consideremos el siguiente lema técnico.

Lema 2.6. *Si $\{a_1, a_2, \ldots, a_n\} = \{1, 2, \ldots, n\}$ entonces el conjunto de transposiciones de la forma $(a_i a_{i+1})$ genera Σ_n, en particular el conjunto $\{(12), (23), (34), \ldots (n-1, n)\}$ genera Σ_n.*

La demostración es el ejercicio 2.21. Ahora observemos que si X es un conjunto de generadores de G y ϕ es un automorfismo de G tal que $\phi(x) = x$ para cada $x \in X$, entonces $\phi = \mathrm{id}_G$. Pues si $g \in G$, entonces existen $x_i \in X$ para $i \in [r]$ tales que $x = \Pi_{i=1}^r x_i$. Por lo tanto

$$\phi(g) = \phi(\Pi_{i=1}^r x_i) = \Pi_{i=1}^r \phi(x_i) = \Pi_{i=1}^r x_i = g.$$

Con todo eso en mente podemos enunciar el teorema:

Teorema 2.20. *Si $n \geq 2$ y $n \neq 6$ entonces $\mathrm{Inn}\,\Sigma_n = \mathrm{Aut}\,\Sigma_n$, y en particular $\mathrm{Aut}\,\Sigma_n \cong \Sigma_n$.*

Demostración. Sea $\phi \in \mathrm{Aut}(\Sigma_n)$, entonces $\phi(12)$ es una transposición $(a_1 a_2)$ ya que $n \geq 2$ y $n \neq 6$. Notemos que $\phi(23)$ también es una transposición (cd). Como (12) no conmuta con (23), entonces (cd) tampoco conmuta con $(a_1 a_2)$ y por lo tanto $\{a_1, a_2\} \neq \{c, d\}$ y $\{a_1, a_2\} \cap \{c, d\} \neq \emptyset$. Entonces (c, d) y $(a_1 a_2)$ comparte un solo elemento y sin restricción podemos suponer que $(cd) = (a_2 a_3) = \phi(23)$ y $|a_1, a_2, a_3| = 3$. Ahora $\phi(34)$ también es una transposición (ef), y como (34) no conmuta con (23) se tiene que (ef) tiene un único término en común con $(a_2 a_3)$, digamos $\phi(34) = (a_3 a_4)$ con $a_4 \neq a_2$. Si $a_4 = a_1$ entonces $(a_1 a_2)$ y $(a_3 a_4)$ tendrían solo un valor en común y no conmutarían, pero (12) y (34) lo hacen pues son dijuntas y obtenemos una contradicción. Luego $a_4 \neq a_1$. Entonces tenemos que $\phi(12) = (a_1 a_2)$, $\phi(23) = (a_2 a_3)$ y $\phi(34) = (a_3 a_4)$, con $4 = |\{a_1, a_2, a_3, a_4\}|$.

Continuando con este proceso, tenemos que $\phi(i,i+1) = (a_i a_{i+1})$ con $\{a_1, a_2, \ldots, a_n\} = [n]$. Consideremos la permutación $\sigma \in \Sigma_n$ que lleva i en a_i y consideremos el automorfismo interior ϕ_σ. Entonces $\phi_\sigma(i,i+1) = \sigma(i,i+1)\sigma^{-1} = (\sigma(i), \sigma(i+1)) = (a_i, a_{i+1})$. Por lo tanto $\phi^{-1}\phi_\sigma(i,i+1) = (i,i+1)$. Como $\{(12),(23),(34),\ldots(n-1,n)\}$ genera Σ_n, entonces $\phi^{-1}\phi_\sigma = 1$ y por lo tanto $\phi = \phi_\sigma$. Es decir, todo automorfismo es un automorfismo interior y $\mathrm{Aut}(\Sigma_n) = \mathrm{Inn}(\Sigma_n)$. La segunda afirmación del teorema sigue de recordar que $\mathrm{Aut}(\Sigma_n)/Z(\Sigma_n) \cong \mathrm{Inn}(\Sigma_n)$. □

2.5. Productos directos y semidirectos

En esta sección estudiaremos maneras de crear nuevos grupos a partir de productos de otros grupos, y cómo reconocer cuándo un grupo dado es isomorfo a un producto de ese tipo.

Dada una colección arbitraria de grupos $\{(G_i, \cdot_i\}_{i\in I}$, definimos su *producto directo externo* como el grupo

$$\prod_{i\in I} G_i = \{f : I \to \bigcup_{i\in I} G_i;\ f(i) \in G_i\ \forall i \in I\}$$

dotado de la multiplicación por componentes, es decir $f \cdot g$ está definida por $f(i) \cdot_i g(i)$ para cada i. Es directo verificar que $\prod_i G_i$ es un grupo y que es abeliano ssi cada G_i lo es. Además, los grupos $\bar{G}_j = G_j \times \prod_{i\neq j}\{e_i\}$ son subgrupos normales de $\prod_i G_i$ e isomorfos a los G_j. Definimos también la *suma directa externa* de los G_i como el conjunto de funciones de soporte finito

$$\bigoplus_{i\in I} G_i = \{f \in \prod_i G_i;\ f(i) \neq e_i \text{ salvo para un subconjunto finito de } I\}.$$

Es un subgrupo normal de $\prod_i G_i$, y coincide con éste cuando I es finito.

Sea G un grupo y $\{H_i\}_{i=1}^n$ una colección finita de subgrupos normales de G. Decimos que G es el *producto directo interno* de los subgrupos H_i si $G = H_2 \cdots H_n$ y si $h_i, k_i \in H_i$ para cada i, entonces la igualdad $h_1 \cdots h_n = k_1 \cdots k_n$ implica que $h_i = k_i$ para cada i. La proposición 2.9 dice que los productos directos internos son básicamente productos directos externos, y para su demostración necesitamos un lema.

Lema 2.7. *Si H, N son subgrupos normales de un grupo G y $N \cap H = \{1\}$, entonces todos los elementos de H conmutan con todos los elementos de N.*

Demostración. Sea $n \in N$, $h \in H$. Notemos que el *conmutador* de n y h dado por $nhn^{-1}h^{-1}$ cumple que

$$N \ni n(hn^{-1}h^{-1}) = (nhn^{-1})h^{-1} \in H$$

pues N y H son normales. Luego $nhn^{-1}h^{-1} = 1$, es decir, $nh = hn$. □

Proposición 2.9. *Sea G grupos y $H_i \lhd G$ para $i \in [n]$ tal que $G = H_1 \cdots H_n$. Las siguientes afirmaciones son equivalentes:*

1. *G es el producto directo interno de los H_i.*
2. *$G \cong H_1 \times \cdots H_n$.*
3. *$H_i \cap H_1 \cdots H_{i-1} H_{i+1} \cdots H_n = \{1\}$ para cada $i \in [n]$.*
4. *$H_i \cap H_1 \cdots H_{i-1} = \{1\}$ para cada $i \in [n]$.*

Demostración. La implicancia $2 \Rightarrow 1$ es directa. Recíprocamente, si G es el producto interno de los H_i tenemos que $g = h_1 \cdots h_n \in G \mapsto (h_1, \ldots, h_n) \in H_1 \times \cdots H_n$ está bien definida (por la condición de unicidad en la escritura), es claramente biyectivo y además es morfismo ya que los H_i son normales en G y $H_i \cap H_j = \{1\}$ si $i \neq k$ (y entonces sus elementos conmutan entre sí). Luego $G \cong H_1 \times \cdots H_n$. Concluimos que 1 es equivalente a 2.

La implicancia $1 \Rightarrow 3$ resulta de notar que si $h_i = h_1 \cdots h_{i-1} h_{i+1} \cdots h_n$ con cada $h_j \in H_j$, entonces la igualdad $1 \cdots 1 h_i 1 \cdots 1 = h_1 \cdots h_{i-1} 1 h_{i+1} \cdots h_n$ implica que $h_j = 1$ para todo j, ya que el neutro 1 está en cada H_j y tenemos la condición de escritura única que garantiza 1. La implicancia $3 \Rightarrow 4$ es trivial.

Finalmente, veamos que $4 \Rightarrow 1$: tomemos $h_j, k_j \in H_j$ para cada j tal que $h_1 \cdots h_n = k_1 \cdots k_n$. Escribiendo la ecuación como $h_n k_n^{-1} = h_{n-1}^{-1} \cdots h_1^{-1} k_1 \cdots k_{n-1}$ y notando que los elementos de distintos H_j conmutan entre sí pues éstos son normales y la hipótesis 3. implica que $H_i \cap H_j = \{1\}$ para $i \neq j$, podemos escribir lo anterior como $h_n k_n^{-1} = s_1 \cdots s_{n-1}$ donde los $s_i = h_i^{-1} k_i \in H_i$. Luego $h_n = k_n$, y un argumento inductivo muestra que para cada i se cumple que $h_i = k_i$. Concluimos que G es el producto directo interno de los H_i. □

Ahora examinemos el caso cuando $n = 2$: el desarrollo anterior muestra que dados N, H grupos cualquiera, podemos formar un grupo G que los contiene tal que $N, H \lhd G$, $NH = G$ y $N \cap H = \{1\}$. Además, la proposición anterior entrega herramientas para ver cuándo un grupo G se puede escribir de esta forma. Queremos estudiar ahora el caso en que N es normal en G pero K no necesariamente lo es. Notemos que NH es grupo por la proposición 2.1 , y que cada $g \in HK$ se puede escribir de manera única como $g = nh$ con $n, \in N$, $h \in H$ pues el mapa $\psi : NH \to N \times H$ es claramente sobreyectivo y es inyectivo ya que $N \cap H = \{1\}$ (ojo: no es morfismo en general). Luego el producto de dos elementos $n_1 h_1, n_2 h_2 \in NH$ se puede escribir como

$$(n_1 h_1)(n_2 h_2) = n_1 (h_1 n_2 h_1^{-1})(h_1 h_2) = n_3 h_3$$

donde $n_3 = n_1 h_1 n_2 h_1^{-1} \in N$ (pues N es normal) y $h_3 = h_1 h_2$. De manera análoga al producto directo, dados N, H grupos cualquiera queremos construir un grupo G que contiene copias isomorfas de N y H tal que $N \cap H = \{1\}$, $NH = G$ y $N \lhd G$. La idea es usar la ecuación 2.5 para definir la multiplicación en G, y para ello debemos fijar el significado del término hnh^{-1} donde $n \in N$, $h \in H$, es decir, debemos partir por la definición de una acción de H en N.

Dados N, H grupos cualquiera y un morfismo $\phi : H \to \mathrm{Aut}(N)$, definimos el *producto semidirecto* de N y H con respecto a ϕ al grupo $N \rtimes_\phi H \doteq N \times H$ dotado de la operación $(n_1, h_1)(n_2, h_2) \doteq (n_1 \phi(h_1)(n_2), h_1 h_2)$. Es un ejercicio tedioso pero directo verificar que $N \rtimes_\phi H$ es un grupo, y que los mapeos $n \in N \mapsto (n, 1) \in N \rtimes_\phi H$ y $h \in H \mapsto (1, h) \in N \rtimes_\phi H$ son isomorfismos. De aquí vemos que (identificando N y H con sus copias isomorfas en el producto) $N \cap H = \{1\}$.

Por otro lado, notemos que si $n \in N$, $h \in H$ entonces

$$\begin{aligned}(1,h)(n,1)(1,h)^{-1} &= (\psi(h)(n),h)(1,h^{-1}) \\ &= (\psi(h)(n)\psi(h)(1),hh^{-1}) \\ &= (\psi(h)(n),1).\end{aligned}$$

Luego la acción de H en N por conjugación es la misma acción definida por ψ. Por último, el cálculo anterior muestra que H normaliza H. Como N también se normaliza a sí mismo y $N \rtimes_\psi H = NH$, concluimos que N es normal en $N \rtimes_\psi H$. Hemos demostrado el siguiente resultado.

Proposición 2.10. *Dados N,H grupos y $\phi : H \to \mathrm{Aut}(N)$, tenemos que $N \rtimes_\phi H$ es un grupo que contiene copias $\bar{N},\bar{H}$ de N,H respectivamente tal que $\bar{N} \cap \bar{H} = \{1\}$, $\bar{N} \lhd N \rtimes_\phi H$ y $N \rtimes_\phi H = \bar{N}\bar{H}$.*

Notemos que cuando el morfismo ψ es trivial obtenemos que $N \rtimes_\psi H$ es el producto directo usual de N y H.

2.6. Ejercicios

Ejercicio 2.1. Complete la demostración del teorema 2.6.

Ejercicio 2.2.

a) Muestre que si G es un semigrupo finito tal que cada elemento es cancelable, entonces G es grupo. ¿Es necesaria la finitud de G?

b) Muestre que si G es un semigrupo, las siguientes condiciones son equivalentes:
   1. G es grupo.
   2. Existe un neutro por la izquierda y cada elemento tiene inverso por la izquierda.
   3. Para cada par $a,b \in G$ las ecuaciones $ax = b$, $ya = b$ tienen solución en G.

   ¿Qué ocurre si en 3. reemplazamos 'cada elemento tiene inverso por la izquierda ' por 'cada elemento tiene inverso por la derecha'?

c) Muestre que si G es grupo y $H \subset G$ es finito, entonces $H \leq G$ ssi H es cerrado bajo el producto en G.

Ejercicio 2.3. Sea G un grupo. Muestre que las siguientes condiciones son equivalentes:

1. G es abeliano.
2. $(ab)^2 = a^2b^2$ para todo $a,b \in G$.
3. $(ab)^{-1} = a^{-1}b^{-1}$ para todo $a,b \in G$.
4. $(ab)^n = a^nb^n$ para todo $n \in \mathbb{Z}$ y todo $a,b \in G$.
5. $(ab)^n = a^nb^n$ para tres enteros consecutivos n y todo $a,b \in G$.

¿Qué ocurre si en 5. reemplazamos 'tres enteros consecutivos' por 'dos enteros consecutivos'?

Ejercicio 2.4. Dado $n \in \mathbb{N}$ sea $\mu_n = \{z \in \mathbb{C}; z^n = 1\}$ el grupo de las raíces n-ésimas de la unidad y sea $\mu(\mathbb{C}) = \{z \in \mathbb{C}; \exists m \in \mathbb{N} \text{ tal que } z^m = 1\}$ el grupo de las raíces de la unidad. Pruebe que $(\mathbb{Q}/\mathbb{Z},+) \cong (\mu(\mathbb{C}),\cdot)$, $(\mathbb{R}/\mathbb{Z},+) \cong (S_1,\cdot)$ y $(\mathbb{C}^*,\cdot)/\mu_n(\mathbb{C}) \cong (\mathbb{C}^*,\cdot)$ para cada $n \in \mathbb{N}$. Concluya que para cualquier $k \in \mathbb{N}$, $(\mathbb{Q}/\mathbb{Z},\cdot)$ contiene un único subgrupo de orden k y que además todos son cíclicos.

Ejercicio 2.5. Sean G_1, G_2 grupos y $H_1 \lhd G_1$, $H_2 \lhd G_2$. Decida y justifique la veracidad de las siguientes afirmaciones:

a) $G_1 \cong G_2$ y $H_1 \cong H_2 \implies G_1/H_1 \cong G_2/H_2$.
b) $G_1 \cong G_2$ y $G_1/H_1 \cong G_2/H_2 \implies H_1 \cong H_2$.
c) $H_1 \cong H_2$ y $G_1/H_1 \cong G_2/H_2 \implies G_1 \cong G_2$.
d) Todo grupo tiene un automorfismo no trivial.
e) Para cada grupo G existe un $n \in \mathbb{N}$ tal que G es isomorfo a un subgrupo de A_n.
f) Existen grupos simples de orden pq^2 donde p y q son primos distintos.
g) La imagen epimorfa de un grupo soluble es soluble.
h) Un subgrupo de un grupo soluble es soluble.
i) Para $N \lhd G$, G es soluble ssi N y G/N lo son.

Ejercicio 2.6.

a) Sea G un grupo abeliano finito y $x = \prod_{g \in G} g$. Muestre que $g^2 = 1$.
b) Pruebe el teorema de Wilson: para cada $p \in \mathbb{N}$ se tiene que $(p-1)! \equiv -1 \mod p$.

Ejercicio 2.7. Determine $\mathrm{Aut}(\mathbb{Z})$ y $\mathrm{Aut}(\mathbb{Z}_n)$ para todo $n \in \mathbb{N}$.

Ejercicio 2.8. Usando el teorema de Lagrange, muestre que si $n, m_1, \ldots, m_k$ son enteros positivos tales que $m_1 + \ldots + m_k = n$, entonces el coeficiente multinomial $\binom{n}{m_1,\ldots,m_k} \doteq n!/\prod_i m_i!$ es un entero positivo, y muestre que para cada $n \in \mathbb{N}$, $n > 1$, se tiene que $\varphi(n)$ es par.

Ejercicio 2.9. Usando el teorema de Cauchy, muestre que cualquier cuerpo finito tiene orden p^n donde p es primo y n es un natural positivo.

Ejercicio 2.10. Sea G un grupo de orden n y $k \in \mathbb{Z}$. Pruebe que las siguientes afirmaciones son equivalentes:

1. k es invertible en $\mathbb{Z}_n^\times$.
2. La ecuación $x^k = e$ tiene una única solución en G.
3. La función $g \mapsto g^k$ es biyectiva en G.

Ejercicio 2.11. Sea F un cuerpo finito de orden q.

a) Determine el orden de $\mathrm{GL}_n(F)$.
b) Muestre que $q^{\frac{n(n-1)}{2}}$ divide a $|\mathrm{GL}_n(F)|$.
c) Pruebe que $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \cong F^\times$.

Ejercicio 2.12.

a) Sea G un grupo de orden n. Muestre que

$$n = \sum_{d|n} \varphi(d) |\{H \subset G; |H| = d \text{ y } H \text{ cíclico}\}|.$$

Indicación: cuente elementos de orden d.
¿Qué nos dice esto si $G = \mathbb{Z}_n$?

b) Demuestre que las condiciones siguientes son equivalentes para un grupo finito G:
   1. G es cíclico.
   2. G contiene a lo más un subgrupo cíclico de cada tamaño.
   3. G contiene a lo más un subgrupo de cada tamaño.
   4. Para cada d divisor de $|G|$, la ecuación $x^d = 1$ tiene a lo más d soluciones en G.

   ¿Qué pasa si G es infinito?

c) Muestre que si G es un subgrupo finito de $F^\times \doteq F\setminus\{0\}$ donde F es un cuerpo, entonces G es cíclico.

Ejercicio 2.13. Sea G un grupo cualquiera. Definimos el *conmutador* de a y $b \in G$ como $[a,b] = aba^{-1}b^{-1}$ y el *subgrupo conmutador* o *subgrupo derivado* de G como $G' = \langle\{[a,b]; a,b \in G\}\rangle$.

a) Muestre que G' es característico en G y que G/G' es abeliano.

b) Pruebe que si $N \lhd G$ es tal que G/N es abeliano, entonces $G' \subset N$. Muestre también que si $G' \leq H \leq G$, entonces $H \lhd G$.

G/G' se llama la *abelianización* de G.

c) Definamos $G^0 = G$ e inductivamente $G^k = (G^{k-1})'$. Muestre que G es soluble ssi existe $k \in \mathbb{N}$ tal que $G^k = \{1\}$.

d) Pruebe que cada G^i es característico en G.

La cadena

$$G = G^0 \leq G' = G^1 \leq G^2 \leq \cdots \leq G^k \leq \cdots$$

se llama la cadena *derivada* de G.

Ejercicio 2.14. Sea G un grupo cualquiera. Definimos los *centros de orden* k para $k \in \mathbb{N}$ inductivamente como los siguientes subgrupos característicos de G: $Z_0(G) = \{1\}$ y si $Z_k(G) \lhd G$ ya está definido, consideramos el cociente $G/Z_k(G)$.

a) Muestre que el centro de $G/Z_k(G)$ es de la forma $Z(G/Z_k(G)) = H/Z_k(G)$ con $Z_k(G) \subseteq H \leq G$ y H es característico en G.

Este subgrupo $H \leq G$ será por definición $Z_{k+1}(G)$. De esta manera generamos la cadena creciente (no necesariamente estrictamente) de subgrupos característicos de G dada por

$$\{1\} = Z_0(G) \leq Z(G) = Z_1(G) \leq Z_2(G) \leq \cdots \leq Z_k(G) \leq \cdots$$

Esta cadena se llama la *cadena central superior* de G, y diremos que G es *nilpotente* si $Z_k(G) = G$ para algún $k \in \mathbb{N}$.

b) Decida y justifique si son o no nilpotentes
   a) Un grupo abeliano G.
   b) $G = \Sigma_n$ para $n \geq 2$.
   c) $G = A_n$ para $n \geq 3$.
   d) Un p-grupo finito G, donde p es primo.

Ahora nos proponemos probar que si G es un grupo nilpotente finito con $|G| = p^k q^k$ (donde p, q son primos distintos), P es un p-subgrupo de Sylow de G y Q es un q-subgrupo de Sylow de G, entonces $G \cong P \times Q$.

c) Pruebe el siguiente lema: Sea G un grupo finito nilpotente y $H < G$ un subgrupo estricto de G. Luego $H < N_G(H)$.
Indicación: Verifique que existe un k tal que $Z_k(G) \subseteq H$ pero $Z_{k+1}(G) \nsubseteq H$, y muestre que $Z_{k+1}(G) \subseteq N_G(H)$.

d) Pruebe el siguiente lema: Sean G un grupo finito, p un número primo y $P \subseteq G$ un p-subgrupo de Sylow de G. Sea también H un subgrupo de G tal que $N_G(P) \subseteq H$. Entonces $N_G(H) = H$.
Indicación: Verifique primero que xPx^{-1} es un p-subgrupo de Sylow de H para cada $x \in N_G(H)$.

e) Muestre que bajo las hipótesis de la proposición a probar, P y Q son subgrupos normales de G y concluya lo pedido.

f) Generalice lo anterior a $|G| = p_1^{k_1} \cdots p_r^{k_r}$ donde los p_i son primos distintos entre sí.

Ejercicio 2.15.

a) Sea G un grupo actuando sobre un conjunto X. Muestre que

$$|\{\text{Orb}(x); x \in X\}||G| = \sum_{g \in G} \text{Fix}_X(g).$$

Este resultado se conoce como el lema de Cauchy-Frobenius (o el lema que no es de Burnside).
Indicación: considere el conjunto $\{(g, x) \in G \times X; g.x = x\}$.

b) Sean X es un conjunto finito, G un grupo finito que actúa sobre X e Y un conjunto finito de cardinal m. Consideremos la acción natural de G en Y^X por componentes. Pruebe que

$$|Y^X/G| = \frac{1}{|G|} \sum_{g \in G} m^{c(g)}$$

donde $c(g)$ es el número de ciclos de g cuando interpretamos g como una permutación de X. Este resultado se conoce como el teorema de enumeración de Pólya sin peso.

c) Calcule el número de maneras en que se pueden pintar con n colores los lados de un polígono regular de 20 aristas si consideramos que dos coloraciones son iguales cuando difieren en una simetría de D_{40}.

Ejercicio 2.16. Sea G un grupo y H un subgrupo de índice finito en G. Suponga que H no tiene elementos de orden finito salvo 1. Sea A un subgrupo finito de G. Demuestre que $|A|$ divide a $[G : H]$.
Indicación: haga actuar A en el conjunto de clases laterales de H y determine el número de elementos de cada órbita.

Ejercicio 2.17. En este ejercicio demostraremos el teorema de Cauchy sin recurrir al lema 2.1.

a) Demuestre el teorema para grupos cíclicos.

b) Pruebe que para cada grupo G y $N \lhd G$, si G/N tiene un elemento de orden p primo entonces G tiene un elemento de orden p.

c) Considerando un subgrupo cíclico no trivial y aplicando inducción, muestre el teorema para grupos abelianos no cíclicos.

d) Demuestre que para todo grupo finito G y $x \in G$, el tamaño de su clase de conjugación es igual al índice del centralizador de g en G.
e) Pruebe el teorema para grupos no abelianos.
Indicación: Use la ecuación de clases y aplique inducción.

Ejercicio 2.18. Sea G un grupo finito de orden pqr donde $p,q,r \in \mathbb{N}$ son primos distintos, y sea n_k el número de k-grupos de Sylow para $k \in \{p,q,r\}$. Muestre que

$$n_p(p-1) + n_q(q-1) + n_r(r-1) \leq pqr.$$

¿Su argumento funciona si $|G|$ es el producto de más de tres primos distintos?

Ejercicio 2.19. Muestre que el número de clases de conjugación en Σ_n es el número de particiones de n (es decir, el número de tuplas $n_1 \geq n_2 \geq \ldots \geq n_s > 0$ tales que $n_1 + \ldots + n_s = n$) y calcule el número de k-ciclos distintos en Σ_n para $k \in \{1,\ldots,n\}$.

Ejercicio 2.20. Pruebe que el orden de una permutación es el mcm de los largos de sus ciclos disjuntos.

Ejercicio 2.21. Muestre que los siguientes conjuntos generan Σ_n para $n \geq 2$:
1. $\{(12),(13),(14),\ldots,(1,n)\}$
2. $\{(12),(23),(34),\ldots,(n-1\,n)\}$
3. $\{(12),(1234\ldots n)\}$

Para $\sigma \in \Sigma_n$, ¿ocurre lo mismo si reemplazamos $1,2,3,\ldots,n$ por $\sigma(1),\sigma(2),\sigma(3),\ldots,\sigma(n)$? Pruebe también que si p es primo, entonces una transposición y un p-ciclo generan Σ_p.

Ejercicio 2.22. Sea K_1 la clase de conjugación de (12) en Σ_6 y K_2 la clase de conjugación de $(12)(34)(56)$ en Σ_6.
a) Muestre que si $\psi \in \mathrm{Aut}(\Sigma_6)$, entonces $\psi(K_1) = K_1$ o $\psi(K_1) = K_3$.
b) Muestre que si $\psi \in \mathrm{Aut}(\Sigma_6)$ y $\psi(K_1) = K_1$, entonces ψ es un automorfismo interior.
c) Muestre que $\mathrm{Aut}(\Sigma_6)/\mathrm{Inn}(\Sigma_6)$ es de orden a lo más 2.
d) Decimos que un subgrupo H de Σ_n es transitivo si para todo par de elementos $i,j \in I_n$, existe $\sigma \in H$ tal que $\sigma(i) = j$ (es decir, si consideramos la acción natural de H sobre $X = \{1,\ldots,n\}$, la órbita de cada elemento es todo X). Sea $\Sigma_6(i) = \{\sigma \in \Sigma_6; \sigma(i) = i\}$. Muestre que si $\phi \in \mathrm{Aut}(\Sigma_6)$ y $\psi(\Sigma_6(i))$ es un subgrupo transitivo de Σ_6, entonces ψ no es un automorfismo interior.
e) Muestre que Σ_5 tiene un subgrupo de índice 6.
f) Sea N un subgrupo de índice 6 en Σ_5 y sea Ω el conjunto de las clases laterales de N en Σ_5. Para cada $\tau \in \Sigma_5$ definimos $\psi_\tau : \Omega \to \Omega$ por $\psi_\tau(\sigma N) = (\tau\sigma)N$. Muestre que $\psi : \Sigma_5 \to \Sigma_\Omega$ definida por $\psi(\tau) = \psi_\tau$ es un monomorfismo de grupos cuya imagen es un subgrupo transitivo de Σ_Ω.
g) Concluya que $\mathrm{Inn}(\Sigma_6)$ es un subgrupo de índice 2 en $\mathrm{Aut}(\Sigma_6)$.

Capítulo 3

Anillos

3.1. Definiciones y ejemplos básicos

Para nosotros un *anillo* $(R,+,\cdot)$ es un conjunto no vacío R junto con dos operaciones binarias $+$ y $\cdot$ que llamamos suma y multiplicación tales que:

1. $(R,+)$ es un grupo abeliano con neutro 0.
2. La multiplicación es asociativa.
3. La multiplicación distribuye respecto a la suma.
4. Existe un neutro para la multiplicación $1 \neq 0$.

En lo sucesivo escribiremos $\cdot$ por yuxtaposición y denotaremos $R^* = R\backslash\{0\}$.

Una tupla $(R,+,\cdot)$ que cumpla los axiomas anteriores salvo 4 se dice anillo *no unitario*. Si la multiplicación en R es conmutativa, diremos que R es un anillo *conmutativo*. Un elemento invertible para la multiplicación se dice *unidad*, y el conjunto de unidades en R se denota $R^\times$. Un anillo donde todo elemento no nulo es unidad se dice *anillo de división*, y un anillo de división conmutativo se dice *cuerpo* . Un elemento $x \in R$ tal que existe $z \in R^*$ que verifica $xz = 0$ ($zx = 0$) se dice *divisor de cero por la izquierda (derecha)*, y diremos que x es *divisor de cero* si lo es por la izquierda y la derecha. Un anillo conmutativo sin divisores de cero se dice *dominio de integridad* o *dominio entero*, o simplemente *dominio*. Esta condición es equivalente a que cada elemento es cancelable para la multiplicación.

El anillo $\mathbb{Z}_m$ es un anillo conmutativo cuyo conjunto de unidades es $\mathbb{Z}_m^\times$ (definido en el capítulo 1) y cuyo conjunto de divisores de cero es $\mathbb{Z}_m\backslash\mathbb{Z}_m^\times$. Es decir, cada elemento en $\mathbb{Z}_m$ es unidad o divisor de cero. El conjunto de matrices cuadradas de tamaño n a coeficientes en un cuerpo K es un anillo no conmutativo y con divisores de cero para $n \geq 2$. El anillo de polinomios sobre una variable $K[X]$ a coeficientes en un cuerpo y el anillo de enteros $\mathbb{Z}$ son ejemplos clásicos de dominios de integridad, cuyo conjunto de unidades son los polinomios de grado 0 y $\{1,-1\}$ respectivamente. Los ejemplos típicos de cuerpos son $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{Z}_p$ con p primo. Veremos más en el capítulo 5.

Si R es un anillo y $x \in R$ entonces $x + x0 = x(1+0) = x1 = x$ de modo que $x0 = 0$, y análogamente $0x = 0$. También se tiene que $(-1)x + x = (-1+1)x = 0x = 0$ y por lo tanto $(-1)x = -x$. Notemos ahora

que $(-x)y + xy = (-x+x)y = 0y = 0$, luego $(-x)y = -xy$ y del mismo modo $x(-y) = -xy$. Finalmente, tenemos que $(-x)(-y) + (-xy) = (-x)(-y) + x(-y) = ((-x)+x)y = 0y = 0$ implica que $(-x)(-y) = xy$.

El párrafo anterior muestra que un elemento $x \in R$ anillo no puede ser unidad y divisor del cero simultáneamente, pues si $xz = 0$ para algún $z \in R$, entonces $x^{-1}xz = z = x^{-1}0 = 0$.

Observación 3.1. Si D es un dominio de integridad finito, entonces D es un cuerpo: consideremos $a \in D$ no nulo y la función $\phi : D \to D$ definida por $\phi(x) = ax$. Si $\phi(x) = \phi(y)$ se tiene que $a(x-y) = 0$, luego como D es un dominio y $a \neq 0$ necesariamente $x - y = 0$ y por lo tanto ϕ es inyectiva. Como D es finito, entonces ϕ también es biyectiva y existe $z \in D$ tal que $\phi(z) = 1$, es decir $az = 1 = za$. Luego D es un cuerpo.

Ejemplo 3.1. El conjunto $\mathbb{Z}[i] = \{a + bi;\ a, b \in \mathbb{Z} \text{ e } i^2 = -1\}$ es un anillo con la suma y producto usual de $\mathbb{C}$. Si $\overline{z}$ denota el conjugado de $z \in \mathbb{Z}[i]$, entonces el conjugado de z es un elemento de $\mathbb{Z}[i]$ y además el número complejo $z\overline{z} = a^2 + b^2 \in \mathbb{Z}$ si $z = a + bi$. Si escribimos $\sqrt{z\overline{z}} = |z|$ podemos ver que $|zw| = |z||w|$ con $z, w \in \mathbb{Z}[i]$ y también $z = 0$ ssi $|z| = 0$. Por lo tanto $\mathbb{Z}[i]$ no tiene divisores de cero: en efecto, si $zz' = 0$ entonces $|z||z'| = |zz'| = 0$ por lo tanto $|z| = 0$ o $|z'| = 0$, es decir, $z = 0$ o $z' = 0$. Si z es una unidad en $\mathbb{Z}[i]$ llamemos w a su inverso, entonces $|z||w| = |zw| = |1| = 1$ de manera que $|z|$ es unidad en $\mathbb{Z}$, es decir, $|z| = 1$. Por lo tanto las únicas unidades de $\mathbb{Z}[i]$ son $1, -1, i$ y $-i$. El anillo $\mathbb{Z}[i]$ se llama el anillo de *enteros Gaussianos*.

Ejemplo 3.2. El conjunto $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2}/\ a, b \in \mathbb{Z} \text{ y } (\sqrt{-2})^2 = -2\}$ es un anillo con la suma y producto usual de $\mathbb{C}$, cuyas únicas unidades son 1 y -1.**[Ejercicio]**

Ejemplo 3.3. Sea $\mathbb{Q}[\sqrt{2}] = \{p(\sqrt{2})/p(X) \in \mathbb{Q}[X]\}$ es el conjunto de todos los polinomios con coeficientes racionales evaluados en $\sqrt{2}$, es un subconjunto de $\mathbb{R}$. Toda potencia par de $\sqrt{2}$ es un número racional (de hecho es entero), y toda potencia impar de $\sqrt{2}$ es un múltiplo entero de $\sqrt{2}$, por lo tanto $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}/\ a, b \in \mathbb{Q}\}$ con la suma y multiplicación usual de $\mathbb{R}$ se tiene que $\mathbb{Q}[\sqrt{2}]$ es una anillo. Como $\sqrt{2} \notin \mathbb{Q}$, se tiene que los únicos racionales a y b que satisfacen $a^2 - 2b^2 = 0$ son $a = 0 = b$. Por lo tanto si $a + b\sqrt{2} \neq 0$, entonces $a \neq 0$ o $b \neq 0$, en cualquier caso $0 \neq a^2 - 2b^2 \in \mathbb{Q}$ por lo tanto el número real

$$\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

es un elemento de $\mathbb{Q}[\sqrt{2}]$, y además

$$(a + b\sqrt{2})\left(\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}\right) = 1$$

Como $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$, entonces $\mathbb{Q}[\sqrt{2}]$ es conmutativo y como vimos arriba es anillo de división, por lo tanto $\mathbb{Q}[\sqrt{2}]$ es un cuerpo.

Ejemplo 3.4. El conjunto de las funciones continuas $f : [0,1] \to \mathbb{R}$ es una anillo con la suma $f + g : [0,1] \to \mathbb{R}$ definida por $(f+g)(x) = f(x) + g(x)$ y el producto $fg : [0,1] \to \mathbb{R}$ definida por $fg(x) = f(x)g(x)$. El neutro aditivo es la función nula (constante igual a cero) y el neutro multiplicativo es la función constante igual a 1. Este anillo es conmutativo, pero no es un dominio de integridad.**[Ejercicio].**

Ejemplo 3.5. El conjunto $\mathbb{H}$ de las matrices cuadradas de 2×2 a coeficientes en $\mathbb{C}$ de la forma

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$$

forman un anillo con la suma y multiplicación habitual de matrices: la suma y la multiplicación son cerradas en $\mathbb{H}$ pues cuando $a,b,c,d\in\mathbb{C}$ tenemos que

$$-\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}=\begin{pmatrix} -a & -b \\ \overline{b} & -\overline{a} \end{pmatrix}=\begin{pmatrix} -a & -b \\ \overline{-(-b)} & \overline{(-a)} \end{pmatrix}$$

y

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}\begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix}=\begin{pmatrix} ac-b\overline{d} & ad+b\overline{c} \\ -c\overline{b}-\overline{a}\overline{d} & -d\overline{b}+\overline{a}\overline{c} \end{pmatrix}$$

$$=\begin{pmatrix} ac-b\overline{d} & \overline{ad+b\overline{c}} \\ \overline{-(ad+b\overline{c})} & \overline{(ac-b\overline{d})} \end{pmatrix}.$$

Las otras propiedades ambas operaciones se heredan directamente de $M_2(\mathbb{C})$, y la identidad de $\mathbb{H}$ corresponde a $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Luego $\mathbb{H}$ es efectivamente un anillo.

Podemos notar además que $\mathbb{H}$ no es conmutativo, pues si tomamos las matrices $i=\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ y la matriz $j=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ vemos que no conmutan:

$$ij=\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\neq\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}=ji.$$

Por otra parte el determinante de un elemento $x\in\mathbb{H}$ es

$$\det(x)=\det\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}=|a|^2+|b|^2$$

donde $|a|=|\alpha+\beta i|=\sqrt{\alpha^2+\beta^2}=\sqrt{a\overline{a}}$. Por lo tanto,si $x\neq 0$ denotamos $\Delta=\det(x)=|a|^2+|b|^2$ tenemos que la inversa de x en $M_2(\mathbb{C})$ es

$$x^{-1}=\frac{1}{\Delta}\begin{pmatrix} \overline{a} & (-b) \\ \overline{b} & a \end{pmatrix}\in\mathbb{H}.$$

Entonces $\mathbb{H}$ es un anillo de división no conmutativo. Además $\mathbb{H}$ es un espacio vectorial sobre $\mathbb{R}$ de dimensión 4 y una base de $\mathbb{H}$ sobre $\mathbb{R}$ es $\{1,i,j,k=ij\}$. Notamos que $i^2=j^2=k^2=-1$ y además $ij=k=-(ji)$, $jk=i=-(kj)$ y $ki=j=-(ik)$. Por lo tanto otra forma de ver $\mathbb{H}$ es el espacio vectorial de dimensión 4 sobre $\mathbb{R}$ con base $\{1,i,j,k\}$ y con tabla de multiplicación como la de arriba. Al conjunto $\mathbb{H}$ se le llama *álgebra de Hamilton* o *álgebra de cuaterniones*.

Si R es un anillo y $x \in R$, entonces definimos x^k con $k \in \mathbb{N}$ (y $k \in \mathbb{Z}$ si $x \in R^\times$) de la misma manera que en el capítulo 2. Se cumplen las mismas identidades $x^{m+n} = x^m x^n$ y $(x^n)^m = x^{mn}$ para $n, m \in \mathbb{N}$ (las demostraciones involucradas sólo usan propiedades de semigrupo cuando n y m son nonegativos).

Ahora notemos que si x, y están un anillo no necesariamente conmutativo R, entonces $(x+y)^2$ no es necesariamente $x^2 + 2xy + y^2$. Sin embargo, si R es un anillo conmutativo y $n \in \mathbb{N}$, entonces se cumple el teorema del binomio de Newton

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

y más generalmente,

$$(x_1 + \cdots + x_r)^n = \sum_{\substack{n_1,\ldots,n_r \in \mathbb{N}; \\ n_1+\cdots+n_r=n}} \binom{n}{n_1, \ldots, n_r} x_1^{n_1} \ldots x_r^{n_r}$$

donde $\binom{n}{n_1,\ldots,n_r} \doteq n!/\prod_i n_i!$, los x_i están en R y la suma se extiende sobre todas las soluciones naturales de la ecuación $n_1 + \cdots + n_r = n$.

Ejemplo 3.6. Un anillo se llama *Booleano* o *de Boole* si para cada elemento $x \in R$ se cumple que $x^2 = x$. Por ejemplo, $\mathbb{Z}_2$ es un anillo Booleano. Si un anillo es Booleano, entonces $x + x = 0$ para cada elemento de R, es decir, cada elemento de un anillo Booleano es su propio inverso aditivo: como $(x+1)^2 = x+1$, la distributividad implica que $(x+1)(x+1) = x^2 + x + x + 1$ y por lo tanto $x^2 + x = 0$, es decir $x + x = 0$. Además notamos que $(x+y)^2 = x+y$, es decir $x^2 + xy + yx + y^2 = x + y$, como $x^2 = x$ y $y^2 = y$, entonces $xy + yx = 0 = xy + xy$, por lo tanto $xy = yx$. Concluimos que todo anillo Booleano es conmutativo, y además todo elemento de un anillo booleano es su propio inverso aditivo.

Sea $X \neq \emptyset$ un conjunto y $\mathscr{P}(X)$ el conjunto de todos los subconjuntos de X. Daremos a $\mathscr{P}(X)$ una estructura de anillo, definiendo la suma como $A + B = (A \setminus B) \cup (B \setminus A)$ y el producto como $AB = A \cap B$. El conjunto vacío es el neutro aditivo y X es el neutro multiplicativo. Además $A^2 = AA = A \cap A = A$, por lo tanto $\mathscr{P}(X)$ es un anillo Booleano.

Si R es un anillo, $\emptyset \neq A \subseteq R$ y si A es un anillo con las mismas operaciones de R, entonces A se llama un *subanillo* de R. Por ejemplo, $\mathbb{H}$ es un subanillo de $M_2(\mathbb{C})$.

Ejemplo 3.7. En el caso de anillos unitarios no es necesario que un subanillo tenga el mismo neutro multiplicativo que el anillo completo. Por ejemplo, si consideramos el anillo $\mathbb{Z}_6$ y nos fijamos en el subconjunto $\{0, 2, 4\}$, notamos que es cerrado respecto a la suma y la multiplicación, y que $4 \neq 1$ actúa como neutro multiplicativo.

Un subconjunto I de un anillo R se dice *ideal* o *ideal bilátero* si verifica:

1. I es subanillo de R.
2. Para cualquier $r \in R$ se cumple que $rI \subseteq I$.
3. Para cualquier $r \in R$ se cumple que $Ir \subseteq I$.

Si I cumple 1 y 2 se dice *ideal izquierdo* y si cumple 1 y 3 se dice *ideal derecho*. Notemos que la condición 1 se puede enunciar de la forma

1'. I es un anillo no necesariamente unitario.
y que en un anillo conmutativo las nociones de ideal izquierdo, derecho y bilátero coinciden.

Ejemplo 3.8. Si $m \in \mathbb{Z}$, entonces $m\mathbb{Z} = \{mk;\ k \in \mathbb{Z}\}$ es un ideal de $\mathbb{Z}$. Más aún, si I es ideal de $\mathbb{Z}$, entonces existe $m \in I$ tal que $I = m\mathbb{Z}$ pues $I \leq \mathbb{Z}$.

Si X es un subconjunto de un anillo R, entonces la intersección de todos los ideales que contienen a X es un ideal de R y se llama el *ideal generado por* X, y se anota $\langle X \rangle$. En el caso particular que $X = \{x\}$ anotamos $\langle x \rangle = (x)$ y llamamos a (x) el *ideal principal generado por* x. Si R es conmutativo, entonces es directo verificar que $(x) = Rx$. Si D es un dominio tal que todo ideal de I es principal, entonces D se llama *dominio de ideales principales* o DIP para abreviar. Por ejemplo, $\mathbb{Z}$ es un DIP.

Si I es ideal de R y $u \in I$, donde u es una unidad, entonces $1 = u^{-1}u \in I$, y como $1R \subseteq I$ obtenemos que $I = R$. Por lo tanto si R es un cuerpo, sus únicos ideales son $\{0\}$ y R. Recíprocamente, si los únicos ideales de un anillo conmutativo son $\{0\}$ y R consideremos $x \in R^*$. Luego $Rx = (x)$ es un ideal distinto de $\{0\}$ y necesariamente $Rx = R$. Por lo tanto, existe $r \in R$ tal que $rx = 1$, y entonces R es cuerpo. Es decir, tenemos el siguiente resultado:

Proposición 3.1. *Un anillo conmutativo es un cuerpo ssi sus únicos ideales son* $\{0\}$ *y* R.

Sean R y R' son anillos con unidad y 1 y $1'$ los neutros multiplicativos de R y R' respectivamente. Por abuso de notación denotamos las operaciones en los dos anillos de la misma forma. Una función $\eta : R \to R'$ se de *morfismo de anillos unitarios* si:

1. η es morfismo entre las estructuras $(R, +, \cdot)$ y $(R', +, \cdot)$, es decir que para cada $x, y \in R$ se verifica que

$$\eta(x + y) = \eta(x) + \eta(y) \text{ y } \eta(xy) = \eta(x)\eta(y).$$

2. $\eta(1) = 1'$.

Si η sólo verifica 1. (o si R o R' son anillos no unitarios) se habla a veces de *morfismos de anillos*. De ahora en adelante hablaremos de morfismos de anillos para referirnos a morfismos de anillos unitarios, y todos los teoremas de isomorfismo (salvo el teorema del resto chino) que veremos son válidos en el contexto de anillos no unitarios con modificaciones directas a las demostraciones respectivas.

Notamos que un morfismo de anillos es un morfismo de grupos abelianos entre $(R, +)$ y $(R', +)$. Por lo tanto $\ker(\eta) = \{x \in R/\ \eta(x) = 0'\}$ es un subgrupo (normal) de $(R, +)$. Pero además, si $r \in R$ y $k \in \ker(\eta)$ se tiene que $\eta(rk) = \eta(r)\eta(k) = \eta(r)0' = 0'$ y del mismo modo $\eta(kr) = \eta(k)\eta(r) = 0'\eta(r) = 0'$. Es decir, $Ker(\eta)$ es un ideal de R. Además, como ya lo vimos para grupos, $\ker(\eta) = \{0\}$ ssi η es inyectiva. Por su parte $\text{im}(\eta)$ es un subanillo de R', pero no necesariamente un ideal de R'.

Ejemplo 3.9. Sea $(G, +)$ un grupo abeliano y sea $\text{End}(G) = \{f : G \to G;\ f \text{ morfismo}\}$. Entonces si definimos $f + g : G \to G$ por $(f + g)(x) = f(x) + g(x)$ y el producto como la composición de funciones, entonces tenemos que $\text{End}(G)$ es un anillo. Reciprocamente si R es un anillo, entonces para cada $r \in R$ definamos la función $\phi_r : (R, +) \to (R, +)$ por $\phi_r(a) = ra$. Notamos que ϕ_r es un morfismos de grupos abelianos. Entonces la función $\eta : R \to \text{End}(R, +)$ definida por $\eta(r) = \phi_r$ es morfismo de anillos. Como $\phi_r(1) = r$, se tiene que η es inyectivo.

Observación 3.2. Si $\phi : K \to R$ un morfismo de anillos con K un cuerpo, entonces como los ideales de K son $\{0\}$ y K se tiene que $\ker(\phi) = \{0\}$ pues $1 \notin \ker(\phi)$. Es decir, todo morfismo que nace de un cuerpo es monomorfismo.

Ejemplo 3.10. Consideremos τ un automorfismo de $\mathbb{Q}[\sqrt{2}]$. Como $\tau(1) = 1$ se tiene que $\tau(n) = n \ \forall n \in \mathbb{Z}$ y si $0 \neq n \in \mathbb{N}$, entonces

$$1 = \tau(1) = \tau\left(n \times \frac{1}{n}\right) = \tau(n)\tau\left(\frac{1}{n}\right) = n\tau\left(\frac{1}{n}\right),$$

es decir

$$\tau\left(\frac{1}{n}\right) = \frac{1}{n}.$$

Además si $m \in \mathbb{Z}$ y $0 \neq n \in \mathbb{N}$, entonces

$$\tau\left(\frac{m}{n}\right) = \tau\left(m \times \frac{1}{n}\right) = \tau(m)\tau\left(\frac{1}{n}\right) = \frac{m}{n}$$

Luego τ fija a $\mathbb{Q}$ punto a punto. Por lo tanto, si $x = a + b\sqrt{2}$ con a y b números racionales, se tiene que $\tau(a + b\sqrt{2}) = a + b\tau(\sqrt{2})$. Entonces para conocer τ basta conocer $\tau(\sqrt{2})$, pero

$$2 = \tau(2) = \tau(\sqrt{2}\sqrt{2}) = \tau(\sqrt{2})\tau(\sqrt{2}) = (\tau(\sqrt{2}))^2,$$

de modo que $\tau(\sqrt{2}) = \sqrt{2}$ o bien $\tau(\sqrt{2}) = -\sqrt{2}$. En ambos casos se obtienen automorfismos. En el primer caso es la identidad y en el otro caso es la "conjugación" $\tau(a + b\sqrt{2}) = a - b\sqrt{2}$.

Ejemplo 3.11. Sea $\phi : \mathbb{R} \to \mathbb{R}$ un automorfismo de anillos. Al igual que en el ejemplo anterior deducimos que $\phi(r) = r$, para cada $r \in \mathbb{Q}$. Además si $x \neq 0$ entonces $\phi(x) \neq 0$ y por tanto $0 < \phi(x)^2 = \phi(x^2)$. Como el conjunto de los números positivos es el mismo que el conjunto de los cuadrados de elementos no nulos en $\mathbb{R}$, se tiene que ϕ transforma números positivos en números positivos. Luego ϕ preserva el orden: si $x < y$ tenemos que $0 < \phi(y - x) = \phi(y) - \phi(x)$ y por lo tanto se tiene que $\phi(x) < \phi(y)$. Si ϕ no es la identidad, entonces existe $x \in \mathbb{R}$ tal que $\phi(x) = y \neq x$. Sin restricción supongamos que $x < \phi(x)$. Por densidad de $\mathbb{Q}$ en $\mathbb{R}$, existe $r \in \mathbb{Q}$ tal que $x < r < \phi(x)$, y como ϕ preserva el orden se tiene que $\phi(x) < \phi(r) < \phi(y)$, pero ϕ deja a cada elemento de $\mathbb{Q}$ fijo, es decir $\phi(x) < r < \phi(y)$. Entonces tenemos que $r < \phi(x)$ y que $\phi(x) < r$, lo que es una contradicción. Concluimos que ϕ es la identidad, es decir, el único automorfismo de anillos de $\mathbb{R}$ es la identidad.

Si R es un anillo y $R \neq I$ es un ideal de R, entonces $(I, +)$ es subgrupo normal de $(R, +)$. Entonces podemos formar el grupo cociente R/I, definiendo la suma por $(a + I) + (b + I) = (a + b) + I$ y más aún, podemos definir un producto en R/I por $(a + I)(b + I) = ab + I$. Tenemos que demostar que esta multiplicación está bien definida, y para ello supongamos que $a + I = a' + I$ y que $b + I = b' + I$, por lo tanto existen $i, j \in I$ tales que $a' = a + i$ y $b' = b + j$ y entonces

$$(a' + I)(b' + I) = a'b' + I = (a + i)(b + j) + I = ab + (aj + ib + ij) + I.$$

Pero tanto aj como ib y ij son elementos de I de modo que $(aj+ib+ij)+I=I$ y

$$(a'+I)(b'+I)=ab+I=(a+I)(b+I).$$

La asociatividad y la distributividad de esta multiplicación en R/I se heredan de las propiedades de la multiplicación de R. y el neutro multiplicativo es la clase del 1, es decir, $1+I$. Este anillo se llama el *anillo cociente* de R sobre I. Por ejemplo, el anillo cociente $\mathbb{Z}/n\mathbb{Z}$ es el anillo $\mathbb{Z}_n$.

Si $I\neq R$ es un ideal de R, entonces la función $\pi: R\to R/I$ definida por $\pi(x)=x+I$ es un morfismo de anillos epiyectivo llamada la *proyeccón canónica.* Es fácil verificar que la estructura de anillo cociente es la única que hace que π sea morfismo, y que la condición de que I sea ideal es equivalente a que la suma y el producto en el cociente estén bien definidas. Además $x\in\ker(\pi)$ ssi $x+I=I$, es decir $\ker(\pi)=I$. Luego obtenemos la siguiente proposición, análoga al resultado para grupos normales.

Proposición 3.2. *Todo ideal propio de R es el kernel de un morfismo de anillos.*

Los siguientes resultados son una extensión de los teoremas de isomorfismo de grupos a anillos.

Teorema 3.1 (Primer teorema de isomorfismo)**.** *Si $\eta: R\to R'$ es un morfismo de anillos, entonces*

$$R/\ker(\eta)\cong \mathrm{im}(\eta)$$

Demostración. El primer teorema de isomorfismo para grupos muestra que $\bar{\eta}: /\ker(\eta)\to \mathrm{im}(\eta)$ definida por $\bar{\eta}(x+\ker(\eta))=\eta(x)$ está bien definida y es isomorfismo de grupos. También es morfismo de anillos por la definición del producto en R/I y porque η lo es. □

Ejemplo 3.12. Si R es anillo, definiendo $\phi:\mathbb{Z}\to R$ por $\phi(k)=\phi\cdot 1$ se verifica directamente que ϕ es morfismo de anillos. Si $\ker(\phi)=n\mathbb{Z}$ (con $n\in\mathbb{N}$) diremos que R tiene *característica* n, y la escribimos como $\mathrm{char}(R)$. Cuando ésta es positiva, corresponde al primer natural tal que $\underbrace{k \text{ veces}}\, 1+\cdots+1=0$. El teorema anterior muestra que existe una copia de $\mathbb{Z}/\mathrm{char}(R)$ en R.

Si R es un dominio de característica positiva, entonces ésta es un número primo: si no, podríamos encontrar $n,m\geq 1$ enteros tales que $(n1)(m1)=\mathrm{char}(R)1=0$, y como R es dominio entonces sin pérdida de generalidad tenemos que $n1=0$, pero $n\notin\ker(\phi)$ pues $n<\mathrm{char}(R)$. Luego R contiene a un cuerpo $\mathbb{Z}/p\mathbb{Z}$ con p primo. Una demostración más corta de lo anterior consiste en observar que char$\mathbb{Z}$ debe ser un ideal primo al ser preimagen del ideal primo $\{0\}\subseteq R$, como veremos más adelante.

Ejemplo 3.13. Sea K un cuerpo de característica p primo y sea $n\in\mathbb{N}$. Notemos que la función $x\mapsto x^{p^n}$ separa las multiplicaciones (pues K es conmutativo) y $1^{p^n}=1$. Además, si $a,b\in K$, tenemos que $(a+b)^p=\sum_{i=0}^{p}=\sum_{k=0}^{p}\binom{p}{k}a^{p-k}b^k$ y cuando $0<k<p$ entonces

$$\binom{p}{k}=\frac{p!}{(p-k)!k!}=\frac{p(p-1)(p-2)\ldots(p-(k-1))}{k!}\in\mathbb{N}.$$

Pero la descomposición prima de $k!$ consiste solamente en primos estrictamente menores que p, de modo que $k!$ divide a $(p-1)(p-2)\ldots(p-(k+1))$, es decir $\binom{p}{k}\equiv 0 \mod p$ cuando $0<k<p$. Luego $(a+b)^p=$

$a^p + b^p$, y aplicando esta igualdad n veces vemos que $(a+b)^{p^n} = a^{p^n} + b^{p^n}$. Luego $x \mapsto x^{p^n}$ es morfismo, llamad el *morfismo de Frobenius*. Es inyectivo pues K no tiene divisores de cero, y si K es finito tenemos que es automorfismo.

Teorema 3.2 (Teorema de correspondencia)**.** *Si I es un ideal propio de un anillo R, entonces existe una correspondencia biunívoca entre los ideales que contienen a I y los ideales del cociente R/I.*

Demostración. Sea $\mathscr{J}$ un ideal de R/I. Como $\mathscr{J} \leq R/I$, el teorema de correspondencia de grupos muestra que $\mathscr{J}$ es la imagen bajo π del grupo $J = \{j \in R;\ j + I \in \mathscr{J}\}$. Es claro que $I \subseteq J$. Si $r \in R$ y $j \in J$, entonces $rj + I = (r+I)(j+I)$ y $jr + I = (j+I)(r+I)$ están en $\mathscr{J}$ pues éste es ideal y entonces J lo es también. Recíprocamente, si $J \supseteq J$ es un ideal de R, entonces $\mathscr{J} = \pi(J)$ es un subgrupo de R/I. Por otro lado, si $r \in R$ entonces $(r+I)\mathscr{J} = \pi(rJ) \subseteq \pi(J)$ y concluimos que $\mathscr{J}$ es ideal de R/I. □

La demostración de los próximos tres teoremas consiste en darse cuenta que los morfismos entregados por los teoremas correspondientes en el contexto de grupos son también morfismos de anillos. Notemos que si I, J son ideales de un anillos R, entonces la suma $I + J$ también lo es.

Teorema 3.3 (Teorema del factor)**.** *Si $\eta : R \to R'$ es un morfismo de anillos e I es un ideal de R tal que $I \leq \ker(\eta)$, entonces existe un único morfismo de anillos $\bar{\eta} : R/I \to R'$ que verifica $\bar{\eta} \circ \pi = \eta$.*

Teorema 3.4 (Segundo teorema de isomorfismo)**.** *Si I, J son ideales de un anillo R, entonces $(I+J)/I \cong I \cap J/J$.*

Teorema 3.5 (Tercer teorema de isomorfismo)**.** *Sean $I \subseteq J$ ideales propios de un anillo R. Entonces $(R/I)/(J/I) \cong R/J$.*

Diremos que dos ideales I, J son *coprimos* o *comaximales* si $I + J = R$, lo que es equivalente a la existencia de $x \in I$, $y \in J$ tales que $x + y = 1$. Esta definición generaliza la condición que concluye el lema de Bézout del capítulo 1. Definimos el *producto* de dos ideales I, J como el ideal compuesto por todas las sumas finitas de productos del tipo ab con $a \in I$, $b \in J$.

La inclusión $IJ \subseteq I \cap J$ se cumple siempre, y si R es conmutativo e I, J son coprimos entonces existen $x \in I$, $y \in J$ tales que $x + y = 1$, de manera que $c = cx + cy \in IJ$ para cada $c \in I \cap J$. Luego $IJ = I \cap J$ cuando R es conmutativo. Es directo verificar que en este caso también se cumple que $(a)(b) = (ab)$ cuando $a, b \in R$.

El siguiente resultado permite descomponer un anillo en unidades más simples al conocer ideales coprimos entre sí. Siempre que hablemos de productos cartesianos de anillos en este contexto, los dotaremos de las operaciones por componentes para tratarlos como anillos.

Teorema 3.6 (Teorema Chino del Resto)**.** *Sean $A_1, \ldots, A_k$ ideales de un anillo conmutativo R tales que los A_i son coprimos a pares. Entonces $R/(A_1 \cap \cdots \cap A_k) \cong R/A_1 \times \ldots R/A_k$ como anillos.*

Demostración. Hagamos inducción en $k \geq 2$: si $k = 2$, entonces consideremos el morfismo de anillos $\psi : R \to R/A_1 \times R/A_2$ dados por las proyecciones naturales módulo A_1 en la primera componente y módulo

A_2 en la segunda. El kernel de ψ es claramente $A_1 \cap A_2$, y ψ resulta ser sobreyectiva: en efecto, como A_1 y A_2 son comaximales existen $x \in A_1$ e $yinA_2$ tales que $x + y = 1$, y entonces $\psi(x) = (0,1)$ (ya que $x = 1-y$) y $\psi(y) = (1,0)$ (ya que $y = 1-x$). Luego las imágenes de las combinaciones lineales $r_1x + r_2y$ recorren todo $R/A_1 \times R/A_2$ cuando r_1, r_2 recorren R. Para el caso general basta usar la hipótesis inductiva con A_1 y $A_2 \ldots A_k$ notando que A_1 y $A_2 \cap \cdots \cap A_k$ son coprimos, pues existen elementos $x_i \in A_1$ e $y_i \in A_i$ para $i = 2, \ldots, k$ tales que $x_i + y_i = 1$, de manera que $1 = (x_2 + y_2) \ldots (x_k + y_k) \in A_1 + (A_2 \cap \cdots \cap A_k)$. □

Ejemplo 3.14. Si $n \in \mathbb{N}$ y su factorización prima es $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, entonces el teorema anterior muestra que

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$$

como anillos ya que $ab\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ si $a, b \in \mathbb{Z}$ son coprimos. En particular, los grupos de unidades de ambos anillos son isomorfos y tienen el mismo cardinal, de donde sigue que $\varphi(n) = \varphi(p_1^{\alpha_1}) \ldots \varphi(p_k^{\alpha_k})$ donde φ es la función indicatriz de Euler.

Por otro lado, el teorema anterior también implica que si $m_1, \ldots, m_k$ son enteros coprimos entre sí y $a_1, \ldots, a_k$ son enteros cualquiera, entonces existe una única solución módulo $m_1 \ldots m_k$ al sistema de congruencias

$$x \equiv a_1 \mod m_1, \ \ldots, \ x \equiv a_k \mod m_k.$$

El ejercicio 3.5 está dedicado a computar eficientemente esta solución.

Si R es un anillo e I es un ideal de R, diremos que I es un *ideal maximal* si $I \neq R$ y si J es ideal de R con $I \subseteq J$, entonces $J = I$ o $J = R$. Un ideal P de un anillo conmutativo se dice *primo* si $P \neq R$ y cada vez que $ab \in P$, implica que $a \in P$ o $b \in P$. Notemos que la preimagen vía morfismos de un ideal primo es un ideal primo, pero que no necesariamente ocurre lo mismo con ideales maximales.

Ejemplo 3.15. Los ideales primos no nulos y los ideales maximales en $\mathbb{Z}$ corresponden a $p\mathbb{Z}$ con p primo.

Proposición 3.3. *Si R es un anillo conmutativo e I es un ideal de R, entonces*

1. *R/I es un cuerpo ssi I es maximal.*
2. *R/I es dominio ssi I es primo.*

Demostración. Demostremos 1: supongamos que I es maximal y consideremos el cociente R/I. Si $x \notin I$, entonces $I + (x)$ es un ideal que contiene propiamente a I y por lo tanto $(x) + I = R$. Luego existen $y \in R$ y $m \in I$, tales que $xy + m = 1$, por lo tanto $(x + I)(y + I) = xy + I = 1 - m + I = 1 + I$, es decir, todo elemento no nulo de R/I es invertible. Por lo tanto R/I es un cuerpo. Recíprocamente, si R es un anillo conmutativo y M es un ideal propio tal que R/M es cuerpo, entonces como los únicos ideales de un cuerpo son solamente todo el cuerpo y $\{0\}$, entonces por teorema de correspondencia, los únicos ideales de R que contienen a M son M y R, por lo tanto M es maximal.

Para demostrar 2 basta notar que si $x, y \in R$, entonces $(x + I)(y + I) = I$ ssi $xy \in I$. □

Notemos que si R es un anillo conmutativo y M es un ideal maximal de R entonces R/M es cuerpo y en particular R/M es dominio de integridad. El teorema anterior prueba que M es ideal primo. Por lo tanto tenemos el siguiente corolario:

Corolario 3.1. *En un anillo conmutativo todo ideal maximal es un ideal primo.*

Concluimos esta sección con una de las pocas aplicaciones del axioma de elección en este texto. Notemos que la demostración usa que R sea unitario.

Teorema 3.7. *Si R es un anillo, todo ideal propio de R está contenido en un ideal maximal de R.*

Demostración. Sea R un anillo y sea $I \neq R$ un ideal. Consideremos $\mathscr{S}$ el conjunto de todos los ideales de R distintos de R y que contienen a I. Como $I \in \mathscr{S}$, tenemos que $\mathscr{S} \neq \emptyset$. El conjunto $\mathscr{S}$ es parcialmente ordenado por inclusión. Consideremos una cadena ascendente $\mathscr{J}$ en $\mathscr{S}$. Consideremos la unión de todos los elementos de la cadena, esto es $\overline{I} = \bigcup_{J \in \mathscr{J}} J$.

Comprobemos que $\overline{I}$ es un ideal: en efecto, como I es uno de los ideales de la unión, se tiene que $0 \in I \subseteq \overline{I}$. Además si $a, b \in \overline{I}$, entonces existen k_1 y k_2 tal que $a \in J_{k_1}$ y $b \in J_{k_2}$, como $\mathscr{J}$ es una cadena, sin restricción podemos suponer que $J_{k_1} \subseteq J_{k_2}$ y por lo tanto $a, b \in J_{k_2}$. Como J_{k_2} es ideal, entonces $a + b \in J_{k_2} \subseteq \overline{I}$. Si $a \in \overline{I}$ entonces existe k tal que $a \in J_k$, entonces como J_k es ideal se tiene que $-a, ra$ y $ar \in J_k$ para cada $r \in R$.

Ya vimos que $I \subseteq \overline{I}$, pero además si $1 \in \overline{I}$, existiría k tal que $1 \in J_k$, en ese caso ocurriría que $J_k = R$, pero tal cosa no ocurre pues todos los elementos de $\mathscr{J}$ son distintos de R. Es decir, $I \subseteq \overline{I} \subseteq R$, y $\overline{I} \neq R$. Luego $\overline{I}$ es una cota superior de la cadena $\mathscr{J}$ en $\mathscr{S}$ y el lema de Zorn muestra que existe un elemento maximal en $\mathscr{S}$, y tal elemento maximal es un ideal maximal de R que contiene a I. □

3.2. Cuerpos de cocientes

Hasta el momento tenemos una forma de construir cuerpos mediante el cociente de un anillo conmutativo por un ideal maximal. Ahora generalizaremos la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$ en el capítulo 1 a cualquier dominio.

Consideremos un dominio D y recordemos que D^* es el conjunto de elementos no nulos de D. Definamos la relación $\sim$ sobre $D \times D^*$ por $(a, b) \sim (c, d)$ ssi $ad = cd$. Exactamente la misma demostración que cuando D es $\mathbb{Z}$ (y que usa que D es dominio) muestra que $\sim$ es de equivalencia. Denotemos por $Q(D)$ al conjunto cociente $D \times D^* / \sim$ y a/b a la clase $[(a, b)]$. Definamos una suma y producto en $Q(D)$ por

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

cuando a/b, $c/d \in Q(D)$. La misma demostración entregada en el capítulo 1 muestra que estas operaciones están bien definidas. Nuevamente, la clase $[(1, 1)] = \{(a, a);\ a \in D^*\}$ es el neutro multiplicativo y la clase $[(0, 1)] = \{(0, a);\ a \in D^*\}$ es el neutro aditivo.

Como $\frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}\times\frac{a}{b}$, se tiene que $Q(D)$ es un anillo conmutativo y más aún, todo elemento no nulo de $Q(D)$ tiene inverso multiplicativo: en efecto, si (a,b) está en $D\times D^*$, y no está en la clase nula, es decir, $a\neq 0$, entonces $(b,a)\in D\times D^*$ y además

$$\frac{a}{b}\times\frac{b}{a}=\frac{ab}{ab}=\frac{1}{1}.$$

Así que $Q(D)$ es un cuerpo, usualmente llamado el *cuerpo de cocientes de* D. Consideremos la inyección canónica $\iota\colon D\to Q(D)$ dada por $\iota(d)=d/1$ y notemos que es efectivamente inyectiva por la definición de $Q(D)$. Además, como

$$\frac{d}{1}+\frac{d'}{1}=\frac{d+d'}{1}\text{ y }\frac{d}{1}\times\frac{d'}{1}=\frac{dd'}{1}$$

tenemos que ι es monomorfismo de anillos, e $\mathrm{im}(\iota)$ es un subanillo de $Q(D)$ isomorfo a D. El próximo teorema muestra que $Q(D)$ es el cuerpo más pequeño que contiene a D. En particular, si D es cuerpo entonces $Q(D)\cong D$.

Teorema 3.8. *Si D es un dominio, K es un cuerpo y $\tau\colon D\to K$ es un monomorfismo, entonces existe un único monomorfismo de cuerpos $\overline{\tau}\colon Q(D)\to K$ tal que $\overline{\tau}\circ\iota=\tau$.*

Demostración. Definamos $\overline{\tau}\left(\frac{a}{b}\right)$ como $\tau(a)\tau(b)^{-1}$. Si $a=0$, entonces $\overline{\tau}\left(\frac{0}{b}\right)=\tau(0)\tau(b)^{-1}=0$. Además, si $\frac{a}{b}=\frac{c}{d}$, es decir, $ad=bc$ con $a\neq 0\neq c$, tenemos que como τ es monomorfismo $\tau(c)\tau(d)^{-1}\neq 0$, entonces

$$\left(\overline{\tau}\left(\frac{c}{d}\right)\right)^{-1}\overline{\tau}\left(\frac{a}{b}\right)=\tau(c)^{-1}\tau(d)\tau(a)\tau(b)^{-1}=\tau(ad)(\tau(bc))^{-1}.$$

Pero como $ad=bc$, se tiene que $\overline{\tau}\left(\frac{c}{d}\right)^{-1}\overline{\tau}\left(\frac{a}{b}\right)=1$, es decir $\overline{\tau}\left(\frac{c}{d}\right)=\overline{\tau}\left(\frac{a}{b}\right)$. Luego $\overline{\tau}$ está bien definida.

Además, $\overline{\tau}$ es morfismo, pues si $a/b,\ c/d\in Q(D)$ entonces

$$\begin{aligned}\overline{\tau}\left(\frac{a}{b}+\frac{c}{d}\right)=\overline{\tau}\left(\frac{ad+bc}{bd}\right)&=\tau(ad+bc)(\tau(bd))^{-1}\\&=(\tau(a)\tau(d)+\tau(b)\tau(c))(\tau(b))^{-1}(\tau(d))^{-1}\\&=\tau(a)\tau(d)(\tau(b))^{-1}(\tau(d))^{-1}+\tau(b)\tau(c)(\tau(b))^{-1}(\tau(d))^{-1}\\&=\tau(a)(\tau(b))^{-1}+\tau(c)(\tau(d))^{-1}=\overline{\tau}\left(\frac{a}{b}\right)+\overline{\tau}\left(+\frac{c}{d}\right)\end{aligned}$$

y además

$$\begin{aligned}\overline{\tau}\left(\frac{a}{b}\times\frac{c}{d}\right)=\overline{\tau}\left(\frac{ac}{bd}\right)&=\tau(ac)(\tau(bd))^{-1}\\&=(\tau(a)\tau(c))(\tau(b))^{-1}(\tau(d))^{-1}\\&=(\tau(a)\tau(b))^{-1})(\tau(c)(\tau(d))^{-1}\\&=\overline{\tau}\left(\frac{a}{b}\right)\times\overline{\tau}\left(\frac{c}{d}\right).\end{aligned}$$

Por otra parte $\overline{\tau}\left(\frac{1}{1}\right)=\tau(1)(\tau(1))^{-1}=1\times 1=1$. Es decir, $\overline{\tau}$ es un morfismo de anillos. Además, $\overline{\tau}$ es inyectiva pues $\tau(a)\tau(b)^{-1}=0$ implica que $a=0$ ya que D es dominio, y entonces $a/b=0/1$. Concluimos notando que para cada $d\in D$ se verifica por definición que $\overline{\tau}(d/1)=\tau(d)$. □

Ejemplo 3.16.

- El cuerpo de cocientes de $\mathbb{Z}$ es $Q(\mathbb{Z})=\mathbb{Q}$, luego cuando R es un dominio de característica 0 obtenemos que existe una copia isomorfa de $\mathbb{Q}$ en R.
- Consideremos el subanillo $\mathbb{Q}[i]=\{a+bi/\ a,b\in\mathbb{Q}\}$ del cuerpo de los complejos $\mathbb{C}$. El conjugado de un elemento $z=a+bi$ de $\mathbb{Q}[i]$ es $\overline{z}=a-bi\in\mathbb{Q}[i]$ y su norma es el número $z\overline{z}=a^2+b^2\in\mathbb{Q}$. Ahora $z\overline{z}=0$ ssi $a=0=b$, por lo tanto cuando $0\neq z\in\mathbb{Q}[i]$ el número complejo

$$\frac{1}{z\overline{z}}\overline{z}=\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}\in\mathbb{Q}[i].$$

  Además $z\times\frac{1}{z\overline{z}}\overline{z}=1$. Luego $\mathbb{Q}[i]$ es un cuerpo que contiene a $\mathbb{Z}[i]$, el anillo de los enteros Gaussianos. Como $\mathbb{Z}[i]$ es un dominio, entonces podemos construir el cuerpo de cocientes $Q(\mathbb{Z}[i])$. ¿Es cierto que $Q(\mathbb{Z}[i])\cong\mathbb{Q}[i]$?.

3.3. Divisibilidad en Anillos

Recordemos que en $\mathbb{R}[X]$ definimos polinomios irreducibles como aquellos polinomios de grado mayor o igual a 1 que no se pueden escribir como productos polinomios de grado mayor o igual a 1. Es decir $p(X)\in\mathbb{R}[X]$ es irreducible si no es un elemento de $\mathbb{R}$ y si $p(X)=r(X)q(X)$ implica que $r(X)$ o $q(X)$ son no nulos de grado cero. Dicho de otra forma, $p(X)\in\mathbb{R}[X]$ es irreducible, si no es nulo, si no es una unidad en $\mathbb{R}[X]$ y si $p(X)=r(X)q(X)$, entonces $r(X)$ o $q(X)$ son unidades en $\mathbb{R}[X]$. En esta sección generalizaremos las nociones de elemento primo y elemento irreducible en un anillo conmutativo.

En lo que sigue R será un anillo conmutativo a menos que se diga lo contrario. Diremos que un elemento no nulo $a\in R$ *divide* a $b\in R$ ssi existe $x\in R$ tal que $ax=b$ y y y y en este caso anotamos $a|b$. Los elementos $a,b\in R$ se dicen asociados si $a|b$ y $b|a$. Notemos que a y b son asociados ssi $(a)=(b)$, y por ende la relación $a\sim b$ ssi a es asociado a b es una relación de equivalencia.

Observación 3.3.

- Si u es una unidad en R y $b \in R$, entonces $u(u^{-1}b) = b$ Es decir, las unidades dividen a todos los elementos del anillo. Recíprocamente si $u \neq 0$ y u divide a todos los elementos del anillo R, entonces en particular divide a 1, es decir, existe $x \in R$ tal que $ux = 1$, es decir u es una unidad. En resumen, $u \neq 0$ es una unidad en R ssi $u|b$ para todo $b \in R$.
- Si a y b son asociados en un dominio D, entonces existen $x, y \in D$ tales que $ax = b$ y $by = a$. Luego $a(xy) = (ax)y = a$ y por lo tanto $xy = 1$, es decir $ax = b$ donde x es una unidad. Reciprocamente, si $a = xb$ con x una unidad, entonces $x^{-1}a = b$, entonces $a|b$ y $b|a$.

Un elemento c no nulo y no unidad de R se dice *irreducible,* si $c = ab$ implica que a es unidad o b es unidad. Si c es irreducible y $d = cu$ con u una unidad, entonces si $d = xy$, entonces $cu = xy$, en este caso $c = (u^{-1}x)y$. Como c es irreducible, se tiene que $u^{-1}x$ es unidad o y es unidad, por lo tanto x es unidad o y es unidad, es decir d es irreducible.

Ejemplo 3.17. El polinomio $X^2 + 1$ es irreducible en $\mathbb{R}[X]$, pero no es irreducible en $\mathbb{C}[X]$, ni tampoco en $\mathbb{Z}_2[X]$ pues en $\mathbb{Z}_2[x]$ se tiene que $X^2 + 1 = (X + 1)(X + 1)$.

Ejemplo 3.18. Si p es primo en $\mathbb{Z}$ entonces p es irreducible en $\mathbb{Z}$, pues si $p = ab$ entonces $p|ab$, por lo tanto $p|a$ o $p|b$, sin restricción, supongamos que $p|a$, entonces existe $x \in \mathbb{Z}$ tal que $px = a$, entonces la igualdad $p = ab$ se puede escribir como $p = pxb$, entonces $xb = 1$, es decir b es unidad.

Ejemplo 3.19. Si $z = a+bi \in \mathbb{Z}[i]$ definimos $N(z) = a^2+b^2 \in \mathbb{N}$. Además se puede comprobar (**[Ejercicio]**) que $N(zw) = N(z)N(w)$ para cada par de elementos $z, w \in \mathbb{Z}[i]$. Si $z \neq 0$ es una unidad en $\mathbb{Z}[i]$, significa que existe $w \in \mathbb{Z}[i]$ tal que $zw = 1$, aplicando N se obtiene:

$$N(z)N(w) = 1$$

Es decir, $N(z)$ es unidad en $\mathbb{Z}$ y $N(z) \in \mathbb{N}$, entonces $N(z) = 1$. Es decir, si $z = a + bi$ es unidad, entonces $a^2 + b^2 = 1$. Entonces los únicos candidatos a unidades en $\mathbb{Z}[x]$ son 1, -1, i y $-i$ y cada uno de ellos es efectivamente unidad en $\mathbb{Z}[i]$, de hecho $1 = 1 \times 1 = (-1)(-1) = i(-i)$.

Ahora, si α es un número compuesto en $\mathbb{Z}$, entonces $\alpha = \beta\gamma$ con β, γ números enteros distintos de 1 y -1. Entonces β y γ no son unidades en $\mathbb{Z}[i]$ entonces α no es irreducible en $\mathbb{Z}[i]$. Sin embargo, hay primos en $\mathbb{Z}$ que no son irreducibles en $\mathbb{Z}[i]$, por ejemplo $2 = (1 + i)(1 - i)$ y tanto $1 + i$ como $1 - i$ no son unidades de $\mathbb{Z}[i]$. Sea p un primo impar, de la forma $4n+3$ para cierto $n \in \mathbb{N}$, y supongamos $p = zw$, con $z, w \in \mathbb{Z}[i]$, entonces $p^2 = N(z)N(w)$, entonces puede pasar que $N(z) = N(w) = p$ o $N(z) = p^2$ y $N(w) = 1$. Si $N(z) = p$, entonces si $z = a + bi$, se tiene que $a^2 + b^2 = p$, entonces sin restricción podemos suponer a impar y b par, en ese caso:

$$(2t + 1)^2 + (2k)^2 = p$$

$$4t^2 + 4t + 1 + 4k^3 = 4n + 3$$

$$4t^2 + 4t + 4k^2 = 4n + 2$$

Pero 4 divide al lado izquierdo de la igualdad, pero no al lado derecho de la igualdad, por lo tanto suponer $N(z) = p$ nos lleva a una contradicción, entonces $N(z) = p^2$ y $N(w) = 1$. Es decir, w es unidad en $\mathbb{Z}[i]$. Es decir, si p es un primo impar de la forma $4n+3$ es irreducible en $\mathbb{Z}[i]$.
En cambio si p es un primo impar de la forma $4n+1$ para cierto entero n, entonces p no es irreducible en $\mathbb{Z}[i]$. **[Ejercicio]**

Si p es un elemento no nulo y no unidad de R, diremos que p es *primo* si cada vez que p divide a un producto entonces divide a uno de los factores. Dicho de otro modo, cuando $p|ab$ entonces $p|a$ o $p|b$.

Notemos que si p es primo en D, un dominio y tenemos que $p = ab$, entonces $p|ab$ y por lo tanto $p|a$ o $p|b$. Sin restricción supongamos que $p|a$. Como $a|p$, entonces existe u una unidad tal que $a = pu$ de manera que $p = ab = pub$. Como D es dominio, se tiene que $1 = ub$, es decir b es unidad y p es irreducible. Es decir, tenemos el siguiente resultado.

Proposición 3.4. *En un dominio de integridad todo elemento primo es irreducible.*

Proposición 3.5. *Sea D un dominio y $a \in D$.*
1. *a es primo ssi (a) es un ideal primo distinto de $\{0\}$.*
2. *a es irreducible ssi (a) es maximal entre ideales principales y es distinto de $\{0\}$.*

En particular, si D es DIP, a es irreducible ssi (a) es maximal.

Demostración. Para probar 1. basta notar que $bc \in (a)$ ssi $a|bc$, y que a es no nulo y no unidad ssi $(a) \neq \{0\}, D$.

Para probar 2., asumamos que a es irreducible y sea (b) un ideal principal que contiene a (a), de manera que $a = xb$ para cierto $x \in D$. Luego b es una unidad (y entonces $(b) = D$) o x es una unidad (y entonces $(b) = (a)$). Luego (a) es maximal entre ideales principales, y además no es $\{0\}$ pues a es no nulo. Recíprocamente, si $\{0\} \neq (a)$ es maximal entre ideales principales, entonces la igualdad $a = bc$ implica que $(a) \subseteq (b)$, y por lo tanto $(b) = D$ (y entonces b es una unidad) o $(b) = (a)$ (y entonces b es asociado a a ya que D es dominio). Notando que $(a) \neq D, \{0\}$ concluimos que a es irreducible. □

Corolario 3.2. *En un DIP D un elemento c es irreducible ssi es primo.*

Demostración. La primalidad de (c) implica que es irreducible en cualquier dominio por la proposición 3.4. Recíprocamente, consideremos c irreducible en D, de manera que (c) es maximal y por lo tanto un ideal primo (y es no nulo pues $c \neq 0$). Luego c también es primo. □

Ejemplo 3.20. Como $\mathbb{Z}[i]$ es un DIP **[Ejercicio],** y como 17 no es irreducible en $\mathbb{Z}[i]$, de hecho

$$17 = (4 + i)(4 - i)$$

y tanto $4 + i$ como $4 + i$ no son unidades en $\mathbb{Z}[i]$, por lo tanto 17 no es primo en $\mathbb{Z}[i]$.

Observación 3.4. En un teorema anterior demostramos que todo ideal propio en un anillo conmutativo está contenido en un ideal maximal. Consideremos un DIP D y $d \in D$ no nulo y no unidad, entonces existe un ideal maximal (c) (con c irreducible) en D que contiene a (d). Es decir, si $d \neq 0$ no es unidad y D es un DIP, existe un elemento irreducible en D que divide a d. En particular si K es un cuerpo y $p(x) \in K[x]$ es un polinomio de grado mayor o igual a 1, entonces existe un polinomio irreducible en $K[x]$ que divide a $p(x)$.

Ejemplo 3.21. Si K es un cuerpo, un polinomio $p(X) \in K[X]$ es irreducible si no se puede escribir en la forma $p(X) = q(X)r(X)$ con $q(X)$ y $r(X)$ polinomios de grado mayor que cero. Es decir, si $p(X)$ es irreducible y $p(X) = q(X)r(X)$ entonces $q(X)$ o $r(X)$ son elementos de K. Si $p(X)$ es irreducible en $K[X]$ entonces $F = K[X]/p(X)$ es un cuerpo pues $(p(X))$ es maximal. Si $p(X)$ es un polinomio de grado n en $K[X]$, dado $f(X) \in K[X]$ eXisten $q(X)$ y $r(X)$ polnomios en $K[X]$ tales que $f(X) = p(X)q(X) + r(X)$ donde $\deg(r(X)) < \deg(p(X))$. Pero $p(X)q(X) \in (p(X))$ por lo tanto $f(X) + (p(X)) = r(X) + (p(X))$. Es decir, toda clase en $K[X]/(p(X))$ tiene un representante de grado menor que $\deg(p(X)) = n$. Concluimos que

$$F = \{a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} + (p(X));\ a_i \in K\}.$$

Los elementos de la forma $a_0 + (p(X))$ forman un subcuerpo de F que es isomorfo a K. Abusando del lenguaje a ese subcuerpo lo llamaremos K. Por lo tanto $p(X) \in K[X]$ puede ser considerado de manera natural en $F[X]$. Definamos $\alpha = X + (p(X)) \in F$ y notemos que $p(\alpha) = p(X) + (p(X)) = (p(X))$. Es decir, α es raíz de $p(X)$ en F. En conclusión, si $p(X)$ es un polinomio irreducible en $K[X]$ con K cuerpo, entonces existe un cuerpo F tal que F contiene una copia isomorfa de K y $p(X)$ tiene al menos una raíz en F. La observación anterior muestra que podemos encontrar tal cuerpo incluso si $p(X)$ no es irreducible, pues podemos considerar algún factor irreducible de $p(X)$.

Diremos que un dominio D verifica la *condición de ideales principales ascendentes* si para cada cadena ascendente de ideales principales

$$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subset \cdots \subseteq D$$

es estacionaria, es decir existe un $m \in \mathbb{N}$ tal que $(a_n) = (a_m)$ para todo $n \geq m$.

Lema 3.1. *Si D es DIP, entonces D verifica la condición de ideales principales ascendentes.*

Demostración. Consideremos una cadena de ideales $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \ldots$ en D. Definamos $I = \bigcup_{i\geq 1}(a_i)$ y notemos que I es ideal: en efecto, como $0 \in (a_1) \subseteq I$ se tiene que $0 \in (a_1) \subseteq I$ y si además $a, b \in I$ y $d \in D$, entonces existen k_1 y k_2 tal que $a \in (a_{k_1})$ y $b \in (a_{k_2})$. Sin pérdida de generalidad podemos suponer que $(a_{k_1}) \subseteq (a_{k_2})$, de manera que $a - b, ra \in (A_{k_2})$. Como D es DIP, entonces $I = (c)$ para cierto $c \in I$ y existe $n \in \mathbb{N}$ tal que $c \in (a_n)$. Luego $I = (a_n)$ y por ende $(a_k) = (a_n)\ \forall k \geq n$. □

Un dominio D se llama un *dominio de factorización única*, escrito DFU, si cada elemento a no nulo y no unidad de D se puede escribir como $a = c_1c_2c_3\cdots c_n$, con c_i irreducible y si además $a = c_1c_2c_3\cdots c_n =$

$d_1 d_2 d_3 \cdots d_m$ con c_i y d_j irreducibles, implica que $n = m$ y que existe $\sigma \in \Sigma_n$ tal que c_i es asociado a $d_{\sigma(i)}$. Esta definición generaliza las propiedades de $\mathbb{Z}$ que resultan del teorema fundamental de la aritmética. El próximo lema servirá para probar que muchos ejemplos conocidos (y en particular, $K[x]$ cuando K es cuerpo) son DFU.

Lema 3.2. *En un DFU todo elemento irreducible es primo.*

Demostración. Sea D un DFU y $r \in D$ un irreducible. Supongamos que r divide a un producto ab, luego r debe ser asociado a uno de los irreducibles de la descomposición en irreducibles de a o de b pues D es DFU. Concluimos que r divide a a o a b. □

Teorema 3.9. *Todo DIP es un DFU.*

Demostración. Sea D un DIP y sea $\mathscr{S}$ el conjunto de elementos no nulos y no unidades de D que no se pueden escribir en la forma $c_1 c_2 c_3 \cdots c_n$ con c_i irreducibles. En particular los elementos de $\mathscr{S}$ no son irreducibles. Probaremos que suponer $\mathscr{S}$ no vacío nos lleva a una contradicción.

Tomemos $a \in \mathscr{S}$. Como a no es unidad, entonces existe un elemento c_a irreducible en D que divide a a (por la observación 3.4), de manera que $a = c_a x_a$ con $x_a \in D^*$.

Notemos que x_a está unicamente determinado por c_a, y que x_a no es irreducible pues si lo fuese, entonces a no estaría en $\mathscr{S}$. Si x_a fuese unidad, entonces a sería asociado a un irreducible y por lo tanto a sería irreducible, pero no lo es. Por lo tanto x_a no es irreducible y no es unidad. Si x_a fuese un producto de irreducibles, entonces a sería un producto de irreducibles, pero no lo es. Luego x_a está en $\mathscr{S}$ y $(a) \subseteq (x_a)$. Si $(a) = (x_a)$, entonces existiría una unidad u tal que $a = u x_a$, como D es dominio, se tendría que $c_a = u$, pero c_a es irreducible, y por definición c_a no es unidad, entonces $(a) \subset (x_a)$.

Como $x_a \in \mathscr{S}$, se tiene que existe c_{x_a} irreducible y $x_{x_a} \in \mathscr{S}$ tal que $(a) \subset (x_a) \subset (x_{x_a})$, luego podríamos contruir inductivamente una cadena estrictamente ascendente de ideales de D, lo que contradice el teorema anterior. Por lo tanto $\mathscr{S} = \emptyset$, es decir, todo elemento no nulo y no unidad se escribe en la forma $c_1 c_2 c_3 \cdots c_n$ con c_i irreducibles para cada $i \in [n]$.

Probemos la unicidad por inducción en n, el mínimo número de factores irreducibles en alguna factorización de $a \in D$. Si $n = 0$, entonces a es una unidad y la igualdad $r = bc$ para algún irreducible b implica que b también es una unidad, de modo que obtenemos una contradicción. Si $n \geq 1$, entonces las igualdades

$$r = p_1 \dots p_n = q_1 \dots q_m$$

donde los p_i, q_i son irreducibles y $m \geq n$ implican que p_1 divide a algún q_j (ya que es primo por el lema 3.2). Luego p_1 es asociado a algún q_j y cancelando p_1 de ambos lados de la ecuación 3.3, nos reducimos a la hipótesis inductiva. □

Sean a, b en R un anillo conmutativo, diremos que c es un *máximo común divisor* de a y b, y anotamos $\mathrm{mcd}(a, b)$ o simplemente (a, b) si se cumplen las dos siguientes condiciones:

1. $c|a$ y $c|b$.
2. $d|a$ y $d|b$ entonces $d|c$.

Estas condiciones se pueden refrasear como
1.' $(a),(b) \subseteq (c)$.
2.' Si $(a),(b) \subseteq (d)$, entonces $(c) \subseteq (d)$.
Si 1 es un máximo común divisor entre a y b, entonces decimos que a y b son *relativamente primos.*

Observación 3.5. Si c y d son mcd entre a y b en R, entonces $c|d$ y $d|c$. Es decir, c y d son asociados. Si R es un dominio, entonces existe u unidad tal que $c = du$.

Proposición 3.6. *Si $a, b \in D$ un DIP, entonces existe el* mcd *entre a y b. Además cualquier máximo común divisor entre a y b se escribe en la forma $ma + nb$ para ciertos $m, n \in D$.*

Demostración. Consideremos el ideal $(a)+(b)$ en D. Como D es un DIP, existe $c \in D$ tal que $(a)+(b) = (c)$. Dado que $a \in (a) + (b) = (c)$ se tiene que $c|a$ y del mismo modo $c|b$. Además existen $m, n \in D$ tales que $c = ma+nb$ y por lo tanto si d divide a a y a b, entonces divide a $c = ma+nb$. Por lo tanto c es un máximo común divisor entre a y b. Recíprocamente, si d es un máximo común divisor de a y b y $c = ma + nb$ es el mcd del párrafo anterior, entonces existe u unidad en D tal que $d = cu = (um)a + (un)b$. □

Proposición 3.7. *Si $a, b \in D$ un DFU, entonces existe el* mcd *entre a y b.*

Demostración. Si $a = 0$ y $b \neq 0$ entonces b es un mcd entre a y b. Si ambos son nulos, entonces 0 es un mcd entre a y b. Si uno de ellos es unidad, entonces la unidad es un mcd entre ambos.

Si a y b no son unidades ni cero, entonces existen c_i irreducibles tales que $a = c_1^{\alpha_1} c_2^{\alpha_2} c_3^{\alpha_3} \cdots c_n^{\alpha_n}$ y $b = c_1^{\beta_1} c_2^{\beta_2} c_3^{\beta_3} \cdots c_n^{\beta_n}$ con los c_i irreducibles y los α_i, β_i números naturales posiblemente nulos. Afirmamos que $c = c_1^{\gamma_1} c_2^{\gamma_2} c_3^{\gamma_3} \cdots c_n^{\gamma_n}$ con $\gamma_i = \min\{\alpha_i, \beta_i\}$ es un mcd entre a y b. Es claro que c divide a a y b, y si d es divisor común de a y b con factorización en irreducibles $r_1^{\delta_1} \dots r_k^{\delta_k}$, tenemos que cada r_i debe dividir a a y b, y (como cada r_i es primo por el lema 3.2) entonces cada r_i divide a algún p_i. Por lo tanto cada r_i es asociado a algún p_i. Notando que si $p_i^k v$ divide a $p_i^n u$ donde $u, v \in D$ no son múltiplos de r_i implica que $k < n$, concluimos que los exponentes de los p_i en d son menores o iguales a γ_i. Luego d divide a c. □

Notemos que el teorema anterior también muestra que para cualquier subconjunto A de un DFU existe el mcd de A (donde definimos el mcd de un conjunto arbitrario de la manera natural).

Finalizamos esta sección con una definición que generaliza la noción de un algoritmo de división. Un dominio D se dice *dominio euclídeo* si existe una norma N sobre D (en este contexto, una función $N : D \to \mathbb{N}$ que verifica $N(0) = 0$) tal que para cada par $a, b \in D$ con $b \neq 0$ existen $q, r \in D$ tales que $a = qb + r$ y $r = 0$ o $N(r) < N(b)$. En particular, replicando las demostraciones del capítulo 1 obtenemos un algoritmo de Euclides en D para computar el mcd de cualquier par de elementos y expresarlo como combinación lineal de éstos. Veamos que los dominios euclídeos poseen buenas propiedades.

Proposición 3.8. *Todo dominio euclídeo es un DIP.*

Demostración. Sea D un dominio euclídeo e I un ideal de D. Sea $b \in I$ de norma minimal en I y tomemos $a \in I$ arbitrario. Luego existen q, r tales que $a = bq + r$ con $r = 0$ o $N(r) < N(b)$. Como $r = a - bq \in I$, si $N(r) < N(b)$ obtenemos una contradicción con la minimalidad de $N(b)$ sobre I, y concluimos que $r = 0$ y $b|a$. Por lo tanto $I = (a)$. □

3.4. Polinomios

En esta sección estudiaremos el anillo de polinomios a coeficientes en un anillo conmutativo R.

Definamos el *anillo de polinomios en una variable sobre* R, escrito $R[X]$, como el conjunto de sucesiones de soporte finito en R, esto es, el conjunto de todos los elementos de la forma $(a_0, a_1, a_2, a_3, \ldots, a_{n-1}, a_n \ldots)$ con $a_i \in R$ para cada $i \in \mathbb{N}$ y tal que existe $m \in \mathbb{N}$ que verifica $a_n = 0$ para todo $n > m$. Dotemos a $R[X]$ la suma coordenada a coordenada

$$(a_i)_i + (b_i)_i = (a_i + b_i)_i$$

y la multiplicación dada por la convolución de sucesiones, es decir

$$(a_i)_i (b_i)_i = (c_i)_i$$

donde para cada $n \in \mathbb{N}$ se define $c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{i+j=n} a_i b_j$. Por ejemplo,

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 + a_1 b_0$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_0 b_2$$

$$\vdots$$

La multiplicación está bien definida: si $(a_i)_i$ y $(b_i)_i$ son tales que $a_k = 0$ para cada $k > n$ y $b_k = 0$ para cada $k > m$, entonces $c_{n+m} = a_n b_m$ y además $c_k = 0$ para todo $k > n + m$. A partir de las propiedades correspondientes en R, es directo ver que $R[X]$ es un anillo conmutativo con neutro aditivo $(0, 0, 0, \ldots)$ y neutro multiplicativo $(1, 0, 0, \ldots)$. Más aún podemos definir $\psi : R \to R[X]$ por $\psi(r) = (r, 0, 0, 0, \ldots)$ y resulta ser un monomorfismo de anillos. Abusando de la notación, denotaremos a las imágenes $\psi(r)$ por r.

Por otra parte, si denotamos por X a la sucesión $(0, 1, 0, 0, \ldots)$, entonces

$$X^2 = (0, 0, 1, 0, 0, 0, \ldots),$$

$$X^3 = (0, 0, 0, 1, 0, 0, \ldots),$$

$$X^4 = (0, 0, 0, 0, 1, 0, \ldots),$$

y en general, si $n \in \mathbb{N}$ entonces $X^n = (\delta_{ni})_i$. A partir de lo anterior obtenemos que si $p = (a_i)_i$ y $m \in \mathbb{N}$ tal que $a_k = 0$, para cada $k > m$, entonces podemos escribir

$$p = a_0(\delta_{0i})_i + a_1(\delta_{1i})_i + \ldots + a_m(\delta_{mi})_i = a_0 + a_1 X + a_2 X^2 + \cdots + a_m X^m.$$

A cada elemento $p \in R[X]$ le llamamos *polinomio* y también lo anotamos como $p(X)$. Si $p = (a_i)_{i \in \mathbb{N}}$ no es el polinomio nulo, entonces hay algún número natural n tal que $a_n \neq 0$. Al mayor entero n tal que $a_n \neq 0$ se le llama el grado del polinomio p, y lo anotamos por $\text{grad}(p(X))$ o $\deg(p(X))$. Definimos el grado del polinomio nulo como $-\infty$. Si $p(X) = \sum_{k=0}^{n} a_k X^k$ no es el polinomio nulo y tiene grado n, entonces al elemento a_n de R se le llama el *coeficiente líder* de $p(X)$. Si el coeficiente lider de un polinomio no nulo es 1, entonces decimos que el polinomio es *mónico.* A veces se escribe $[X^n]p(X)$ para denotar al coeficiente que acompaña a X^n en $p(X)$.

Proposición 3.9. *Sea R un anillo conmutativo y $p(X), q(X) \in R[X]$.*

1. $\text{grad}(p(X)+q(X)) \leq \text{máx}\{\text{grad}(p(X)), \text{grad}(q(X))\}$.
2. $\text{grad}(p(X)q(X)) \leq \text{grad}(p(X)) + \text{grad}(q(X))$ *con igualdad si R es un dominio.*

Demostración. Sean $p(X) = \sum_{k=0}^{n} a_k X$ y $q(X) = \sum_{k=0}^{m} b_k X^k$ donde $n = \text{grad}(p(X))$ y $m = \text{grad}(q(X))$. Para probar 1. notemos que

$$p(X) + q(X) = \sum_{k=0}^{\text{máx}\{n,m\}} (a_k + b_k) X^k$$

donde $a_k = 0$ cuando $k > n$ y $b_k = 0$ cuando $k > m$. La desigualdad cuando $p(X)$ o $q(X)$ es nulo es directa.

Para probar 2. notemos que la definición de $p(X)q(X)$ implica que el grado de $p(X)q(X)$ es a lo más $n+m$, con igualdad ssi el coeficiente $a_n b_m \neq 0$. La desigualdad cuando $p(X)$ o $q(X)$ es nulo nuevamente es directa. □

Definimos también las *series de Laurent* a coeficientes en R como

$$R((X)) = \{f : \mathbb{Z} \to R;\ \exists k \in \mathbb{Z},\ \forall j < k \quad f(j) = 0\}$$

y las *series formales* a coeficientes en R como

$$R[[X]] = \{f \in R((X));\ f(j) = 0\ \forall j < 0\}.$$

Es decir, las series formales son básicamente polinomios de grado infinito y las series de Laurent son series formales donde permitimos una cantidad finita de términos del tipo $a_{-k}X^{-k}$ con $k \in \mathbb{N}$. Dotamos a ambos conjuntos de la suma componente a componente y la multiplicación dada por $(a_k)_k \cdot (b_k)_k = (c_k)_k$ donde $c_k = \sum_{j \in \mathbb{Z}} a_{k-j} b_j$. Al igual que antes se verifica que la multiplicación está bien definida. Es claro que los polinomios se incluyen de manera natural en las series formales, y usaremos la misma notación que antes para escribir una serie formal como sumas de monomios.

Definimos el *orden* de una serie formal $p(X) = \sum_{k \geq 0} a_k X^k$, escrito $\text{ord}(p(X))$, como el mínimo entero k tal que $a_k \neq 0$, o ∞ si $p(X)$ es nulo. De manera análoga se demuestran propiedades similares a las del grado: si $p(X), q(X) \in R((X))$, entonces

1. $\text{ord}(p(X)+q(X)) \geq \text{mín}\{\text{ord}(p(X)), \text{ord}(q(X))\}$.
2. $\text{ord}(p(X)q(X)) \geq \text{ord}(p(X)) + \text{ord}(q(X))$ con igualdad cuando R es un dominio.

La siguiente proposición caracteriza las unidades de $R((X))$:

Proposición 3.10. *Sea R un dominio. Luego $p(X) = \sum_{k \geq 0} a_k X^k \in R((X))$ es unidad ssi $a_{ord(p(X))}$ lo es en R.*

Demostración. Notemos que $p(X) \in R((X))$ es unidad ssi $h(X) = X^{\text{ord}(p(X))} p(X)$ lo es (pues los X^k tienen inversos X^{-k} en $R((X))$), y que si escribimos $h(X) = \sum_{k \geq 0} b^k X^k$, entonces $b_0 = a_{\text{ord}(p(X))}$. Luego podemos reducirnos al caso en que $p(X) \in R[[X]$ y $\text{ord}(p(X)) = 0$.

Notemos primero que $p(X) \in R[[X]]$ no puede tener un inverso en $R((X))\backslash R[[X]]$, pues como R es dominio tenemos que si $p(X)$ es invertible entonces

$$0 = \text{ord}(1) = \text{ord}(p(X)) + \text{ord}(p(X)^{-1}) = \text{ord}(p(X)^{-1}).$$

Si a_0 es una unidad en R, tratemos de construir un inverso de $p(X)$ en $R[[X]]$: si $g(X) = \sum_{k\geq 0} b_k X^k \in R[[X]$ es tal que

$$p(X)g(X) = \sum_{k\geq 0}\sum_{j=0}^{k} a_{k-j}b_j X^k = 1,$$

entonces igualando los coeficientes de ambos lados de la ecuación obtenemos que $\sum_{j=0}^{k} a_{k-j}b_j = \delta_{1k}$ para cada $k \in \mathbb{N}$. Si a_0 es invertible en R, entonces podemos despejar los b_k como $b_0 = a_0^{-1}$ y $b_k = -a_0^{-1}\sum_{i=1}^{k} a_i$para $k \geq 1$.

Recíprocamente, la ecuación 3.4 muestra que cuando a_0 no es unidad en R entonces la ecuación $a_0 b_0 = 1$ no se puede resolver para b_0, y por lo tanto $p(X)$ no tiene inverso en $R[[X]]$. □

En particular, si K es un cuerpo entonces $K((X))$ también lo es.

En lo que sigue, nos restringiremos a trabajar con polinomios.

Proposición 3.11. *D es un dominio si y solo si $D[X]$ es un dominio, y en tal caso las unidades de $D[X]$ son las unidades de D.*

Demostración. Si $D[X]$ es un dominio, la copia de D en $D[X]$ también lo es. Recíprocamente, si D es un dominio, entonces la igualdad $\deg(p(X)q(X)) = \deg(p(X)) + \deg(q(X))$ muestra que $p(X)q(X)$ no puede ser nulo sin que $p(X)$ o $q(X)$ lo sea.

Por otro lado, es claro que si $d \in D$ es unidad entonces también lo es en $D[X]$. Ahora supongamos que $p(X)$ es invertible en $D[X]$ y sea $p^{-1}(X)$ su inverso, entonces

$$0 = \deg(1) = \deg(p(X)p^{-1}(X)) = \deg(p(X)) + \deg(p^{-1}(X))$$

Por lo tanto $\deg(p(X)) = 0 = \deg(p^{-1}(X))$, es decir $p(X) \in D$ y su inverso también está en D. □

Sea $\alpha \in R$. La *evaluación en α* es el morfismo de anillos $\psi_\alpha \colon R[X] \to R$ definida por $\psi_\alpha(p(X)) = \sum_{k=0}^{n} a_k\alpha^k$ donde $p(X) = \sum_{k=0}^{n} a_k X^k$. También escribimos $p(\alpha) = \psi_\alpha(p(X))$ y llamamos *función polinomial* asociada a $p(X)$ a la función de R en sí mismo dada por $\alpha \mapsto p(\alpha)$. Si $p(X) \in R[X]$ y $\alpha \in \mathbb{R}$ es tal que $p(\alpha) = 0$, decimos que α es una raíz de $p(X)$.

Ejemplo 3.22.

- Consideremos el polinomio $p(X) = X^2 + X$ en $\mathbb{Z}_6[X]$. Notemos que su función polinomial asociada es tal que $p(0) = p(5) = p(2) = p(3) = 0$ y $p(1) = p(4) = 2$. Luego este polinomio de grado 2 tiene 4 raíces.
- En $\mathbb{Z}_6[X]$ los polinomios $1 + 2X$ y $1 + 3X$ son polinomios de grado 1 cuyo producto es también un polinomio de grado 1. Los polinomios $2 + 2X^2$ y $3X + 3X^4$ son polinomios no nulos cuyo producto es el polinomio nulo.
- Si p es primo, el pequeño teorema de Fermat (ver el ejemplo 2.3) muestra que para cada $x \in \mathbb{Z}_p$ se cumple que $x^p = x$. Luego el polinomio $p(X) = X^p - X \in \mathbb{Z}_p[X]$ tiene asociada la función nula, pese a no ser el polinomio nulo.

Uno de los resultados más importantes del anillo de polinomios sobre un cuerpo es la existencia un algoritmo de división. Si el anillo R no es cuerpo también existe una algoritmo de la división pero cuando el coeficiente líder del divisor $d(X)$ es invertible. El enunciado preciso es como sigue:

Teorema 3.10 (Algoritmo de la división)**.** *Sea R un anillo conmutativo y $p(X), d(X) \in R[X]$ tal que el coeficiente líder de $d(X)$ es una unidad en R. Entonces existen únicos polinomios $q(X)$ y $r(X)$ tales que $p(X) = d(X)q(X) + r(X)$ con $\text{grad}(r(X)) < \text{grad}(d(X))$.*

Demostración. Veamos la unicidad: si

$$p(X) = d(X)q(X) + r(X) = d(X)q'(X) + r'(X)$$

y $r(X) \neq 0 \neq r'(X)$ con $\text{grad}(r(X)) < \text{grad}(d(X))$ y $\text{grad}(r'(X)) < \text{grad}(d(X))$, entonces

$$d(X)(q(X) - q'(X)) = r'(X) - r(X).$$

Como el coeficiente líder de $d(X)$ no es un divisor de cero, entonces si $q(X) - q'(X)$ no es el polinomio nulo, se tiene que $\text{grad}(d(X)(q(X) - q'(X))) = \text{grad}(d(X)) + \text{grad}((q(X) - q'(X))) \geq \text{grad}(d(X))$, pero por otra parte si $r'(X) - r(X)$ no es el polinomio nulo $\text{grad}(r'(X) - r(X)) \leq \text{máx}\{\text{grad}(r'(X)), \text{grad}(r(X))\} < \text{grad}(d(X))$ y obtenemos una contradicción.

Ahora la existencia: notemos primero que $d(X)$ es no nulo, pues su coeficiente líder es una unidad. Si $\text{grad}(d(X)) > \text{grad}(p(X))$, entonces basta tomar $q(X) = 0$ y $r(X) = p(X)$. Consideremos el caso $p(X)$ no nulo y $\text{grad}(d(X)) \leq \text{grad}(p(X))$. Haremos inducción sobre el grado de p. Si $\text{grad}(p) = 0$, entonces $\text{grad}(d(X)) \leq \text{grad}(p(X))$ implica que $\text{grad}(d(X)) = 0$. Por lo tanto $p(X)$ y $d(X)$ son elementos de R no nulos y $d(X)$ es unidad en R. Luego $p(X) = d(X)(d(X)^{-1}p(X)) + 0$ y basta tomar $q(X) = d(X)^{-1}p(X)$ y $r(X) = 0$. Supongamos que la propiedad es cierta para todo polinomio $p(X) = \sum_{k=0}^{n} a_k X^n$ de grado menor o igual a n y divisor $d(X) = \sum_{k=0}^{m} b_k X^m$ con b_m unidad, $a_n \neq 0$ y $m \leq n$. El polinomio $(a_n b_m^{-1} X^{n-m})d(X)$ tiene grado n y coeficiente líder a_n al igual que $p(X)$, y por lo tanto al hacer la resta $p(X) - (a_n b_m^{-1} X^{n-m})d(X)$ se obtiene un polinomio de grado menor que n, o el polinomio nulo. Si $p(X) - (a_n b_m^{-1} X^{n-m})d(X) = 0$, entonces basta tomar $q(X) = a_n b_m^{-1} X^{n-m}$ y $r = 0$. Si $p(X) - (a_n b_m^{-1} X^{n-m})d(X)$ es un polinomio de grado menor que n y no nulo, entonces la hipótesis inductiva entrega la existencia de $q'(X)$ y $r(X)$ con $\text{grad}(r(X)) < \text{grad}(d(X))$ tales que:

$$p(X) - (a_n b_m^{-1} X^{n-m})d(X) = d(X)q'(X) + r(X),$$

es decir

$$p(X) = d(X)(q'(X) + a_n b_m^{-1} X^{n-m}) + r(X).$$

Tomando $q(X) = q'(X) + a_n b_m^{-1} X^{n-m}$ obtenemos lo que queríamos probar. □

Corolario 3.3 (Teorema del Resto)**.** *Si R es un anillo conmutativo y $p(X) \in R[X]$ y $\alpha \in R$, entonces existe $q(X)$ tal que $p(X) = (X - \alpha)q(X) + p(\alpha)$.*

Demostración. Si $p(X) = 0$, entonces basta tomar $r(X) = 0 = q(X)$. Si $p(X)$ no es el polinomio nulo, por el teorema anterior podemos tomar $d(X) = (X - \alpha)$, cuyo coeficiente líder es 1, y tenemos que existe $q(X)$ y $r(X)$ tales que $p(X) = q(X)(X - \alpha) + r(X)$ donde el grado de $r(X)$ es menor que $1 = \text{grad}((X - \alpha))$, es decir, $r(X) \in R$. Considerando la función polinomial asociada a p y evaluando en α se tiene que $p(\alpha) = q(\alpha)(\alpha - \alpha) + r(X) = r(X)$, lo que termina la demostración. □

Corolario 3.4. *Si R es un anillo conmutativo, entonces $\alpha \in R$ es raíz de $p(X)$, si y solo si existe $q(X) \in R[X]$ tal que $p(X) = q(X)(X - \alpha)$.*

Observación 3.6. En el caso del polinomio $p(X) = X^2 + X$ en $\mathbb{Z}_6[X]$ del ejemplo 3.22, notamos que tiene como raíces $0, 2, 3$ y 5, y si factorizamos $p(X) = X(X + 1) = X(X - 5)$. En esta descomposición se ven claramente las raíces 0 y 5, pero por ningún lado se ven las raíces 2 y 3. Esto podría hacer pensar que el corolario anterior es falso, pero no hay problema alguno. La razón es que $X(X + 1) = X(X - 5)$ no es la única forma de descomponer $p(X)$ en $\mathbb{Z}_6[X]$. Otra forma de descomponer $X^2 + X \in \mathbb{Z}_6[X]$ es $X^2 + X = (X - 2)(X + 3) = (X - 2)(X - 3)$ y aquí vemos que $p(X)$ tiene raíces 2 y 3. Si R es un cuerpo, entonces esta situación no ocurrirá en $R[X]$, es decir, la descomposición en $R[X]$ es única en algún sentido que describiremos más adelante.

El próximo resultado usa fuertemente el que D sea un dominio, de modo que su conclusión no aplica al polinomio de la observación anterior.

Corolario 3.5. *Si D es un dominio y $n \in \mathbb{N}$, entonces un polinomio de grado n en $D[X]$ tiene a lo más n raíces distintas en D.*

Demostración. Sean $\{\alpha_1, \alpha_2, \alpha_3, \dots, \} \subseteq D$ las raíces distintas de $p(X)$, un polinomio en $D[X]$ de grado n. Notemos que en particular no es el polinomio nulo. Definamos $m = |\{\alpha_i\}| \leq \infty$. Por el corolario anterior se tiene que existe $q_1(X) \in D[X]$ tal que $p(X) = q_1(X)(X - \alpha_1)$, y evaluando en α_2 se tiene que $0 = p(\alpha_2) = q_1(\alpha_2)(\alpha_2 - \alpha_1)$. Como $\alpha_2 - \alpha_1 \neq 0$ y D es un dominio, se tiene que $q_1(\alpha_2) = 0$. Nuevamente el corolario anterior se tiene que existe $q_2(X)$ tal que $q_1(X) = q_2(X)(X - \alpha_2)$ y por lo tanto $p(X) = q_2(X)(X - \alpha_2)(X - \alpha_1)$. Evaluando la igualdad anterior en α_3 se tiene que $0 = p(\alpha_3) = q_2(\alpha_3)(\alpha_3 - \alpha_2)(\alpha_3 - \alpha_1)$, y como $(\alpha_3 - \alpha_2)(\alpha_3 - \alpha_1) \neq 0$ y D es un dominio, se tiene que $q_2(\alpha_3) = 0$. Continuando inductivamente este argumento, se tiene que para cada $k \leq m$ existe $q_k(X)$ tal que

$$p(X) = q_k(X)(X - \alpha_k)(X - \alpha_{k-1}) \cdots (X - \alpha_2)(X - \alpha_1).$$

Como $p(X)$ no es el polinomio nulo, tampoco lo es $q_k(X)$, y dado que D es dominio tenemos que

$$n = \deg(p(X)) = \deg(q_k(X)(X - \alpha_k)(X - \alpha_{k-1}) \cdots (X - \alpha_2)(X - \alpha_1))$$

$$= \deg(q_k(X)) + k \geq k.$$

Concluimos que $m \leq n$, es decir, el número de raíces distintas de un polinomio es menor o igual al grado del polinomio. □

Observación 3.7. Si D es un dominio infinito, entonces el único polinomio que tiene a todos los elementos de D como raíces es el polinomio nulo. Más generalmente, si dos polinomios $p(X)$ y $q(X)$ son tales que sus funciones polinomiales coinciden, entonces el polinomio $P(X) = p(X) - q(X)$ tiene a todos los elementos de D como raíces. Por lo tanto $P(X)$ es el polinomio nulo y $p(X) = q(X)$ como polinomios.

Teorema 3.11 (Algoritmo de la división en un cuerpo K)**.** *Sea K un cuerpo y $p(X), d(X) \in K[X]$ tal que $d(X)$ es no nulo. Entonces existen únicos polinomios $q(X)$ y $r(X)$ tales que*

$$p(X) = d(X)q(X) + r(X)$$

con $\text{grad}(r(X)) < \text{grad}(d(X))$*. En particular, $K[X]$ es un dominio euclídeo, un DIP y un DFU.*

Ejemplo 3.23. Consideremos el anillo de polinomios con coefientes en $\mathbb{R}$ y el ideal I generado por el polinomio $c(X) = X^2 + 1$. Supongamos que $J = (p(X))$ es un ideal que contiene a I. Como $I \subseteq J$, en particular $X^2 + 1 \in J$, es decir, existe $q(X)$ tal que $X^2 + 1 = p(X)q(X)$ y luego $deg(p(X) + \deg(q(X)) = 2$. Luego el grado de $p(X)$ es $0, 1$ o 2.

Si el grado de $p(X)$ es cero, entonces $p(X) = p$ es un elemento no nulo de $\mathbb{R}$ y concluimos que $J = (p) = \mathbb{R}[X]$. Si el grado de $p(X)$ es 2, entonces $q(X)$ es un elemento no nulo de $\mathbb{R}$, entonces $q(X) = q$ es invertible en $K[X]$, entonces $X^2 + 1 = q(p(X))$ si y solo si $q^{-1}(X^2 + 1) = p(X)$, es decir $p(X) \in I$, es decir $J = I$. Si $\deg(p(X)) = 1$, digamos $p(X) = aX + b$ con $a \neq 0$, entonces $-b/a$ sería una raíz de $X^2 + 1$ en $\mathbb{R}$, lo cual es falso. Por lo tanto si $I \subseteq J$, entonces $J = I$ o $J = \mathbb{R}[X]$. Es decir, $I = (X^2 + 1)$ es un ideal maximal en $\mathbb{R}[X]$.

Por lo tanto el cuociente $\mathbb{R}[X]/I$ es un cuerpo. El ejemplo 3.21 muestra que

$$\mathbb{R}[X]/I = \{aX + b + (X^2 + 1);\ a, b \in \mathbb{R}\}.$$

Además notamos que $(aX + b) + I + (cX + d) + I = (a + c)X + (b + d) + I$ y por otro lado

$$\begin{aligned}(aX + b)(cX + d) &= acX^2 + (ad + bc)X + bd + I \\ &= ac(X^2 + 1 - 1) + (ad + bc)X + bd + I \\ &= (ad + bc)X + (bd - ac) + I.\end{aligned}$$

Por lo tanto es directo ver que el morfismo $\phi : \mathbb{R}[X]/I \to \mathbb{C}$ definido por $\phi(aX + b + I) = ai + b$ es un isomorfismo de cuerpos, pues es claramente sobreyectiva y además $ai + b = 0$ implica que $b = a = 0$ (ya que son reales), lo que muestra que ϕ es inyectiva.

Terminemos esta sección con una herramienta importante para el estudio de extensiones de cuerpos. Definimos la *derivada formal* de un polinomio $p(X) = \sum_{k=0}^{n} a_k X^k$ como $p(X)' = \sum_{k=1}^{n} k a_k X^k$. Es directo ver que cuando $c \in R$ y $p(X), q(X) \in R[X]$ entonces $(cp(X) + q(X))' = cp(X)' + q(X)'$, y en el próximo

capítulo veremos que esto dice que $(\cdot)' \colon R[X] \to R[X]$ es un morfismo de R-módulos. Por otro lado, si $m \in \mathbb{N}$ entonces

$$\begin{aligned}(X^m p(X))' &= \left(\sum_{k=0}^{n} a_k X^{k+m}\right)' = \sum_{k=1}^{n} (k+m) a_k X^{k+m-1} \\ &= \sum_{k=1}^{n} k a_k X^{k-1} X^m + \sum_{k=1}^{n} m a_k X^k X^{m-1} \\ &= X^m \sum_{k=1}^{n} k a_k X^{k-1} + m X^{m-1} \sum_{k=1}^{n} a_k X^k = X^m (p(X))' + (X^m)' p(X)\end{aligned}$$

de modo que por linealidad podemos concluir que para cada par $p(X), q(X) \in R[X]$ se verifica la regla de Leibniz $(p(X)q(X))' = p(X)'q(X) + p(X)q(X)'$. Esta propiedad y una inducción corta muestran que para cada $\alpha \in R$, $m \in \mathbb{N}$ se tiene que $(X-\alpha)^{m\prime} = m(X-\alpha)^{m-1}$, y más generalmente $p(X)^{m\prime} = m p(X)^{m-1}$ cuando $p(X) \in R[X]$.

Diremos que $\alpha \in R$ es una raíz múltiple de $p(X)$ si $p(X) = (X-\alpha)^m q(X)$ con $m \geq 2$ y $q(X) \in R[X]$. Si α no es raíz de $q(X)$ diremos que α es una raíz de *multiplicidad* m. Notemos que si lo anterior ocurre, entonces $p(X)' = (X-\alpha)^m q(X)' + m(X-\alpha)^{m-1} q(X)$ y luego α también es raíz de $p(X)'$. Recíprocamente, si α es raíz de $p(X)$ y $p(X)'$, entonces derivando $p(X) = (X-\alpha)q(X)$ tenemos que $q(X) = p(X)' - (X-\alpha)q(X)'$ y α es raíz de $q(X)$. Luego α es raíz múltiple de $p(X)$. Hemos demostrado el siguiente resultado.

Proposición 3.12. *$\alpha \in R$ es raíz múltiple de $p(X) \in R[X]$ ssi α es raíz de $p(X)$ y $p(X)'$.*

En particular, si R es un dominio y $\operatorname{mcd}(p(X), p(X)') = 1$ entonces $p(X)$ no tiene raíces múltiples en cualquier cuerpo que contenga a R.

3.5. Polinomios sobre un DFU

En esta sección estudiaremos propiedades del anillo de polinomios sobre un DFU y en particular la irreducibilidad de estos polinomios. En lo que sigue D siempre denotará un DFU.

Si $p(X) = \sum_{k=0}^{n} a_k X^k \in D[X]$, entonces definimos el *contenido* de $p(X)$ como $c(p) = \operatorname{mcd}(\{a_0, \ldots, a_n\})$, que existe pues D es DFU. Notemos que el contenido está definido salvo por la multiplicación de una unidad. Si escribimos $d = c(p)$, entonces $a_i = d a_i'$ para ciertos $a_i' \in D$ y obtenemos la descomposición $p(X) = d p'(X)$ donde $p'(X) = \sum_{k=0}^{n} a_i' X^i$ tiene contenido 1. Un polinomio cuyo contenido es una unidad se dice *primitivo*. Luego para cada polinomio se puede factorizar $p(X) = c(p) p'(X)$ con $p'(X)$ primitivo. Más aún, si $p(X) = e h(X)$ con $e \in D$ y $h(X) = \sum_{k=0}^{n} b_i X^i$ primitivo, entonces $a_i = e b_i$ y además $c(p) = \operatorname{mcd}(\{e b_1, \ldots, e b_n\})$, que es asociado a $e \operatorname{mcd}(\{b_1, \ldots, b_n\}) = e$.

Teorema 3.12 (Lema de Gauss)**.** *El producto de polinomios primitivos también es primitivo.*

Demostración. Sea D un DFU y $p(X), q(X) \in D[X]$ primitivos tales que $p(X)q(X)$ no lo es. Escribamos $d = c(p(X)q(X))$ y tomemos p un divisor primo de d. Notemos que p no divide a $p(X)$ ni a $q(X)$ pero sí a su producto. Consideremos ahora el dominio de integridad $\bar{D} = D/(p)$ y definamos el morfismo $\psi : D[X] \to \bar{D}[X]$ como la reducción módulo p de cada coeficiente, es decir

$$\psi\left(\sum_{k=0}^{n} a_k X^k\right) = \sum_{k=0} \pi(a_k) X^k$$

donde π es la proyección canónica a $\bar{D}$. Luego $\psi(p(X))\psi(g(X)) = \psi((p(X)g(X)) = 0$ ya que d divide a $p(X)g(X)$, pero tanto $\psi(p(X))$ como $\psi(g(X))$ son no nulos. Obtenemos una contradicción con que $\bar{D}$ es dominio y concluimos que $p(X)q(X)$ debe ser primitivo. □

Ahora notemos que si $p(X) \in Q(D)[X]$ es no nulo, podemos encontrar $b \in D$ tal que $bp(X) = h(X) \in D[X]$ (tomando b como el mcd de los denominadores de los coeficientes de $p(X)$ por ejemplo). Luego podemos escribir $p(X) = c(h(X))/bh'(X)$ con $h'(X)$ primitivo. Si tenemos dos factorizaciones $p(X) = \beta q(X) = \beta' q'(X)$ con $\beta, \beta' \in Q(D)$ y $q(X), q'(X) \in D[X]$ primitivos, entonces podemos escribir $\beta = a/b$ y $\beta' = a'/b'$ con $a, a' \in D$ y $b, b' \in D^*$, de manera que $ab'q(X) = a'bq'(X)$. Como $q(X)$ y $q'(X)$ son primitivos, $ab' = c(ab'q(X))$ es asociado a $a'b = c(a'bq'(X))$, y obtenemos que β y β' difieren por multiplicación por una unidad de D. Concluimos que para cada $p(X) \in Q(D)[X]$ no nulo podemos encontrar $\beta \in Q(D)$ y $q(X) \in D[X]$ primitivo tales que $p(X) = \beta q(X)$ y β es único salvo unidad de D. Llamamos a tal β el contenido de $p(X)$.

Observación 3.8. Sean $p(X), q(X) \in D[X]$ primitivos y asociados en $Q(D)$, es decir existe $\delta \in Q(D)$ no nulo tal que $p(X) = \delta q(X)$. Escribiendo $\delta = a/b$ con $a, b \in D^*$ obtenemos que $bp(X) = aq(X)$. Como $p(X), q(X)$ son primitivos, tenemos que a y b son asociados en $D[X]$ y por ende existe $u \in D^\times$ tal que $\delta = a/b = u$. Es decir, en realidad $p(X)$ y $q(X)$ son asociados en D.

Proposición 3.13. *Sea $p(X) \in D[X]$ de grado positivo. $p(X)$ es irreducible en $D[X]$ ssi es primitivo y es irreducible en $Q(D)[X]$.*

Demostración. Probemos la implicancia $\Rightarrow$: notemos que tal $p(X)$ debe ser primitivo, pues en caso contrario existiría $p \in D$ primo (y entonces irreducible en D) que dividiría a $p(X)$, y como p también sería irreducible en $D[X]$ obtendríamos una contradicción con que $p(X)$ tiene grado positivo. Ahora supongamos que $p(X)$ es reducible en $Q(D)[X]$, digamos $p(X) = a(X)b(X)$ con $a(X), b(X) \in Q(D)[X]$ de grado positivo. Descompongamos $a(X) = \alpha a'(X)$ y $b(X) = \beta b'(X)$ con $\alpha, \beta \in Q(D)$ y $a'(X), b'(X) \in D[X]$ primitivos. El lema de Gauss muestra que $a'(X)b'(X)$ es primitivo, y la igualdad $p(X) = \alpha\beta a'(X)b'(X)$ implica que $p(X)$ y $a'(X)b'(X)$ son asociados en $Q(D)$. La observación anterior implica que son asociados en D, es decir que existe $u \in D^\times$ tal que $p(X) = ua'(X)b'(X)$, lo que contradice la irreducibilidad de $p(X)$ en $D[X]$.

Ahora $\Leftarrow$: supongamos que podemos factorizar $p(X) = q(X)h(X)$ con $q(X), h(X) \in D[X]$. Como $p(X)$ es irreducible en $Q(D)[X]$, sin pérdida de generalidad podemos suponer que $q(X)$ es una unidad en $Q(D)[X]$, es decir, $q(X) = q \in Q(D)^\times$. Notemos que $q = q(X) \in D$, y debe ser una unidad pues $p(X)$ es primitivo. Luego $p(X)$ es irreducible en $D[X]$. □

Teorema 3.13. *Un anillo conmutativo R es DFU ssi $R[X]$ es DFU.*

Demostración. Si $R[X]$ es DFU, entonces cada $r \in R^*$ se puede factorizar únicamente (salvo unidades de $R[X]$, es decir, unidades de R) como irreducibles de $R[X]$ de grado 0, es decir, irreducibles de R. Concluimos notando que R también debe ser dominio porque $R[X]$ lo es.

Recíprocamente, supongamos que R es un DFU. Como R es dominio, $R[X]$ también lo es. Sea $p(X) \in R[X]$ de grado positivo y notemos que sin pérdida de generalidad podemos tomar $p(X)$ primitivo, pues si no, la escritura $p(X) = c(p(X))\bar{p}(X)$ donde $\bar{p}(X)$ es primitivo permite concluir el caso general. Ahora como $Q(R)[X]$ es un DFU (pues es DIP), $p(X)$ se puede escribir como producto de irreducibles $p_1(X), \dots, p_k(X)$ en $Q(R)[X]$. Cada $p_i(X)$ se puede descomponer como $p_i(X) = \beta_i h_i(X)$ donde $h_i(X) \in R[X]$ es primitivo y $\beta_i = c(p_i(X)) \in Q(R)$, y sigue por el lema de Gauss que $p(X) = \prod_i \beta_i h(X)$ con $h(X) \in R[X]$ primitivo. La observación 3.8 muestra que $\prod_i \beta_i \in R^\times$ y entonces podemos escribir $p(X) = uh_1(X)\cdots h_k(X)$ con $u \in R^\times$ y los $h_i(X)$ primitivos e irreducibles en $R[X]$.

Finalmente, la escritura es única: si $p_1(X)\cdots p_k(X) = q_1(X)\cdots q_m(X)$ donde los $p_i, q_i \in R[X]$ son irreducibles en $R[X]$, entonces $k = m$ y cada p_i es asociado a q_i en $Q(R)[X]$ (salvo un reordenamiento de índices), pues $Q(R)[X]$ es un DFU y los p_i, q_i también son irreducibles en $Q(R)[X]$ por la proposición anterior. La observación 3.8 muestra que los p_i, q_i son asociados en R. Concluimos que $R[X]$ es DFU. □

Ejemplo 3.24. Dado $n \in \mathbb{N}$ y un anillo conmutativo R, definimos inductivamente el *anillo de polinomios en n variables a coeficientes en R* por $R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$. Si I es un conjunto de índices arbitrario, definimos el *anillo de polinomios en $|I|$ variables a coeficientes en R* como

$$\bigcup_{i_1,\dots,i_k \in I; k \in \mathbb{N}} R[X_{i_1}, \dots, X_{i_k}]$$

con la suma y el producto natural. El resultado anterior muestra que todos estos anillos son DFU si R lo es.

Proposición 3.14 (Criterio de Eisenstein)**.** *Sea D un DFU. Si $p(X) = \sum_{k=0}^n a_k X^k \in D[X]$ tiene grado n y $p \in D$ es irreducible tal que p no divide a a_n, p divide a a_i para $i = 0, 1, \dots, n-1$ y p^2 no divide a a_0, entonces $p(X)$ es irreducible en $Q(D)[X]$.*

Demostración. Como p no divide a a_n tenemos que p no divide a $c(p)$, luego escribiendo $p(X) = c(p)p'(X)$ con $p'(X) = \sum_{k=0}^n a'_k X^k \in D[X]$ primitivo vemos que p no divide a a'_n, p divide a a'_i para $i = 0, 1, \dots, n-1$ y p^2 no divide a a_n vemos que p no divide a a'_n, p divide a a'_i para $i = 0, 1, \dots, n-1$ y p^2 no divide a a'_n. Como $c(p)$ es una unidad en $Q(D)[X]$, basta demostrar que $p'(X)$ es irreducible en $Q(D)[X]$ y la proposición anterior muestra que basta demostrar que lo es en $D[X]$.

Supongamos entonces que $p'(X) = g(X)h(X)$ con $g(X) = \sum_{k=0}^r g_k X^k$ y $h(X) = \sum_{k=0}^s h_k X^k$ polinomios en $D[X]$ de grado $r, s \geq 1$ respectivamente. Como $a'_0 = g_0 h_0$ y $p | a_0$, entonces sin pérdida de generalidad podemos suponer que $p | g_0$. Notemos que como p^2 no divide a a'_0 entonces p no divide a h_0. Si p dividiera a todos los coeficientes de $g(X)$, entonces p dividiría a todos los coeficientes de $p'(X)$, lo que no es cierto.

Definamos entonces k como el menor entero positivo tal que g_k no es divisible por p. Como

$$a'_k = g_k h_0 + \underbrace{g_{k-1}h_1 + g_{k-2}h_2 + \cdots + g_0 h_k}_{\text{divisible por } p}$$

y como p divide a a'_k, entonces p divide a g_k o a h_0 y obtenemos una contradicción. Luego $p'(X)$ es irreducible en $D[X]$ y $p(X)$ lo es en $Q(D)[X]$. □

Ejemplo 3.25. Si $p \in \mathbb{Z}$ es primo y $n \geq 1$, el polinomio $X^n - p$ es irreducible en $\mathbb{Q}[X]$ y en $\mathbb{Z}[X]$.

3.6. Ejercicios

Ejercicio 3.1.

a) Sea R un anillo y e un idempotente para la multiplicación que conmuta con todos los elementos de R (decimos que e es un *idempotente central*). Muestre que $R \cong eR \times (1-e)R$.

b) Pruebe que un anillo booleano finito es isomorfo a $\mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$.

Ejercicio 3.2. Sea R un anillo. Un elemento $u \in R$ se dice nilpotente si existe $n \in \mathbb{N}$ tal que $u^n = 0$.

a) Muestre que R no tiene nilpotentes ssi $a^2 = 0 \implies a = 0$ para todo $a \in R$ (y en particular cualquier dominio no tiene nilpotentes).

b) Asumamos que R es conmutativo. Muestre que si $u \in R$ es nilpotente, entonces $1+u$ es una unidad y concluya que la suma de un nilpotente con una unidad es una unidad.

Ejercicio 3.3. Si R es un anillo no unitario, verifique que $(\mathbb{Z} \times R, \bar{+}, \bar{\cdot})$ es un anillo unitario donde definimos $\bar{+}$ como la suma por coordenadas y $(m,a)\bar{\cdot}(n,b) = (mn, na + nb + ab)$, y que R es isomorfo a un subanillo de $\mathbb{Z} \times R$.

Ejercicio 3.4. Sea X un conjunto no vacío y consideremos el anillo $(\mathscr{P}(X), \triangle, \cap)$.

a) Muestre que $\mathscr{P}(X)$ es DIP ssi X es finito, y que para cada $A \subset X$ se tiene que $X \cong \mathscr{P}(A) \times \mathscr{P}(A^c)$.

b) Un *filtro* es una colección $\mathscr{F} \subset \mathscr{P}(X)$ tal que:
   1. $\emptyset \notin \mathscr{F}$.
   2. para todo $A, B \in \mathscr{F}$, $A \cap B \in \mathscr{F}$.
   3. para todo $A \in \mathscr{F}$ y $C \supset A$, $C \in \mathscr{F}$.

   Dado $\mathscr{F} \subset \mathscr{P}(X)$, definimos $I(\mathscr{F}) = \{A \subset X ; A^c \in \mathscr{F}\}$. Muestre que $\mathscr{F}$ es un filtro ssi $I(\mathscr{F})$ es un ideal propio.

c) Concluya que todo filtro puede ser extendido a un ultrafiltro (es decir, un filtro maximal para la inclusión).

Ejercicio 3.5. Sean $m_1, \ldots, m_k$ enteros coprimos entre sí y $a_1, \ldots, a_k$ enteros cualquiera. Definamos $m = m_1 \ldots m_k$ y $m'_i = m/m_i$ para $i \in [k]$. Muestre cómo calcular eficientemente t_i, el inverso módulo m_i de m'_i, y pruebe que la solución del sistema de congruencias

$$x \equiv a_1 \mod m_1, \ \ldots, \ x \equiv a_k \mod m_k$$

es $x = a_1 t_1 m_1' + \cdots + a_k t_k m_k'$ mód m.

Ejercicio 3.6. Sea R un anillo conmutativo.

a) Muestre que los elementos nilpotentes de R forman un ideal y encuentre un contraejemplo para esta afirmación cuando R no es conmutativo. Este ideal se llama el *nilradical de* R y se denota $\mathfrak{N}(R)$.

b) Muestre que $\mathfrak{N}(R) = \bigcap_{\mathfrak{p}\in \mathrm{Spec}(R)} \mathfrak{p}$ donde $\mathrm{Spec}(R)$ (el espectro primo de R) es el conjunto de todos los ideales primos de R.
Indicación: para la inclusión hacia la izquierda, tome un $x \in R$ no nilpotente y considere el conjunto $\{I \subset R; I \text{ ideal y } x^n \notin I\ \forall n > 0\}$.

c) Definimos el *radical de Jacobson* como la intersección de todos los ideales maximales de R y lo denotamos $\mathfrak{R}(R)$. Muestre que $x \in \mathfrak{R}(R)$ ssi $1 + xy$ es invertible para cada $y \in R$.

d) Encuentre el radical de Jacobson de $\mathbb{Z}_n$ en función de la factorización prima de n.

Ejercicio 3.7. Sea R un anillo conmutativo e $I \subset R$ un ideal cualquiera. Definimos el *radical de* I como $\mathrm{rad}(I) = \{r \in R; r^n \in I \text{ para algún } n \in \mathbb{N}\}$. Muestre que $\mathrm{rad}(I)$ es un ideal que contiene a I, y que $(\mathrm{rad}(I))/I = \mathfrak{N}(R/I)$.

Ejercicio 3.8. Un anillo conmutativo R se dice *Noetheriano* si cualquier cadena ascendente de ideales (no necesariamente principales) es estacionaria. Muestre que las siguientes afirmaciones son equivalentes.

1. R es Noetheriano.
2. Todo ideal de R es finitamente generado.
3. Toda colección no vacía de ideales de R tiene elemento maximal respecto a la inclusión.

Ejercicio 3.9. Un anillo R se dice *Artiniano* si cualquier cadena descendente de ideales es estacionaria. Consideremos un anillo R Artiniano. Pruebe que:

a) Si R es dominio, entonces también es cuerpo.

b) Si R es conmutativo, entonces todo ideal primo es maximal.

Ejercicio 3.10. Sea D un dominio de integridad.

a) Suponga que D satisface la condición de ideales principales ascendentes. Pruebe que todo $x \in D$ no nulo y no unidad se puede escribir como $x = c_1 c_2 \cdots c_{n_x}$ donde c_i es irreducible para $i \in [n_x]$.

b) Muestre que si D es DFU, D satisface la condición de ideales principales ascendentes.

c) Muestre que D es DFU ssi satisface la condición de ideales principales ascendentes y todo elemento irreducible es primo.

Ejercicio 3.11. Sea R un anillo. Para cada $E \subset R$ definimos $V(E) \subset \mathrm{Spec}(R)$ (ver el ejercicio 3.6) como el conjunto de todos los ideales primos que contienen a E. Muestre que:

a) Si I es el ideal generado por E, entonces $V(E) = V(I) = V(\mathrm{rad}(I))$.

b) Si I y J son ideales, entonces $V(IJ) = V(I \cap J) = V(I) \cup V(J)$. Generalice esto para un número finito de ideales.

c) Dada una colección de ideales $(I_\lambda)_{\lambda\in\Lambda}$, entonces $\bigcup_{\lambda\in\Lambda} V(I_\lambda) = V\left(\sum_{\lambda\in\Lambda} I_\lambda\right)$, donde $\sum_{\lambda\in\Lambda} I_\lambda$ es el ideal generado por $\bigcup_{\lambda\in\Lambda} I_\lambda$.

d) $V(0) = \text{Spec}(R)$ y $V(R) = \emptyset$.

Lo anterior prueba que la colección $\{V(E)\}_{E \subset R}$ es la colección de cerrados de un espacio topológico. La topología resultante se llama *topología de Zariski*.

Ejercicio 3.12. Sea R un anillo. Muestre que:

a) R es cuerpo ssi $R[X]$ es DIP.
b) Si R es conmutativo, (X) es ideal primo en $R[X]$ ssi R es un dominio.
c) Si R es conmutativo, (X) es ideal maximal en $R[X]$ ssi R es cuerpo.
d) Si R es conmutativo y $\mathfrak{p}$ es un ideal primo, entonces $\mathfrak{p}[X]$ (los polinomios con coeficientes en $\mathfrak{p}$) es un ideal primo de $R[X]$ ¿Es verdad que si $\mathfrak{m}$ es maximal en R, entonces $\mathfrak{m}[X]$ es maximal en $R[X]$?

Ejercicio 3.13. Si A es un anillo conmutativo y $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$, demuestre que f es una unidad en $A[X]$ ssi a_0 es una unidad en A y $a_1, \cdots, a_n$ son nilpotentes.
Indicación: si $b_0 + b_1X + \cdots + b_nX^n$ es el inverso de f puede probarse por inducción en r que $a_n^{r+1} b_{m-r} = 0$ lo que implica que a_n es nilpotente (no olvide que la suma de una unidad con un nilpotente es unidad).

Ejercicio 3.14. a) Sea D un DFU, y sea $q \in Q(D)$ raíz de un polinomio $a_mX^m + a_{m-1}X^{m-1} + \cdots + a_0$ donde los $a_i \in \mathbb{Z}$ y $m \geq 1$. Escriba $q = c/d$ con $r, d \in D$ y $\text{mcd}(c, d)$. Muestre que $c|a_0$ y $d|a_m$.

b) Sea K un cuerpo y $p(X) \in K[X]$ un polinomio tal que $\text{grad}(p(X)) \leq 3$. Muestre que $p(X)$ es irreducible en $K[X]$ ssi no tiene raíces en K.

Ejercicio 3.15. Sea R un dominio.

a) Pruebe que si $p(X), g(X) \in R[X]$ y definimos la composición $(p \circ g)(X) \in R[X]$ de la manera natural, entonces $(p \circ g)'(X) = (p' \circ g)(X)g'(X)$.
b) Sea $R(X) \doteq Q(R[X])$ el cuerpo de *funciones racionales* a coeficientes en R. Muestre que la derivada en $R(X)$ dada por

$$\left(\frac{p(X)}{q(X)}\right)' = \frac{p'(X)q(X) - p(X)q'(X)}{q(X)^2}$$

está bien definida, es lineal y coincide con la derivada en $R[X]$.

Ahora supondremos que F es un cuerpo de característica 0.

c) Dado $a \in F$ y $p(X) \in F[X]$, muestre que se cumple la fórmula de Taylor

$$p(X) = \sum_{k=0}^{n} \frac{p^{(k)}(a)}{k!}(X - a)^k$$

para cada $n \geq \text{grad}(p(X))$.
d) Recordemos que $a \in R$ es raíz múltiple de $p(X) \in R[X]$ ssi $p(a) = p'(a) = 0$. Generalice este test para detectar raíces de grado $m \in \mathbb{N}$.

Ejercicio 3.16. Muestre que cualquier función de un cuerpo finito en sí mismo es polinomial.

Ejercicio 3.17. Sea R un anillo conmutativo, $n \in \mathbb{N}$ y $A \in M_n(R)$.

a) Pruebe que $\det(A^t) = \det(A)$ y concluya que det es multilineal en las columnas.
b) Denotemos por $A(i|j)$ a la matriz en $M_{n-1}(R)$ que consiste en A sin la fila i ni la columna j. Pruebe la fórmula de Laplace:

$$\det(A) = \sum_{i=1}^{n}(-1)^{i+r}A_{i,r}\det(A(i|r)) = \sum_{j=1}^{n}(-1)^{l+j}A_{l,j}\det(A(l|j))$$

para cada $l, r \in [n]$.
c) Definamos la *adjunta* de A como la matriz $\operatorname{adj}(A) \in M_n(R)$ dada por $\operatorname{adj}(A)_{i,j} = (-1)^{i+j}\det(A(j|i))$. Muestre que $\operatorname{adj}(A)A = A\operatorname{adj}(A) = \det(A)I_n$.
d) Concluya que A es invertible en $M_n(R)$ ssi $\det(A)$ es invertible en R, y que la ecuación $AB = I$ implica que $BA = I$ para $B \in M_n(R)$.

Ejercicio 3.18. Considere el anillo de enteros gaussianos $\mathbb{Z}[i]$. Para $z \in \mathbb{C}$ definimos $N(z) = z\bar{z}$.
a) Muestre que $N(zw) = N(z)N(w)$ para cualquier par de complejos z y w.
b) Muestre que si $z, w \in \mathbb{Z}[i]$ y $w \neq 0$, entonces existen $q, r \in \mathbb{Z}[i]$ tales que $z = wq + r$ y $N(r) \leq N(w)/2$. Indicación: aproxime z/w.

Ejercicio 3.19. Sea D un dominio de integridad provisto de una función $\delta : D \to \mathbb{N}$ tal que:
1. $\delta(a) = 0$ ssi $a = 0$.
2. $\delta(ab) = \delta(a)\delta(b)$ para todo $a, b \in D$.
3. $\delta(a + b) \leq \max\{\delta(a), \delta(b)\}$ para todo $a, b \in D$.
4. Para cada $a, b \in D$ con $b \neq 0$ existen q y r tales que $a = bq + r$ y $\delta(r) < \delta(b)$.

Demuestre que D es un cuerpo o $D = K[X]$ con K un cuerpo.
Indicación: Muestre que los elementos b de D que cumplen $\delta(b) = 1$ son invertibles.

Ejercicio 3.20. Sea I un conjunto no vacío de índices dotado de un orden parcial $\leq$ y para cada $i \in I$ sea A_i un grupo abeliano aditivo. Supongamos que I es un conjunto dirigido (es decir que para cada $i, j \in I$ existe un $k \in I$ tal que $i, j \leq k$) y que para cada par de índices i, j con $i \leq j$ existe un mapa $\rho_{ij} : A_i \to A_j$ tal que:

- $\rho_{jk} \circ \rho_{ij} = \rho_{ik}$ cuando $i \leq j \leq k$.
- $\rho_{ii} = \mathrm{id}_{A_i}$ para cada $i \in I$.

Sea B la unión disjunto de los A_i, y definamos la relación $\sim$ sobre B por $a \sim b$ ssi existe un k con $i, j \leq k$ tal que $\rho_{ik}(a) = \rho_{jk}(b)$ donde $a \in A_i$, $b \in A_j$.
a) Muestre que $\sim$ es relación de equivalencia sobre B. El conjunto cociente se llama *límite directo* o *inductivo* del sistema dirigido $\{A_i\}$ y se escribe $\varinjlim A_i$. Para abreviar, denotemos $A = \varinjlim A_i$ y $\bar{x} \in A$ la clase de $x \in B$.
b) Pruebe que la proyección canónica $\rho_i : A_i \to A$ definida por $\rho_i(a) = \bar{a}$ es inyectiva si cada ρ_{ij} lo es.
c) Supongamos que cada ρ_{ij} es un morfismo de grupos. Muestre que si $a \in A_i$, $b \in B_j$ entonces la operación $\bar{a} + \bar{b} = \overline{\rho_{ik}(a) + \rho_{jk}(b)}$ (donde k es cualquier índice tal que $i, j \leq k$ está bien definida). Concluya que los mapas ρ_i son morfismos.

d) Supogamos que los A_i son anillos conmutativos con unidad y los ρ_{ij} son morfismos de anillos unitarios. Defina una estructura de anillo conmutativo con unidad sobre A de tal manera que los ρ_i sean morfismos de anillos.

e) Bajo las hipótesis de c), pruebe que el límite directo posee la siguiente propiedad universal: si C es un grupo abeliano tal que para cada $i \in I$ existe un morfismo $\psi_i : A_i \to C$ que verifica $\psi_i = \psi_j \circ \rho_{ij}$, entonces existe un único morfismo $\psi : A \to C$ tal que $\psi \circ \rho_i = \psi_i$ para cada i. Concluya que el límite directo de los $\{A_i\}$ es único salvo isomorfismo.

f) Sea I la colección de intervalos abiertos $U = (a, b)$ de la recta real que contienen a un real fijo p. Ordenemos I por inclusión reversa ($U \leq V$ ssi $V \subseteq U$) de tal manera que $(I, \leq)$ sea un conjunto dirigido. Para cada $W \in I$ sea A_W el anillo de funciones continuas en U a valores reales, y para $V \subseteq U$ definamos los mapeos de restricción $\rho_{UV} : A_U \to A_V$ por $f \mapsto f|_V$. Sea $A = \varinjlim A_U$. Muestre que los ρ_{UV} son morfismos de anillos y que los $\rho_U : U_V \to A$ son sobreyectivos y no inyectivos. A se llama el anillo de *gérmenes de funciones continuas* en p.

Ejercicio 3.21. Sean I un conjunto de índices parcialmente ordenado y A_i un grupo para cada $i \in I$. Supongamos que tenemos para cada par $i \leq j$ un mapa $\mu_{ji} : A_j \to A_i$ tal que:

- $\mu_{ji} \circ \mu_{kj} = \mu_{ki}$ cuando $i \leq j \leq k$.
- $\mu_{ii} = \mathrm{id}_{A_i}$ para cada $i \in I$.

Sea P el subconjunto de elementos $(a_i)_{i \in I}$ del producto directo $\prod_i A_i$ tales que $\mu_{ji}(a_j) = a_i$ cuando $i \leq j$. El conjunto P se llama el *límite inverso* o *proyectivo* del sistema $\{A_i\}$, y se escribe $\varprojlim A_i$. De ahora en adelante asumiremos que los μ_{ji} son morfismos de grupos.

a) Muestre que $P \leq \prod_i A_i$.

b) Supongamos que $I = \mathbb{N}$ y definamos $\mu_i : P \to A_i$ la proyección en la i-ésima componente. Muestre que cada μ_i es sobreyectiva si cada μ_{ji} lo es. Luego cada A_i es un grupo cociente de P.

c) Supongamos que los A_i son anillos conmutativos con unidad y los μ_{ji} son morfismos de anillos unitarios. Defina una estructura de anillo conmutativo con unidad sobre A de tal manera que los μ_i sean morfismos de anillos.

d) Muestre que el límite inverso posee la siguiente propiedad universal: si D es un grupo tal que para cada $i \in I$ existe un morfismo $\pi : D \to A_i$ que verifica $\pi_i = \mu_{ji} \circ \pi_j$ cuando $i \leq j$, entonces existe un único morfismo $\pi : D \to P$ tal que $\mu_i \circ \pi = \pi_i$ para cada i. Concluya que el límite directo de los A_i es único salvo isomorfismo.

e) Sean p primo, $I = \mathbb{N}$, $A_i = \mathbb{Z}/p^i\mathbb{Z}$ y sean μ_{ji} los mapeos de proyección natural $\mu_{ji} : a \mod p^j \mapsto a \mod p^i$. El límite inverso $\mathbb{Z}_p \doteq \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ se llama anillo de *enteros p-ádicos*.

   i. Muestre que cada elemento de $\mathbb{Z}_p$ se puede escribir de manera única como una suma formal infinita $b_0 + b_1 p + b_2 p^2 + \ldots$ donde cada $b_i \in \{0, 1, \ldots, p-1\}$. Concluya que $\mathbb{Z}_p$ tiene cardinal c. **Indicación:** Escriba un residuo y luego describa los mapas μ_{ji}.

   ii. Pruebe que $\mathbb{Z}_p$ es un dominio de integridad que contiene una copia de los enteros.

   iii. Pruebe que $b_0 + b_1 p + \ldots$ es una unidad en $\mathbb{Z}_p$ ssi $b_0 \neq 0$.

   iv. Pruebe que el único ideal maximal de $\mathbb{Z}_p$ es $p\mathbb{Z}$ y que $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ (donde $p = 0 + 1p + 0p^2 + 0p^3 + \ldots$). Muestre que todo ideal no trivial de $\mathbb{Z}_p$ es de la forma $p^n\mathbb{Z}_p$ con $n \in \mathbb{N}$.

v. Muestre que si $a_1 \not\equiv 0 \mod p$ entonces hay un elemento $a = (a_i) \in \mathbb{Z}_p$ que verifica $a_j^{p-1} \equiv 1 \mod p^j$ y $\mu_{j1}(a_j) = a_1$ para todo j. Deduzca que $\mathbb{Z}_p$ contiene $p-1$ raíces $(p-1)$-ésimas de la unidad distintas.

Capítulo 4

Módulos

4.1. Definiciones y ejemplos básicos

Consideremos un anillo R y $(M,+)$ un grupo abeliano y supongamos que existe una función (llamada *ponderación*) de $R\times M$ en M, denotada por yuxtaposición $(r,m)\to rm$ tal que para cada $r,r'\in R$, $m,m'\in M$ se tiene que

1. $(r+r')m = rm+r'm$.
2. $r(m+m') = rm+rm'$.
3. $r(r'm) = (rr')m$.
4. $1m = m$.

Entonces diremos que M es un *R-módulo izquierdo* o simplemente un *R-módulo*. De forma análoga, si tenemos una función de $M\times R$ en M que satisface el mismo tipo de propiedades, podemos definir *R*-módulos derechos. Esta definición extiende la idea de espacio vectorial a estructuras donde los escalares provienen de un anillo cualquiera. Podemos pensar a un módulo como una acción de R en un grupo abeliano M. Por abuso de lenguaje denotaremos al neutro aditivo de M y al neutro aditivo de R por 0.

A una suma $\sum_{i=1}^{n} r_iu_i$ donde $\{r_i\}_i\subseteq R$ y $\{u_i\}_i\subseteq M$ se llama una *combinación lineal* del conjunto $\{u_i\}_i$. Si $\{u_i\}_i\subseteq M$ es tal que el único conjunto $\{r_i\}_i\subseteq R$ que verifica

$$\sum_{i=1}^{n} r_iu_i = 0$$

es el conjunto $\{r_i\}=\{0\}$, entonces diremos que $\{u_i\}$ es *linealmente independiente*, o l.i.

Observación 4.1. Sea M un R-módulo. Entonces se cumple para cada $r\in R$, $m\in M$ que

- $r0 = 0$.
- $0m = 0$.
- $(-1)m = -m$.
- $(-r)m = -(rm) = r(-m)$.

- $(-r)(-m) = rm$.

Si R es un anillo conmutativo, una *R-álgebra* es un R-módulo M donde M es un anillo cuyo producto $\cdot$ satisface $r(m \cdot n) = (rm) \cdot n = m \cdot (rn)$ para cada $r \in R$ y $m, n \in M$.

Ejemplo 4.1.

- Si G es un grupo abeliano, podemos dotarlo de una estructura de $\mathbb{Z}$-módulo definiendo la multiplicación escalar como $(k, g) \in \mathbb{Z} \times G \mapsto kg \in G$ de la manera que lo hicimos en el capítulo 2.
- Si G es un grupo abeliano, entonces $R = \mathrm{End}(G) = \{\eta : G \to G \ \ \eta \text{ es morfismo de grupos}\}$ es un anillo con la suma $f + g : G \to G$ definida por $(f + g)(x) = f(x) + g(x)$ y como producto la composición de funciones. Entonces G es un R-módulo definiendo para cada f en R y para cada $n \in G$ el producto por escalar $fn = f(n)$. Reciprocamente si M es un D-módulo para cierto anillo D, entonces para cada $d \in D$ definimos $\mu_d : M \to M$ por $\mu_d(m) = dm$. Cada μ_d es un morfismo de grupos abelianos y además $\mu_d \circ \mu_{d'} = \mu_{dd'}$, es decir $\{\mu_d;\ d \in D\}$ es un subanillo del anillo de endomorfismos de M.
- Sea V un espacio vectorial sobre un cuerpo K y $T : V \to V$ una función lineal. Entonces podemos considerar a V como un $K[X]$-módulo: si $p(X) = \sum_{k=0}^{n} a_k X^k \in K[X]$, definimos $p(T) = \sum_{k=0}^{n} a_k T^k$ donde $T^0 = I$ la función identidad y T^k es la composición $T \circ T \circ T \cdots \circ T$ k veces, la cual es una función lineal de V en V. Luego si $p(X) \in K[X]$ y $v \in V$ definimos la multiplicación $p(X)v = p(T)(v)$, y entonces dotamos a V de una estructura de $K[X]$-módulo.
  Recíprocamente, si V es un $K[X]$-módulo entonces definiendo K como los polinomios de grado 0 unión el polinomio nulo, V satisface los axiomas de espacio vectorial sobre K. Además si consideramos la acción del polinomio X sobre V, se tiene que la función $T : V \to V$ definida por $T(v) = Xv$ verifica que $T(v+v') = X(v+v') = Xv + Xv' = T(v) + T(v')$ y además $T(kv) = X(kv) = (Xk)v = k(Xv) = kT(v)$ para cada $v, v' \in V$ y $k \in K$ y por ende T es una función lineal. Entonces $p(X)v = p(T)v$.
  Es decir, todo $K[X]$-módulo se pude considerar como V un espacio vectorial sobre K y una función lineal destacada $T : V \to V$ y donde la multiplicación escalar está definida por $p(X)v$ como $p(T)(v)$. A este módulo definido por el par (k^n, T) lo denotamos como M_T.
- Si R es un anillo y A es un subanillo de R, entonces podemos considerar R como un A-módulo considerando la multiplicación escalar como la propia multiplicación de R. En particular, cuando A y R son cuerpos tenemos que R se puede considerar como un espacio vectorial sobre A. En este caso decimos que R es una extensión del cuerpo A, y a la dimensión $\dim_A(R)$ se le llama el grado de la extensión y se anota $[R : A] = \dim_A R$. Por ejemplo $[\mathbb{C} : \mathbb{R}] = 2$, y $[\mathbb{R} : \mathbb{Q}] = \infty$.

Si M es un R-módulo y N es un subgrupo (abeliano) de $(M, +)$ que es cerrado bajo la acción de R, es decir, para cada $r \in R$ y $n \in N$ se cumple que $rn \in N$, entonces N se llama un *R-submódulo* de M. Una manera rápida de verificar que N es un submódulo de M es ver que $rn + n' \in N$ para todo $r \in R$ y $n, n' \in N$ y que $N \neq \{0\}$. Notemos que los submódulos de los espacios vectoriales son los subespacios vectoriales, y los submódulos de un anillo R (visto como un R-módulo sobre sí mismo) son los ideales de éste.

Dado un subconjunto X de un R-módulo M, definimos el *submódulo generado por X* al submódulo

$$N = \left\{ \sum_{k=0}^{n} \lambda_i u_i;\ n \in \mathbb{N},\ \lambda_i \in R \text{ y } u_i \in X \right\}$$

que corresponde al menor submódulo de M que contiene a X. Si $m \in M$ entonces $\langle\{m\}\rangle$ lo denotamos por $\langle m\rangle$ y le llamamos el submódulo generado por m, o *submódulo cíclico* generado por m. Es directo ver que $Rm = \langle m\rangle$. Si X es un conjunto finito y $\langle X\rangle = M$, entonces diremos que M es un módulo *finitamente generado* o *de tipo finito* sobre R.

Cuando M y M' son R-módulos, decimos que una función $\eta\colon M \to M'$ es un *morfismo de módulos*, o una *función R-lineal* si verifica que para cada $m, m' \in M$ y $r \in R$

1. $\eta(m+m') = \eta(m) + \eta(m')$.
2. $\eta(rm) = r\eta(m)$.

La condición 1. dice que η es un morfismo de grupos. Es claro que $\ker(\eta)$ e $\mathrm{im}(\eta)$ son submódulos de M y M' respectivamente.

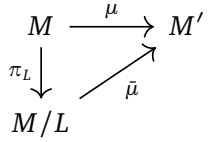
Ejemplo 4.2. Las funciones $\mathbb{Z}$-lineales entre dos grupos abelianos son simplemente los morfismos de grupos. Por otro lado, si V es un espacio vectorial sobre K y T una función lineal de V en sí mismo, las funciones $K[X]$-lineales de M_T en sí mismo son las funciones lineales (en el sentido clásico) que conmutan con T.

Observación 4.2. Si $\eta\colon M \to M'$ es un morfismo de R-módulos y si $\{\lambda_k\}_{k=1}^n \subseteq R$ y $\{u_k\}_{k=1}^n \subseteq M$ entonces

$$\eta\left(\sum_{k=1}^n \lambda_k u_k\right) = \sum_{k=1}^n \lambda_k \eta(u_k).$$

Si M es un R-módulo y N es un submódulo de M, entonces podemos definir el grupo abeliano cuociente M/N y además podemos hacer actuar R en las clases laterales de manera natural por $r(m+N) = rm+N$. Para ver que esta multiplicación escalar está bien definida, notemos que $m+N = m'+N$ quiere decir que existe $n \in N$ tal que $m' = m+n$, entonces $r(m'+N) = rm'+N = r(m+n)+N = rm+rn+N$, pero como $rn \in N$ se tiene que $r(m'+N) = r(m+N)$. Esta ponderación satisface todas las condiciones para que M/N sea un R-módulo. Se llama el *módulo cuociente* entre M y N. Definimos como siempre la proyección canónica por $\pi_N\colon M \to M/N$ por $\pi_N(m) = m+N$.

Teorema 4.1 (Teorema del factor)**.** *Sea $\mu\colon M \to M'$ una función lineal entre R-módulos y L un submódulo de M que está contenido en el kernel de μ. Entonces existe una única función lineal $\overline{\mu}\colon M/L \to M'$ tal que $\mu = \overline{\mu} \circ \pi_L$. Es decir, hay una única función $\overline{\mu}$ que hace que el siguiente diagrama conmute.*

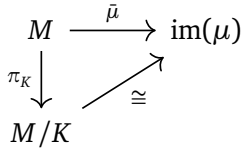


Además, $\mathrm{im}(\overline{\mu}) = \mathrm{im}(\mu)$ *y* $\ker(\overline{\mu}) = \ker(\mu)/L$.

Demostración. Idéntica a la demostración del teorema en un contexto de grupos, notando que el morfismo de grupos entregado por el teorema es también un morfismo de módulos. □

Corolario 4.1 (Primer teorema del isomorfismo)**.** *Si $\mu: M \to M'$ es R-lineal, entonces $M/\ker(\mu) \cong \text{im}(\mu)$.*

Demostración. Al considerar la función $\tilde{\mu}: M \to \text{im}(\mu)$ definida por $\tilde{\mu}(m) = \mu(m)$, que es un epimorfismo, y $L = \ker(\mu) = K$ en el teorema del factor, se tiene que $\overline{\tilde{\mu}}$ es un isomorfismo.



□

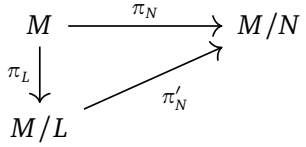
Ejemplo 4.3. Sea M un módulo sobre un anillo conmutativo R y $m \in M$. Consideremos el epimorfismo $f: R \to \langle m \rangle$ definido por $f(r) = rm$. El kernel de f es el *aniquilador* de m y se denota $\text{Ann}(m) = \{r \in R \; rm = 0\}$ y es un submódulo de R, es decir, es un ideal de R. Por el primer teorema del isomorfismo tenemos que $R/\text{Ann}(m) \cong \langle m \rangle$.

Corolario 4.2 (Segundo teorema del isomorfismo)**.** *Si N, L son submódulos de un un R-módulo M, entonces $N/(N \cap L) \cong (N + L)/L$.*

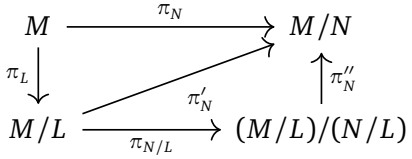
Demostración. Idéntica a la demostración del teorema en un contexto de grupos, notando que el isomorfismo de grupos considerado también es morfismo de módulos. □

Corolario 4.3 (Tercer teorema del isomorfismo)**.** *Si N, L son R—submódulos de un un R-módulo M, y $L \subseteq N$ entonces $(M/L)/(N/L) \cong M/N$.*

Demostración. Consideremos la proyección canónica $\mu_N: M \to M/N$, la cual es epiyectiva. Como $L \subseteq \ker(\mu)$ entonces existe una única función lineal π'_N tal que el diagrama conmuta:



Tal π'_N es epiyectiva pues π_N lo es. Ahora bien, el kernel de π'_N es el conjunto N/L, entonces existe un único morfismo π''_N que hace que el diagrama inferior conmute:



Como π'_N es epiyectiva, π''_N también lo es, y como $\ker(pi'_N)$ es N/L se tiene que π''_N también es inyectiva. □

Si M es un R-módulo y N, L son submódulos de M tales que $N+L=M$ y $N\cap L=\{0\}$, entonces decimos que M es la *suma directa* de N y L y anotamos $M=N\oplus L$.

Ejemplo 4.4. Consideremos la función lineal $T:\mathbb{R}^2\to\mathbb{R}^2$ definida por $T(x,y)=(x-y,x+y)$ y consideremos $\mathbb{R}^2$ como un $\mathbb{R}[X]$ módulo del modo que mostramos antes, esto es $p(X)v=p(T)v$. Por ejemplo, si $p(X)=X^2$, entonces $p(X)(1,0)=T(T(1,0))=T(1,1)=(0,2)$. Tomemos ahora $q(X)=X^2-2X+2$, luego $q(X)(1,0)=T^2(1,0)-2T(1,0)+2(1,0)=(0,2)-2(1,1)+(2,0)=(0,0)$. Es decir, existe un elemento no nulo r del anillo $R=\mathbb{R}[X]$, en nuestro caso $r=X^2-2X+2$ y un elemento no nulo $m\in M=\mathbb{R}^2$, en nuestro caso $m=(1,0)$, tal que $rm=0$. De hecho, para todo $v\in\mathbb{R}^2$ se tiene que $r(X)v=0$.

Los polinomios que aniquilan a todo $\mathbb{R}^2$ no son poco comunes: si E es un espacio vectorial sobre un cuerpo K y de dimensión $n\in\mathbb{N}$, y le damos la estructura de un $K[X]$-módulo tomando una función lineal $T:E\to E$, entonces el conjunto $S=\{T^k;\ k\in\mathbb{N}\}$ es linealmente dependiente en $L(E,E)$, el espacio vectorial de funciones lineales de E en sí mismo (pues éste tiene dimensión n^2). Una combinación lineal no trivial de elementos en S que es igual al morfismo nulo define un polinomio $p(X)\in K[X]^*$ tal que $p(X)v=0$ para todo $v\in E$.

Si M es un R-módulo y $m\in M$ es tal que existe $0\neq r\in R$ para el cual $rm=0$, entonces decimos que m es un elemento de *torsión.* Si en un módulo 0 es el único elemento de torsión, entonces M se dice *libre de torsión.* , y si los elementos de torsión son todo M diremos que M es *de torsión*. Por ejemplo, un espacio vectorial sobre un cuerpo K es libre de torsión, y en el ejemplo anterior se ve que cualquier $K[X]$-módulo (en un espacio vectorial de dimensión finita) es de torsión. El conjunto de todos los elementos de torsión de M se denota por $T(M)$ o $\mathrm{tor}(M)$. Cuando DR es un dominio, tenemos que dados $m,m'\in\mathrm{tor}(M)$ existen $r,r'\in R^*$ tal que $rm=r'm'=0$. Tomemos $q\in R$ cualquiera y definamos $d=rr'\neq 0$ (pues D es dominio) de modo que $d(qm+m')=qr'(rm)+r(r'm')=0$. Luego $\mathrm{tor}(M)$ es un submódulo de M cuando R es dominio. Es claro también que $\mu(\mathrm{tor}(M))\subseteq\mathrm{tor}(M')$ cuando $\mu:M\to M'$ es R-lineal.

Ejemplo 4.5. Si G es un grupo abeliano finito de orden $m\in\mathbb{N}$, el teorema de Lagrange asegura que $mg=0$ para cada $g\in G$, de modo que G es un $\mathbb{Z}$-módulo de torsión, y en particular lo podemos ver como un $\mathbb{Z}_m$-módulo. Si G es tal que existe un primo p que verifica $pg=0$ para todo $g\in G$, entonces de la misma manera G es un $\mathbb{Z}_p$-espacio vectorial.

Ahora veremos el análogo en módulos de la suma directa interior de grupos y la suma directa de espacios vectoriales: dados un conjunto arbitrario de índices I y para cada $i\in I$ un R-módulo M_i, definimos el *producto directo* de los M_i como el R-módulo $\prod_{i\in I}M_i$ dotado de la suma y ponderación por escalares componente a componente. Definimos también la *suma directa externa* de los M_i como

$$\bigoplus_{i\in I}M_i=\{(a_i)_{i\in I}\in\prod_{i\in I}M_i:\ a_i=0 \text{ salvo finitos índices}\}$$

dotado de las operaciones heredadas de $\prod_{i\in I}M_i$.

Igual que en el contexto de grupos, decimos que un R-módulo M es la *suma directa interna* de una familia de submódulos $\{M_i\}_{i\in I}$ si

1. El conjunto $\bigcup_{i\in I} M_i$ genera M.
2. Para cada $j \in I$ se tiene que $M_j \cap \langle \bigcup_{i\neq j} M_i \rangle = \{0\}$.

Notemos que la condición 2 es equivalente a que si $\sum_{k=1}^n x_k = 0$ con los $x_k \in M_{i_k}$, entonces cada $x_i = 0$, y esto es equivalente a su vez a que la igualdad $\sum_{k=1}^n x_k = \sum_{k=1}^n y_k$ (donde cada $x_k, y_k \in M_{i_k}$) implica que $x_k = y_k$ para cada k. Como antes, la suma directa externa e interna sólo difieren en su nombre.

Proposición 4.1. *M es la suma directa interna de los M_i ssi $M \cong \bigoplus_{i\in I} M_i$.*

Demostración. La implicancia $\Leftarrow$ es directa. Para la otra implicancia, basta notar que la función $\psi : \bigoplus_{i\in I} M_i \to M$ definida por $\psi((x_i)_{i\in I}) = \sum_{i\in I} x_i$ está bien definida (pues hay finito términos no nulos en cada $(x_i)_{i\in I}$) y es epiyectiva por la condición 1 de la definición de suma directa interna. La condición 2 muestra que también es inyectiva. □

4.2. Módulos Libres

Sea M un R-módulo. Decimos que un subconjunto $\{u_i\}_{i\in I}$ de M es una *R-base* o simplemente una *base* de M sobre R si cumple que

1. $\{u_i\}_i$ es generador de M.
2. $\{u_i\}_i$ es linealmente independiente.

Si M tiene una base de tamaño n, decimos que M es un R-módulo *libre de rango n*. Es fácil ver que para cualquier conjunto I de índices, $\bigoplus_{i\in I} R$ es un R-módulo libre con base $\{e_i\}_{i\in I}$. El siguiente teorema muestra que es el único salvo isomorfismo.

Teorema 4.2. *Si M es un R-módulo libre con base $B \subseteq M$, entonces $M \cong \bigoplus_{b\in B} R$. En particular, R^n es el único R-módulo libre de rango n salvo isomorfismo.*

Demostración. Basta notar que M es la suma directa interna de los módulos cíclicos $\{Rb\}_{b\in B}$, pues éstos generan M y además si $\sum_{k=1}^n r_k b_k = 0$ con cada $r_k \in R$, $b_k \in B$, entonces la independencia lineal muestra que $r_k = 0$ para cada k y luego $r_k b_k = 0$. Notemos que un módulo libre no puede tener elementos de torsión salvo el 0, y por lo tanto $Rb \cong R/\mathrm{Ann}(b) \cong R$, y podemos usar la proposición 4.1 para concluir. □

Proposición 4.2. *Sea R un anillo, M un R-módulo y B un subconjunto de M. Las siguientes afirmaciones son equivalentes.*

1. *B es base de M.*
2. *Para cada $m \in M$ existe un único $(r_b)_{b\in B} \in \bigoplus_{b\in B} R$ tal que $m = \sum_{b\in B} r_b b$.*
3. *Para cada R-módulo N y función $f : B \to N$, existe una única función $\bar{f} : M \to N$ tal que $\bar{f}\big|_B = f$.*

Demostración. La equivalencia $1 \equiv 2$ es directa por la proposición anterior. La implicancia $2 \Rightarrow 3$ sigue de notar que tal función $\bar{f}$ está definida por su valor en todo B (pues éste genera a M) y podemos extenderla

por linealidad a todo M (pues cada elemento en M se escribe de manera única como combinación lineal de B) para obtener una función R-lineal. La implicancia $3 \Rightarrow 2$ es un ejercicio. □

Corolario 4.4. *Todo R-módulo es isomorfo al cociente de un módulo libre.*

Demostración. Sea M un R-módulo cualquiera y tomemos $B = M$ y $F = \bigoplus_{b\in B} R$. La función $\psi : F \to M$ definida por $\psi((r_b)_b) = \sum_{b\in B} r_b b$ es un morfismo epiyectivo de módulos, y por lo tanto $M \cong F/\ker(\psi)$. Concluimos notando que F es libre. □

El siguiente teorema dice que definir rango para un módulo libre sobre un anillo conmutativo R es una buena definición, es decir, si un módulo libre sobre R tiene una base con n elementos y otra base con m elementos, entonces $n = m$.

Teorema 4.3. *Si R es un anillo conmutativo y M es un R-módulo libre donde $B = \{x_1, x_2, x_3, \ldots, x_n\}$ y $C = \{y_1, y_2, y_3, \ldots, y_m\}$ son R-bases de M, entonces $n = m$.*

Antes de dar la demostración del teorema, necesitaremos algunos resultados de matrices. Si R es un anillo cualquiera, entonces $M_{n\times m}(R)$ denota el R-módulo de todas las matrices de $n \times m$ donde la poneración es el escalamiento habitual de una matriz, esto es $r(a_{ij}) = (ra_{ij})$. Si $A = (f_{ij}) \in M_{p\times n}$ y $C = (c_{ij}) \in M_{n\times q}$, entonces la matrix $P = (p_{ij}) \in M_{p\times q}$ se define como aquella matriz que en su entrada ij tiene el valor

$$p_{ij} = \sum_{k=1}^{n} f_{ik}c_{kj}.$$

Esa multiplicación satisface $A(B+cC) = AB+cAC$ si $A \in M_{p\times n}$ y $B, C \in M_{n\times q}$. También se cumple $(A+cB)C = AC + cBC$ si $A, B \in M_{p\times n}$ y $C \in M_{n\times q}$. En el caso $n = m$, escribimos $M_{n\times n} = M_n(R)$ y resulta que es una R-álgebra con el producto matricial recién definido. $M_n(R)$ también es un anillo cuyo neutro multiplicativo es la matriz identidad I_n, aquella que tiene 1 en cada posición de la diagonal y todos los otros coeficientes son cero. Si $A = (a_{ij}) \in M_{n\times m}$ e $i \in [n]$ entonces la i-ésima fila de A lo podemos considerar como un vector $(a_{i1}, a_{i2}, \cdots, a_{im}) \in R^m$.

Sea R conmutativo. Una función $d : M_n(R) \to R$ se dice *multilineal* si es lineal en cada fila y *alternada* si cuando A tiene dos filas iguales, entonces $d(A) = 0$. Dada $\sigma \in \Sigma_n$ y $A \in M_n(R)$, definimos la matriz A_σ como la matriz cuya i-ésima fila es la fila $\sigma(i)$-ésima de A.

Proposición 4.3. *Sea $d : M_n(R) \to R$ multilineal alternada, $A \in M_n(A)$ y $\tau \in \Sigma_n$ una transposición. Entonces $d(A) = -d(A_\tau)$.*

Demostración. Consideremos la matriz C que tiene las mismas filas que A, salvo que la fila i y la fila j son reemplazadas por la suma de la fila i con la fila j. Entonces C tiene dos filas iguales de manera que $d(C) = 0$, pero por multilinealidad se tiene que

$$d(C) = d(A_1) + d(A_2) + d(A) + d(A_\tau)$$

donde A_1 tiene las mismas filas que A salvo que en la fila j tiene a la fila i, y la matriz A_2 tiene las mismas filas que A salvo que en la fila i tiene a la fila j. Luego $d(A_1) = d(A_2) = 0$, y

$$0 = d(C) = d(A_1) + d(A_2) + d(A) + d(B) = d(A) + d(A_\tau).$$

□

Observación 4.3. Recíprocamente, si R es un anillo conmutativo de característica distinta de 2 y $d : M_n(R) \to R$ es multilineal tal que cuando $A \in M_n(R)$ y $\tau \in \Sigma_n$ es una transposición se tiene que $d(A_\tau) = -d(A)$ entonces d es alternada.

Como toda permutación es un producto de transposiciones, deducimos el siguiente corolario.

Corolario 4.5. *Sea $d : M_n(R) \to R$ multilineal alternada, $A \in M_n(A)$ y $\sigma \in \Sigma_n$. Entonces $d(A_\sigma) = \operatorname{sgn}(\sigma) d(A)$.*

El siguiente teorema define la función determinante.

Teorema 4.4. *Existe una única función $d : M_n(R) \to R$ que es multilineal alternada y tal que $d(I_n) = 1$.*

Demostración. Denotemos por $A = (f_1, f_2, \ldots, f_n)$ la matriz cuya $i-$ésima fila es $f_i \in R^n$.Con esta notación la matriz identidad es $(e_1, e_2, \ldots e_n)$, donde $\{e_i\}$ es la base canónica de R^n. Volviendo a A tenemos que $f_i = a_{i1}e_1 + a_{i2}e_2 + \cdots + a_{in}e_n$, para ciertos $a_{ij} \in R$. Si d es mutilineal alternada, entonces al aplicar d a A y usar la multilinealidad se obtiene

$$d(A) = \sum_{f \in [n]^{[n]}} a_{1f(1)} a_{2f(2)} \cdots a_{nf(n)} d(e_{f(1)} e_{f(2)} \cdots e_{f(n)})$$

donde f recorre el conjunto de las funciones de $[n]$ en sí mismo. Pero $d(e_{f(1)} e_{f(2)} \cdots e_{f(n)}) = 0$, si $f(i) = f(j)$ con $i \neq j$, entonces

$$d(A) = \sum_{\sigma \in \Sigma_n} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} d(e_{\sigma(1)} e_{\sigma(2)} \cdots e_{\sigma(n)})$$

pero por el corolario anterior

$$d(A) = \sum_{\sigma \in \Sigma_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} d(e_1 e_2 \cdots e_3).$$

Entonces si tal función del teorema existe, necesariamente queda definida por la ecuación anterior.

Verifiquemos que nuestra función d satisface las condiciones del teorema. Primero notemos que escribiendo $I_n = (a_{i,j})_{i,j \in [n]}$ tenemos que si $\sigma_\in \Sigma_n$ es tal que $\sigma(k) \neq k$ para algún valor de $k \in [n]$, entonces $a_{k\sigma(k)} = 0$ y por lo tanto $a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} = 0$. Luego el único sumando no nulo es $a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} = 1$ cuando $\sigma = (1)$, y sigue que $d(I_n) = 1$.

Veamos que es multilineal: sea $A \in M_n(R)$ tal que su i-ésima fila es

$$(x_{i1}, x_{i2}, \ldots, x_{in}) + c(y_{i1}, y_{i2}, \ldots, y_{i1})$$

y las otras filas de A son $(x_{j1}, x_{j2}, \ldots, x_{jn})$. Entonces

$$\begin{aligned} d(A) &= \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma) x_{1\sigma(1)} x_{2\sigma(2)} \cdots (x_{i\sigma(i)} + c y_{i\sigma(i)}) \cdots a_{n\sigma(n)} \\ &= \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma) x_{1\sigma(1)} x_{2\sigma(2)} \cdots (x_{i\sigma(i)}) \cdots a_{n\sigma(n)} \\ &\quad + \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma) x_{1\sigma(1)} x_{2\sigma(2)} \cdots (c y_{i\sigma(i)}) \cdots a_{n\sigma(n)} \\ &= \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma) x_{1\sigma(1)} x_{2\sigma(2)} \cdots x_{i\sigma(i)} \cdots a_{n\sigma(n)} \\ &\quad + c \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma) x_{1\sigma(1)} x_{2\sigma(2)} \cdots y_{i\sigma(i)} \cdots a_{n\sigma(n)} \\ &= d(B) + c d(C) \end{aligned}$$

donde B tiene las mismas filas de A, salvo que en la fila i tiene al vector $(x_{i1}, x_{i2}, \ldots, x_{in})$ y la matriz C tiene las mismas filas que A salvo que en la fila i tiene al vector $(y_{i1}, y_{i2}, \ldots, y_{in})$. Por lo tanto d es multilineal.

Ahora bien, supongamos que $n \geq 2$ (el teorema en el caso $n = 1$ es directo) y consideremos la permutación $\tau = (12) \in \Sigma_n$. Observemos que si $k \geq 3$, entonces $\sigma(k) = \sigma\tau(k)$ y que si σ recorre todo Σ_n, entonces también lo hace $\sigma\tau$. Luego si $A \in M_n(R)$ es arbitraria, tenemos que

$$\begin{aligned} d(A_\tau) &= \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma\tau) a_{1\sigma\tau(1)} a_{2\sigma\tau(2)} a_{3\sigma\tau(3)} \cdots a_{n\sigma\tau(n)} \\ &= \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma\tau) a_{1\sigma(2)} a_{2\sigma(1)} a_{3\sigma(3)} \cdots a_{n\sigma(n)} \\ &= \sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma)(-1) a_{2\sigma(1)} a_{1\sigma(2)} a_{3\sigma(3)} \cdots a_{n\sigma(n)} \\ &= -\sum_{\sigma\in\Sigma_n} \operatorname{sgn}(\sigma) a_{2\sigma(1)} a_{1\sigma(2)} a_{3\sigma(3)} \cdots a_{n\sigma(n)} \\ &= -d(A). \end{aligned}$$

Entonces si permutamos las dos primeras filas de una matriz, la función d cambia el signo. La demostración para el caso $\tau = (ij)$ es idéntica a la anterior. Por lo tanto d es la única función multilineal alternada de $M_n(R)$ a R tal que $d(I_n) = 1$. □

A tal función se le llama el *determinante* y como hemos visto, es la única multilineal alternada que tal que $d(I_n) = 1$. La denotaremos por $\det(A)$.

Observación 4.4. Si D es una matriz diagonal de $M_n(R)$, es decir si $D = (d_{ij})$, entonces la fila i-ésima de D es $d_{ii}e_i$ donde e_i es el $i-$ésimo vector de la base canónica, y como det es multilineal, se tiene que

$$\det(D) = \Pi_{i=1}^{n} d_{ii} \det(I_n) = \Pi_{i=1}^{n} d_{ii}.$$

En particular, si en una matriz diagonal D existe $d_{ii} = 0$ para algún $i \in [n]$ se tiene que $\det(D) = 0$.

Proposición 4.4. *Toda función multilineal alternada $d : M_n(R) \to R$ es un múltiplo escalar del determinante.*

Demostración. La demostración anterior prueba que cualquier función multilineal alternada $d : M_n(R) \to R$ está totalmente determinada por su acción en la base canónica, es decir, en $d(e_1, e_2, \ldots, e_n)$. De hecho cualquier función multilineal alternada es de la forma

$$d(A) = \sum_{\sigma \in \Sigma_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} a_{3\sigma(3)} \cdots a_{n\sigma(n)} d(e_1, e_2, e_3, \ldots, e_n).$$

Escribiendo a $d(e_1, e_2, e_3, \ldots, e_n) = r$, tenemos que

$$d(A) = r \sum_{\sigma \in \Sigma_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} a_{3\sigma(3)} \cdots a_{n\sigma(n)} = r \det(A).$$

□

Teorema 4.5. *Si $A, B \in M_n(R)$ entonces* $\det(BA) = \det(B)\det(A)$.

Demostración. Probemos primero que la función $X \in M_n(R) \mapsto d(X) = \det(XA) \in R$ es multilineal alternada: sea $A \in M_n(R)$ y notemos que si B tiene en la fila i al vector $(x_{i1}, x_{i2}, \ldots, x_{in}) + c(y_{i1}, y_{i2}, \ldots, y_{in})$ y en la fila $j \neq i$ al vector $(x_{j1}, x_{i2}, \ldots, x_{jn})$ entonces

$$d(B) = \det(BA) = \det((B_1 + cB_2)A) = \det(B_1A) + c\det(B_2A).$$

donde B_1 es la matriz que tiene las mismas filas que B salvo que en la fila i tiene al vector $(x_{i1}, x_{i2}, \ldots, x_{in})$ y la matriz B_2 tiene las mismas filas que B salvo que en la fila i tiene al vector $(y_{i1}, y_{i2}, \ldots, y_{in})$, Por lo tanto d es una función multilineal.

Por otra parte, consideremos la matriz $B = (b_{ij})$ y la matriz $BA = (c_{ij})$ donde el coeficiente c_{ij} es $\sum_{k=1}^{n} b_{ik}a_{ki}$. Entonces la fila 1 de BA es $\sum_{k=1}^{n} b_{1k}a_{k1}$ que corresponde a la fila 2 de $B_{(12)}A$, y la fila 2 de BA es la fila 1 de $B_{(12)}A$. El resto de las filas de BA y de $B_{(12)}A$ coinciden. Por lo tanto BA y $B_{12}A$ son iguales salvo que las filas 1 y 2 están permutadas y entonces

$$d(B_{12}) = \det(B_{12}A) = -\det(BA) = d(B).$$

Luego d es multilineal alternada.

Por lo tanto existe $r \in R$ tal que $d(X) = r\det(X)$ entonces evaluando en $X = I_n$ se tiene que

$$d(I_n) = \det(A) = r\det(I_n) = r$$

y por lo tanto $r = \det(A)$. Concluimos que

$$\det(BA) = d(B) = r\det(B) = \det(A)\det(B) = \det(B)\det(A).$$

□

Corolario 4.6. *Si $A, B \in M_n(R)$, entonces* $\det(AB) = \det(BA)$.

Ahora, estamos en condiciones de demostrar el Teorema 4.3.

Demostración. Supondremos que $m \neq n$ y sin restricción supondremos que $m < n$. Cada elemento de B se escribe como combinación lineal de C y viceversa, es decir

$$x_j = \sum_{i=1}^{m} b_{ij} y_i, \quad \forall j \in [n],$$

$$y_s = \sum_{r=1}^{n} c_{rs} x_r, \quad \forall r \in [m].$$

Reemplazando se tiene

$$x_j = \sum_{i=1}^{m}\sum_{k=1}^{n} b_{ij} c_{ki} x_k,$$

$$y_s = \sum_{r=1}^{m}\sum_{t=1}^{n} c_{rs} b_{tr} y_t.$$

Como B y C son bases, tenemos que la única combinación lineal de elementos de B que produce a $x_i = \sum_{k=0}^{n} \lambda_i x_i$ es $\lambda_j = 0$ si $j \neq i$ y $\lambda_i = 1$, y lo mismo ocurre con los elementos de C. Entonces

$$\sum_{i=1}^{m} b_{ij} c_{ki} = \sum_{i=1}^{m} c_{ki} b_{ij} = \delta_{kj}, \tag{4.1}$$

$$\sum_{r=1}^{n} c_{rs} b_{tr} = \sum_{r=1}^{m} b_{tr} c_{rs} = \delta_{ts}. \tag{4.2}$$

Definamos las matrices B y C en $M_n(R)$ por

$$B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

$$C = \begin{pmatrix} c_{11} & \cdots & c_{1m} & 0 & \cdots & 0 \\ c_{21} & \cdots & c_{2m} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{n1} & \cdots & c_{nm} & 0 & \cdots & 0 \end{pmatrix}.$$

Las ecuaciones 4.1 y 4.2 se pueden escribir como

$$BC = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} = I_n,$$

$$CB = \begin{pmatrix} I_m & 0_{m\times(n-m)} \\ 0_{(n-m)\times m} & 0_{(n-m)\times(n-m)} \end{pmatrix}.$$

Por lo tanto $\det(BC) = 1$ y $\det(CB) = 0$ (por la observación 4.4) y como $\det(BC) = \det(CB)$ obtenemos una contradicción. Concluimos que $n = m$. □

Observación 4.5. Una demostración más corta de lo anterior es como sigue: sea R un anillo conmutativo y $n, m \in \mathbb{N}$ tal que $R^n \cong R^m$ como R-módulos. Sea $M \in M_{m\times n}(R)$ la matriz que representa el isomorfismo η que lleva a R^n en R^m, y $N \in M_{n\times m}(R)$ la matriz asociada a η^{-1}, de manera que $MN = \mathrm{id}_{R^m}$ y $NM = \mathrm{id}_{R^n}$. Reduciendo los coeficientes de M y N módulo I, un ideal maximal de R, obtenemos dos matrices $M \in M_{m\times n}(R/I)$ y $N \in M_{n\times m}(R/I)$ que cumplen las mismas ecuaciones que M y N. Como R/I es un cuerpo, la teoría usual de la dimensión muestra que $n = m$.

4.3. Módulos finitamente generados sobre un DIP

En esta sección estudiaremos los módulos finitamente generados sobre un DIP con el fin de demostrar teoremas profundos sobre grupos abelianos finitamente generados (es decir, los $\mathbb{Z}$-módulos finitamente generados) y sobre la forma canónica de Jordan una transformación lineal T de un espacio vectorial de dimensión finita en sí mismo.

Teorema 4.6. *Sea D un DIP y D^n el módulo libre de rango n. Entonces todo submódulo N de D^n es libre y de rango m con $m \leq n$.*

Demostración. Si $N = \{0\}$ no hay nada que probar. Supondremos entonces que $N \neq \{0\}$.

Haremos inducción en n. Si $n = 1$, entonces todo submódulo N de $D^1 = D$ es un ideal de D. Como D es un DIP existe $d \in D^*$ tal que $N = (d) \neq \{0\}$. Por definición d genera N, y si $\lambda d = 0$ entonces $\lambda = 0$ pues D es dominio. Luego $\{d\}$ es una base de N sobre D, por lo tanto N es un submódulo libre de rango 1.

Supongamos que el resultado es cierto para D^k con $k < n$ y consideremos en D^n un submódulo N. Consideremos además el submódulo K de D^n generado por $\{e_2, \ldots, e_n\}$. K es un módulo libre con $\{e_2, \ldots, e_n\}$ como base, y por el Teorema 4.2 $K \cong D^{n-1}$. Si $N \subseteq K$ concluimos por hipótesis inductiva. Basta entonces ver el caso $N \not\subseteq K$.

Si $N \not\subseteq K$, sea $I = \{d \in D \,;\, de_1 + y \in N \text{ para cierto } y \in K\}$. Como $0 \in N \cap K$ tenemos que $0e_1 + 0 \in N$ y por lo tanto $0 \in I$. Si $d_1e_1 + y_1 \in N$ y $d_2e_1 + y_2 \in N$ con $y_1, y_2 \in K$, entonces

$$d_1e + y_1 + d_2e_1 + y_2 = (d_1 + d_2)e_1 + (y_1 + y_2) \in N.$$

Como K es submódulo, $y_1 + y_2 \in K$ y por lo tanto, $d_1 + d_2 \in I$. Además, si $r \in D$, entonces $rde_1 + ry \in N$ y $ry \in K$. Por lo tanto, I es ideal de D. Como todo elemento de D^n es de la forma $de_1 + y$ con $y \in K$ y existe $x \in N$ tal que $x \notin K$, entonces también existe $d \in D$ no nulo e $y \in K$ tal que $x = de_1 + y$, en particular $I \neq \{0\}$. Como D es un DIP e I es no trivial, existe $c \in D$ no nulo tal que $I = (c)$. Sea $f_1 = ce_1 + y_1 \in N$ con $y_1 \in K$ y sea $L = K \cap N$, que es submódulo de K. Por hipótesis inductiva, L es submódulo libre de K con base $\{v_1, v_2, \ldots, v_s\}$ donde $s \leq n-1$.

Afirmamos que $\{f_1, v_1, v_2, \ldots, v_s\}$ es base de N. En efecto, sea $x \in N$. Luego existe $b \in I$ e $y \in K$ tal que $x = be_1 + y$. Como $b \in I = (c)$, podemos escribir $b = k_1c$ para cierto $k_1 \in D$. Entonces

$$\begin{aligned} x &= k_1ce_1 + y \\ &= k_1(ce_1 + y_1) - k_1y_1 + y \\ &= k_1f_1 + (y - k_1y_1) \end{aligned}$$

y notando que $y_1, y \in K$ tenemos que $y - k_1y_1 \in K$. Por otra parte, $x - k_1f_1 \in N$ pues x y k_1f_1 están en N. Como $x - k_1f_1 = y - k_1y_1$, deducimos que $y - k_1y_1 \in N$ y en consecuencia, $y - k_1y_1 \in N \cap K$. Por lo tanto, existen $\lambda_1, \lambda_2, \ldots, \lambda_s \in D$ tales que

$$y - k_1y_1 = \lambda_1v_1 + \lambda_2v_2 + \cdots + \lambda_sv_s$$

y remplazando,

$$x = k_1f_1 + \lambda_1v_1 + \lambda_2v_2 + \cdots + \lambda_sv_s.$$

Entonces todo elemento de N es combinación lineal de elementos de $\{f_1, v_1, \ldots, v_s\}$.

Supongamos ahora que

$$k_1f_1 + \lambda_1v_1 + \cdots + \lambda_sv_s = 0 \qquad (*)$$

Esto equivale a

$$k_1 c e_1 + k_1 y_1 + \lambda_1 v_1 + \cdots + \lambda_s v_s = 0,$$

y notando que $k_1 y_1 + \lambda_1 v_1 + \cdots + \lambda_s v_s \in K$ podemos escribirlo en la base $\{e_2, \cdots, e_n\}$, es decir, existen $\eta_2, \eta_3, \ldots, \eta_n \in D$ tales que

$$k_1 y_1 + \lambda_1 v_1 + \cdots + \lambda_s v_s = \eta_2 e_2 + \eta_3 e_3 + \cdots \eta_n e_n.$$

Por lo tanto,

$$k_1 c e_1 + \eta_2 e_2 + \eta_3 e_3 + \cdots + \eta_n e_n = 0$$

y ya que $\{e_2, \cdots, e_n\}$ es base, $\eta_i = 0 = k_1 c$ para cada i. Como $c \neq 0$ y D es dominio, entonces $k_1 = 0$. Reemplazando en $(*)$, obtenemos que

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_s v_s = 0$$

y concluimos que $\lambda_i = 0$ para cada $i = 2, \ldots, s$ pues $\{v_1, \ldots, v_n\}$ es base de L. Luego $\{f_1, v_1, \ldots, v_s\}$ es l.i. y por ende es una base de N de tamaño $s+1$. Como $s \leq n-1$, entonces $s+1 \leq n$ y concluimos el teorema. □

Lema 4.1. *Si M es libre de rango m y N es libre de rango n sobre un dominio R, entonces $M \oplus N$ es un módulo libre de rango $m+n$.*

Demostración. Sea $\{x_1, x_2, \ldots, x_m\}$ base de M y $\{y_1, y_2, \ldots, y_n\}$ base de N. Afirmamos que

$$\{(x_1, 0), (x_2, 0), \ldots, (x_m, 0), (0, y_1), (0, y_2), \ldots, (0, y_n)\}$$

es base de $M \oplus N$: en efecto, sea $(x, y) \in M \oplus N$. Entonces

$$(x, y) = \left(\sum_{i=1}^{m} \alpha_i x_i, \sum_{j=1}^{n} \beta_i y_i \right) = \sum_{i=1}^{m} \alpha_i (x_i, 0) + \sum_{j=1}^{n} \beta_i (0, y_i).$$

Supongamos que $\sum_{i=1}^{m} \lambda_i (x_i, 0) + \sum_{j=1}^{n} \eta_j (0, y_i) = 0$, y examinando la igualdad por componentes vemos que

$$\sum_{i=1}^{m} \lambda_i x_i = 0 \quad \text{y} \quad \sum_{j=1}^{n} \eta_j y_j = 0$$

y por lo tanto $\lambda_i = 0, \eta_j = 0$ para cada $i \in [m]$, $j \in [n]$. □

Teorema 4.1. Sea R un DIP, M un R-módulo libre de rango n y $N \neq \{0\}$ un submódulo de M. Entonces existe una base $\{y_1, \ldots, y_n\}$ de M tal que $\{a_1 y_1, a_2 y_2, \ldots, a_m y_m\}$ es base de N para ciertos $a_i \in R \setminus \{0\}$ que verifican $a_i | a_j$ si $i \leq j$.

Demostración. Sea $N \subseteq M$ un R-submódulo y $\phi : M \to R$ un morfismo de módulos. Entonces $\phi(N)$ es un submódulo de R visto como un R-módulo, es decir, $\phi(N)$ es un ideal de R. Como R es un DIP, se tiene que $\phi(N) = (a_\phi)$ para cierto $a_\phi \in R$. Definamos entonces $\Omega = \{(a_\phi)\,;\ \phi : M \to R \quad R\text{-lineal}\}$. Notemos que $\{0\} \in \Omega$ (pues corresponde al morfismo nulo) y por lo tanto Ω es no vacío. Por otra parte, la proyección

$$\begin{array}{rccc} \pi_i : & M & \to & R \\ & \sum_{j=1}^n \alpha_j x_j & \mapsto & \alpha_i \end{array}$$

donde $\{x_i\}_{i=1}^n$ es base de M, es un R-morfismo de módulos. Como $N \neq \{0\}$, existe $i \in [n]$ tal que $\pi_i(N) \neq 0$ y entonces existen elementos distintos de $\{0\}$ en Ω.

Si $(a_{\phi_1}) \subseteq (a_{\phi_2}) \subseteq \cdots (a_{\phi_n}) \subseteq (a_{\phi_{n+1}}) \subseteq \cdots$ es una cadena ascendente de ideales principales de Ω, el Teorema asegura que esta cadena es estacionaria y por lo tanto existe $n \in \mathbb{N}$ tal que $(a_{\phi_n}) = (a_{\phi_{n+k}})$ para todo $k \geq 0$, de manera que (a_{ϕ_n}) es cota superior de la cadena. El lema de Zorn muestra la existencia de un elemento maximal de Ω. Denotemos $(a_\phi) = (a_1)$ a tal elemento, es decir, $(a_\phi) = (a_1) = \phi(N)$. Como $a_1 \in \phi(N)$, entonces tenemos que existe $y \in N$ tal que $a_1 = \phi(y)$, y como (a_1) es maximal y Ω tiene elementos distintos de (0), deducimos que $a_1 \neq 0$ y también $y \neq 0$.

Sea $\eta : M \to R$ un morfismo de módulos cualquiera y sea $(d) = (a_1, \eta(y))$. Notemos que $a_1, \eta(y) \in (d)$ y por lo tanto $d | a_1, \eta(y)$ y además $d = r_1 a_1 + r_2 \eta(y)$ para ciertos $r_1, r_2 \in R$. Definamos el morfismo $\mu : M \to R$ por $\mu = r_1\phi + r_2\eta$. Se tiene que

$$\mu(y) = r_1\phi(y) + r_2\eta(y) = r_1 a_1 + r_2\eta(y) = d$$

de modo que $d \in \mu(N)$ y entonces $(d) \subseteq \mu(N)$. Como $(a_1) \subseteq (d) \subseteq \mu(N)$ y (a_1) es maximal en Ω, se tiene que $(a_1) = (d) = \mu(N)$. Por lo tanto a_1 es asociado a d y como $d | \eta(y)$, sigue que $a_1 | \eta(y)$. Es decir, para toda $\eta : M \to R$ R-lineal, a_1 divide a $\eta(y)$. En particular, $a_1 | \pi_i(y)$ para todo $i \in [n]$. Es decir, para cada i existe $b_i \in R$ tal que $a_1 b_i = \pi_i(y)$ y entonces podemos escribir $y = a_1 b_1 x_1 + a_1 b_2 x_2 + \cdots + a_1 b_n x_n$.

Sea $y_1 = \sum_{i=1}^n b_i x_i$, de modo que $a_1 y_1 = \sum_{i=1}^n a_1 b_i x_i = y$. Pero $a_1 = \phi(y) = \phi(a_1 y_1) = a_1\phi(y_1)$ y como $a_1 \neq 0$ y R es dominio, obtenemos que $\phi(y_1) = 1$. Afirmamos que $M = Ry_1 \oplus \ker(\phi)$: en efecto, si $x \in M$ podemos escribir $x = \phi(x)y_1 + (x - \phi(x)y_1)$ y calculamos

$$\phi(x - \phi(x)y_1) = \phi(x) - \phi(x)\phi(y_1) = \phi(x)(1 - \phi(y_1)) = 0.$$

Por lo tanto $x - \phi(x)y_1 \in \ker(\phi)$ y $\phi(x)y_1 \in Ry_1$, es decir $M = Ry_1 + \ker(\phi)$. Ahora si $x \in Ry_1 \cap \ker(\phi)$, entonces existe $r \in R$ tal que $x = ry_1$ y $\phi(ry_1) = 0 = r\phi(y_1) = r$ de manera que $x = 0$. Concluimos que efectivamente $M = Ry_1 \oplus \ker(\phi)$.

Afirmamos también que $N = Ra_1 y_1 \oplus (N \cap \ker(\phi))$: en efecto, cuando $x \in N$ podemos descomponer $x = \phi(x)y_1 + (x - \phi(x)y_1)$. Como $x \in N$ y $\phi : M \to R$ es morfismo, $\phi(x) \in \phi(N) = (a_1)$ y luego $\phi(x) = b_x a_1$ para algún $b_x \in R$. Por lo tanto,

$$\phi(x)y_1 = b_x a_1 y_1 = b_x y \in Ry \subseteq N,$$

de donde sigue que $x - \phi(x)y_1 \in N \cap \ker(\phi)$ (pues $\phi(y_1) = 1$). Entonces

$$N = Ry + \ker(\phi) \cap N = Ra_1 y_1 + (\ker(\phi) \cap N).$$

Por otra parte, si $ra_1y_1 = x \in Ra_1y_1 \cap N \cap \ker(\phi)$, entonces $\phi(ra_1y_1) = 0 = ra_1\phi(y_1) = ra_1$. Por lo tanto, $ra_1 = 0$. Como $a_1 \neq 0$ y R es dominio, $r = 0$. Luego $x = 0$ y sigue que $N = Ra_1y_1 \oplus (N \cap \ker(\phi))$.

Ahora como $\phi(y_1) = 1$, se tiene que $\phi(ry_1) = r$ para todo $r \in R$. Por lo tanto, la función

$$\begin{array}{rccc} \phi|_{Ry_1}: & Ry_1 & \to & R \\ & ry_1 & \mapsto & r \end{array}$$

es un isomorfismo. Entonces $ry_1 \neq 0$ para cada r no nulo, de modo que Ry_1 tiene a $\{y_1\}$ como base. Luego podemos escribir $M = Ry_1 \oplus \ker(\phi)$, y si M tiene rango n entonces el rango de $\ker(\phi)$ es $n-1$. Hagamos inducción en n: si $n = 1$, entonces $M = Ry_1$ y entonces cualquier submódulo tiene rango 1 o 0, es decir $N = Rz$ para cierto $z \in N$ o bien $N = \{0\}$, pero estamos suponiendo $N \neq \{0\}$. Notando que $a_1y_1 \neq 0$ obtenemos que $N = Ra_1y_1$ por la descomposición del párrafo anterior.

Si el resultado es cierto para todo M con $\text{rango}(M) \leq n-1$, entonces $M = Ry_1 \oplus \ker(\phi)$ donde $\ker(\phi)$ tiene rango $n-1$. Por la hipótesis inductiva, $\ker(\phi)$ tiene una base $\{y_2, \ldots, y_n\}$ tal que $\ker(\phi) \cap N$ es un submódulo de $\ker(\phi)$ con base $\{b_2y_2, \ldots, b_my_m\}$, donde $m \leq n$ y $b_2|b_3|b_4|\cdots|b_m$. Como la suma es directa, $\{y_1, \ldots, y_n\}$ es base de M y $\{a_1y_1, b_2y_2, \ldots, b_my_m\}$ es base de N. Definamos el morfismo

$$\begin{array}{rccc} \Psi: & M & \to & R \\ & \sum_{i=1}^n \alpha_i y_i & \mapsto & \alpha_1 + \alpha_2 \end{array}$$

Notemos que $\Psi(a_1y_1) = a_1 \in \Psi(N)$. Por maximalidad de a_1 en Ω se tiene que $(a_1) = \Psi(N)$, por lo tanto $\Psi(b_2y_2) \in \Psi(N) = (a_1)$ y por ende $a_1|\Psi(b_2y_2) = b_2$. Luego la inducción está completa. □

Pese a que el resultado anterior usa el axioma de elección y resulta fundamental en la demostración del próximo teorema, los corolarios mencionados al principio del capítulo (sobre grupos abelianos finitamente generados y formas de Jordan de funciones lineales en espacios vectoriales de dimensión finita) se pueden probar de manera elemental, es decir, sin recurrir al lema de Zorn.

Teorema 4.2 (Teorema fundamental de descomposición de módulos finitamente generados sobre un DIP)**.** Sea R un DIP y M un R-módulo finitamente generado. Entonces

1. M es isomorfo a una suma directa de módulos cíclicos. Más precisamente,

   $$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

   para algún entero $r \geq 0$ y elementos no nulos $a_1, a_2, \ldots, a_m \in R$, que no son unidades y satisfacen $a_1|a_2|a_3|\cdots|a_m$.
2. M es libre de torsión ssi M es libre.
3. En la descomposición en módulos cíclicos que da 1., se cumple que

   $$\text{tor}(M) \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

   En particular, M es de torsión ssi $r = 0$, y en este caso $(a_m) = \text{Ann}(M)$.

Demostración. Demostramos la parte 1, pues las partes 2 y 3 siguen fácilmente de ésta (notando que el aniquilador del R-módulo $R/(b)$ es exactamente (b)). Sea

$$n = \text{mín}\{|A|;\ A \text{ es conjunto generador de } M\}$$

y sea $\{x_1, \ldots, x_n\}$ un conjunto generador de ese cardinal. Definamos el morfismo epiyectivo

$$\begin{array}{rccc} \pi: & R^n & \to & M \\ & (a_1, \ldots, a_n) & \mapsto & \sum_{i=1}^n \alpha_i x_i \end{array}$$

de manera que $R^n/\ker(\pi) \cong M$ y $\ker(\pi)$ es un submódulo de R^n. El Teorema 4.1 asegura la existencia de una base $\{y_1, \ldots, y_n\}$ de R^n tal que $\ker(\pi)$ tiene base $\{a_1 y_1, \ldots, a_m y_m\}$ con $m \leq n$ y $a_1 | a_2 | \cdots | a_m$. Por lo tanto,

$$M \cong (Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n)/(Ra_1 y_1 \oplus Ra_2 y_2 \oplus \cdots Ra_m y_m).$$

Definamos ahora el morfismo

$$\begin{array}{rccc} \eta: & Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n & \to & R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m} \\ & r_1 y_1 + r_2 y_2 + \cdots + r_n y_n & \mapsto & (r_1 + (a_1), r_2 + (a_2), \ldots, r_m + (a_m), r_{m+1}, \ldots, r_n) \end{array}$$

y notemos que

$$\begin{aligned} \ker(\eta) &= \{r_1 y_1 + \cdots + r_n y_n;\ r_1 \in (a_1), r_2 \in (a_2), \ldots, r_m \in (a_m), r_{m+1} = 0, \ldots, r_m = 0\} \\ &= Ra_1 y_1 \oplus Ra_2 y_2 \oplus \cdots \oplus Ra_m y_m. \end{aligned}$$

Luego

$$(Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n)/(Ra_1 y_1 \oplus Ra_2 y_2 \oplus \cdots \oplus Ra_m y_m) \cong R^{n-m} \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m).$$

Si a es unidad se cumple que $R/(a) \cong \{0\}$. Entonces podemos sacar esos cuocientes del módulo $R^{n-m} \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$ y considerar sólo aquellos a_i que no son unidades. Esto termina la demostración. □

Los a_i del teorema anterior se llaman *factores invariantes* de M.

Observación Sea $a \in R$, R un DIP. Entonces como R es un DFU, existen $p_1, \ldots, p_r$ primos tales que $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ con $\alpha_i \in \mathbf{N}$, $\alpha_i \neq 0$. Entonces la función

$$\begin{array}{rccc} \eta: & R/(a) & \to & R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_r^{\alpha_r}) \\ & x + (a) & \mapsto & (x + (p_1^{\alpha_1}), x + (p_2^{\alpha_2}), \ldots, x + (p_r^{\alpha_r})) \end{array}$$

es un isomorfismo por el Teorema del Resto Chino.

Teorema 4.3 (Teorema fundamental de descomposición de módulos finitamente generados sobre un DIP: segunda versión)**.** Sea R un DIP y sea M un R-módulo finitamente generado. Entonces M es isomorfo a un módulo de la forma

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_r^{\alpha_r})$$

donde $r \geq 0$ y $p_i^{\alpha_i}$ son potencias positivas de elementos primos de R.

Demostración. Resultado inmediato del teorema anterior y la observación anterior. □

Las potencias $p_i^{\alpha_i}$ del teorema anterior se llaman *divisores elementales* de M.

Teorema 4.4. Sea R un DIP y $M \neq \{0\}$ un R-módulo finitamente generado y de torsión con (a) su aniquilador. Suponga que $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ y sea $N_i = \{x \in M;\ p_i^{\alpha_i} x = 0\}$ para $i \in [r]$. Entonces N_i es un submódulo de M cuyo aniquilador es $p_i^{\alpha_i}$ y es el submódulo de M de todos los elementos aniquilados por alguna potencia de p_i. Además, se tiene la descomposición

$$M = N_1 \oplus N_2 \oplus N_3 \oplus \cdots \oplus N_r.$$

Demostración. Resulta inmediato del teorema anterior. □

Los submódulos N_i del teorema anterior se llaman las *componentes p_i-primarias* de M.

Lema 4.2. *Sea R un DIP y p primo en R. Sea $F = R/(p)$.*

1. *Si $M = R^r$, entonces $M/pM \cong F^r$*
2. *Si $M = R/(a)$ con a no nulo en R, entonces*

$$M/pM \cong \begin{cases} F & si\ p \mid a\ en\ R \\ \{0\} & si\ p \nmid a\ en\ R \end{cases}$$

3. *Sea $M = R/(a_1) \oplus \cdots \oplus R/(a_r)$ donde cada a_i es divisibles por p. Entonces $M/pM \cong F^k$.*

Observación 4.6. $pM = \{pm | m \in M\}$. $0 \in pM$ y si $pm, pm' \in pM$, entonces $pm + pm' = p(m + m') \in pM$. Por lo tanto, $pm + pm' \in pM$. Si $r \in R$ y $pm \in pM$, entonces $r(pm) = (rp)m = (pr)m = p(rm) \in pM$. Luego, pM es submódulo de M.

Demostración. Para la parte 1, definamos el epimorfismo

$$\begin{array}{rccl} \phi: & R^r & \to & (R/p)^r \\ & (x_1, x_2, \ldots, x_r) & \mapsto & (x_1 + (p), x_2 + (p), \ldots, x_r + (p)) \end{array}$$

. Además,

$$\begin{aligned} \ker(\phi) &= \{(x_1, x_2, \ldots, x_r) \in R^n;\ x_i \in (p)\} \\ &= \{(a_1 p, a_2 p, \ldots, a_r p) \in R^n;\ a_i \in R\} \\ &= pM. \end{aligned}$$

Por lo tanto $R^r/pM \cong (R/p)^r$, de donde sigue que $M/pM \cong (R/p)^r = F^r$.

Para la parte 2, notemos que

$$p(R/(a)) = pM = \{p(r+(a));\ r \in R\} = \{pr+(a);\ r \in R\} = ((p)+(a))/(a).$$

Si $p \mid a$, entonces $(p)+(a) = (p)$. Luego $p(R/(a)) = pM = (p)/(a)$ y por lo tanto $M/pM = (R/(a))/((p)/(a)) \cong R/(p) = F$. Si $p \nmid a$, entonces $(p)+(a) = R$ pues (p) es maximal. Sigue que $p(R/(a)) = pM = R/(a)$, y luego $M/pM = (R/(a))/(R/(a)) = \{0\}$.

Para la parte 3, notemos que $pM \cong (p)/(a_1) \oplus (p)/(a_2) \oplus \cdots \oplus (p)/(a_k)$, y por lo tanto el tercer teorema de isomorfismo implica que

$$\begin{aligned} M/pM &= (R/(a_1))/((p)/(a_1)) \oplus (R/(a_2))/((p)/(a_2)) \oplus \cdots \oplus (R/(a_k))/((p)/(a_k)) \\ &\cong F \oplus F \oplus \cdots \oplus F = F^r. \end{aligned}$$

□

El siguiente teorema muestra que los factores invariantes y los divisores elementales (cada uno por separado) forman un sistema completo de invariantes en la clase de módulos que estamos considerando, y que tiene sentido hablar de los factores invariantes y los divisores elementales (salvo unidades) de un módulo.

Teorema 4.5 (Teorema fundamental de descomposición de módulos finitamente generados sobre un DIP: unicidad)**.**

1. Dos R-módulos finitamente generados M_1 y M_2 son isomorfos ssi tienen el mismo rango libre y los mismos factores invariantes (salvo unidades).
2. Dos R-módulos finitamente generados M_1 y M_2 son isomorfos ssi tienen el mismo rango libre y los mismos divisores elementales (salvo unidades).

Demostración. La implicancia $\Leftarrow$ de las afirmaciones 1 y 2 es directa.

Probamos la implicancia $\Rightarrow$ en 2: supongamos que $\phi\colon M_1 \to M_2$ es isomorfismo y sea $\operatorname{tor}(M_i)$ el submódulo de torsión de cada M_i. Es claro que $\phi(\operatorname{tor}(M_1)) \subseteq \operatorname{tor}(M_2)$, y considerar ϕ^{-1} en vez de ϕ permite concluir que $\phi(\operatorname{tor}(M_1)) = \operatorname{tor}(M_2)$, es decir $\operatorname{tor}(M_1) \cong \operatorname{tor}(M_2)$. De aquí sigue que

$$R^{r_1} \cong M_1/\operatorname{tor}(M_1) \cong M_2/\operatorname{tor}(M_2) \cong R^{r_2},$$

de manera que $r_1 = r_2$ pues R es conmutativo.

Entonces nos podemos reducir al caso en que M_1 y M_2 son de torsión. Sea $(a) \subseteq R$ el aniquilador de M_1 y M_2 (los dos aniquiladores coinciden ya que M_1 y M_2 son isomorfos) y escribamos $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la descomposición prima de a. Dado $p \in R$, definamos $N_1(p) = \{m \in M_1;\ p^\alpha m = 0 \text{ para algún } \alpha \in \mathbb{N}\}$. Sea $m \in N_1(p)$, de manera que $\phi(m) \in N_2(p) = \{m \in M_2;\ p^\alpha m = 0 \text{ para algún } \alpha \in \mathbb{N}\}$ ya que $\phi(p^\alpha m) = 0 = p^\alpha \phi(m)$. Concluimos que $\phi(N_1(p)) \subseteq N_2(p)$ y análogamente $\phi^{-1}(N_2(p)) \subseteq N_1(p)$. Luego $N_1(p) \cong N_2(p)$ para cada $p \in R$, y del Teorema 4.4 sigue que

$$M_1 \cong N_1(p_1) \oplus N_1(p_2) \oplus \cdots \oplus N_1(p_r)$$

y

$$M_2 \cong N_2(p_1) \oplus N_2(p_2) \oplus \cdots \oplus N_2(p_r)$$

con $N_1(p_i) \cong N_2(p_i)$ para todo $i \in [r]$. Luego basta probar la implicancia para el caso $M_1 \cong M_2$ con aniquilador común p^α. Haremos inducción sobre α. Si $\alpha = 0$, entonces $p^\alpha = 1$ y $M_1 = \{0\} = M_2$, y no hay nada que hacer.

Supongamos el resultado cierto para cualquier $M_1' \cong M_2'$ módulos de torsión finitamente generados sobre R con aniquiladores p^k con $k < \alpha$. Sean M_1 y M_2 R-módulos de torsión finitamente generados con aniquilador p^α. Supongamos que los divisores elementales de M_1 son

$$\underbrace{p, \ldots, p}_{m \text{ veces}}, p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_s}$$

con $2 \leq \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_s$, es decir, $M_1 \cong R/(p) \oplus \cdots \oplus R/(p) \oplus R/(p^{\alpha_1}) \oplus \cdots \oplus R/(p^{\alpha_s})$, lo que implica que $pM_1 \cong (1) \oplus (1) \oplus \cdots \oplus (1) \oplus R/(p^{\alpha_1 - 1}) \oplus \cdots \oplus R/(p^{\alpha_s - 1})$ con divisores elementales $p^{\alpha_1 - 1}, p^{\alpha_2 - 1}, \ldots, p^{\alpha_s - 1}$.

Análogamente, M_2 tiene divisores elementales

$$\underbrace{p, \ldots, p}_{n \text{ veces}}, p^{\beta_1}, p^{\beta_2}, \ldots, p^{\beta_t}$$

con $2 \leq \beta_1 \leq \beta_2 \leq \cdots \leq \beta_t$ y entonces pM_2 tiene divisores elementales $p^{\beta_1 - 1}, p^{\beta_2 - 1}, \ldots, p^{\beta_t - 1}$. Como $M_1 \cong M_2$ entonces $pM_1 \cong pM_2$ y el aniquilador de pM_1 es $p^{\alpha - 1}$, lo mismo que para M_2. La hipótesis inductiva implica que los divisores elementales de pM_1 y pM_2 son los mismos (salvo unidades).

Por lo tanto $s = t$ y además

$$\begin{aligned} p^{\beta_1 - 1} &= p^{\alpha_1 - 1} u_1 \quad &\Rightarrow \quad & (p^{\beta_1 - 1}) = (p^{\alpha_1 - 1}) \\ p^{\beta_2 - 1} &= p^{\alpha_2 - 1} u_2 \quad &\Rightarrow \quad & (p^{\beta_2 - 1}) = (p^{\alpha_2 - 1}) \\ &\vdots \\ p^{\beta_t - 1} &= p^{\alpha_t - 1} u_t \quad &\Rightarrow \quad & (p^{\beta_t - 1}) = (p^{\alpha_t - 1}). \end{aligned}$$

Luego $(p^{\beta_i}) = (p^{\alpha_i})$ para todo $i \in [t]$, de donde sigue que $\beta_i = \alpha_i$ para cada i. Por último, la parte 3. del lema anterior muestra que

$$M_1/pM_1 \cong F^{m+s} \qquad M_2/pM_2 \cong F^{n+s}.$$

Como $M_1 \cong M_2$ y $pM_1 \cong pM_2$ (bajo el mismo isomorfismo), entonces $M_1/pM_1 \cong M_2/pM_2 \cong F^{n+s} \cong F^{m+s}$. Por lo tanto $n = m$ y concluimos que M_1 y M_2 tienen los mismos divisores elementales. Esto termina la demostración de la parte 2.

Ahora la parte 1: notemos que a_m, el último de los factores invariantes de M_1, es el producto de las potencias máximas de los divisores elementales p_i de M_1. Lo mismo ocurre con M_2: si b_r es el último de los factores invariantes de M_2, entonces b_r es el producto de las potencias máximas de los divisores elementales p_i de M_2, que son los mismos de M_1 por la parte 2. Luego $a_m = b_r$. Del mismo modo, a_{m-1} es el producto de las potencias máximas de los p_i una vez sacados las potencias de a_m y así en adelante. Luego los factores invariantes de M_1 y M_2 son los mismos si $M_1 \cong M_2$. □

Corolario 4.6. Sea G un grupo abeliano finitamente generado. Entonces

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}$$

con $m_1 \mid m_2 \mid \cdots \mid m_r$ naturales mayores que 1.

En particular, si G es finito con $n = |G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la descomposición prima de $|G|$, tenemos que

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}$$

con $m_1 \mid m_2 \mid \cdots \mid m_r$ y además $m_1 m_2 \cdots m_r = n$. El grupo G también se puede descomponer de manera única como

$$G \cong \mathbb{Z}^r \oplus G_1 \oplus \cdots \oplus G_k$$

donde $|G_i| = p_i^{\alpha_i}$ y

$$G_i \cong \mathbb{Z}_{p_i^{\beta(1,i)}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{\beta(l_i,i)}}$$

para ciertos naturales $\beta(i,j) \geq 2$ tales que $\sum_i \beta(i,j) = \alpha_j$ para cada $j \in [k]$.

En ambos casos, los enteros m_i y $\beta(i,j)$ determinan a G salvo isomorfismo.

Observación 4.7. Sea G un grupo abeliano finito y $n = |G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la descomposición prima de $|G|$.

- La condición $m_i \mid m_r$ para cada $i \in [r]$ del corolario anterior muestra que cada divisor primo de $n = |G|$ debe dividir a m_r. En particular, si n es libre de cuadrados entonces el único grupo abeliano de orden n salvo isomorfismos es $\mathbb{Z}_n$.
- Dado $s \in \mathbb{N}$, sea $p(s)$ el número de particiones de s, es decir, el número de soluciones enteras de

  $$n_1 + \cdots + n_r = s;\ n_1 \geq n_2 \geq \cdots \geq n_r > 0, r \in \mathbb{N}.$$

  Las listas $\{\beta_{i,j}\}_{i \in [l_j]}$ para $j \in [k]$ determinan unívocamente a un grupo abeliano de orden n, y la cantidad de listas de este tipo (para un j fijo) es $p(\alpha_j)$. Luego la cantidad de grupos abelianos de orden n es $p(\alpha_1) \cdots p(\alpha_k)$.
- Las componentes p_i-primarias de un grupo abeliano finito G son los p_i-subgrupos de Sylow de éste. Luego G es isomorfo al producto de sus subgrupos de Sylow.

Ejemplo 4.6. Sea G un grupo abeliano de orden 180. Entonces $|G| = 2^3 \cdot 3^2 \cdot 5$ y por lo tanto, m_r es divisible por $2 \cdot 3 \cdot 5$. Esto nos da cuatro posibilidades,

$$m_r = 2^2 \cdot 3^2 \cdot 5 \qquad m_r = 2^2 \cdot 3 \cdot 5 \qquad m_r = 2 \cdot 3^2 \cdot 5 \qquad m_r = 2 \cdot 3 \cdot 5$$

- Si $m_r = 2^2 \cdot 3^2 \cdot 5$, entonces $G \cong \mathbb{Z}_{180}$, el grupo cíclico de orden 180.
- Si $m_r = 2^2 \cdot 3 \cdot 5$, entonces $m_{r-1} = 3$ y por lo tanto $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{60}$.
- Si $m_r = 2 \cdot 3^2 \cdot 5$, entonces $m_{r-1} = 2$ y por lo tanto $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{90}$.
- Si $m_r = 2 \cdot 3 \cdot 5$, entonces $m_{r-1} = 2 \cdot 3$ y por lo tanto $G \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{30}$.

En términos de divisores elementales, $|G| = 180 = 2^2 \cdot 3^2 \cdot 5$. Tenemos los siguientes casos:

- 2^2 admite una descomposición del exponente de la forma 2 o bien $1+1$.
- 3^2 admite una descomposición del exponente de la forma 2 o bien $1+1$.
- 5 admite una descomposición del exponente de la forma 1.

En una tabla:

Potencias	Descomposición del exponente	Grupos
2^2	2 ó $1+1$	$\mathbb{Z}_4$ ó $\mathbb{Z}_2 \oplus \mathbb{Z}_2$
3^2	2 ó $1+1$	$\mathbb{Z}_9$ ó $\mathbb{Z}_3 \oplus \mathbb{Z}_3$
5	1	$\mathbb{Z}_5$

Con los grupos de última columna armamos todas las combinaciones posibles tomando uno de cada fila. De esa forma recuperamos los factores invariantes:

Grupos	Factores invariantes
$\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{180}$	$2^2 \cdot 3^2 \cdot 5$
$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{60}$	$2^2 \cdot 3 \cdot 5$ y 3
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{90}$	$2 \cdot 3^2 \cdot 5$ y 2
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{30}$	$2 \cdot 3 \cdot 5$ y $2 \cdot 3$

Corolario 4.7. *Si V es un espacio vectorial sobre K de dimensión $n \in \mathbb{N}$ y $T : V \to V$ es lineal, entonces existen únicos polinomios mónicos $p_i(X) \in K[X]$ tales que*

$$V \cong K[X]/(p_1(X)) \oplus \cdots K[X]/(p_m(X))$$

como $K[X]$-módulos y $p_1(X) \mid \cdots \mid p_m(X)$. El polinomio $p_m(X)$ genera el aniquilador de V, y cada $K[X]/(p_i(X))$ es invariante bajo T.

Decimos que el polinomio $p_m(X)$ del corolario anterior es el *polinomio minimal* de T. Definimos también el *polinomio característico* de T como $\det(XI - A)$, donde A es cualquier matriz que representa a T. Es fácil ver que esta definición no depende de la elección de una base de V para representar T. Notemos que el polinomio característico siempre tiene grado n. Diremos también que el morfismo T del corolario anterior (y por extensión, cualquier matriz $A \in M_n(K)$ que represente a T al elegir una base) es *cíclico* si V es un módulo cíclico.

Observación 4.8. Supongamos que $V \cong K[X]/p(X)$ con $\operatorname{grad}(p(X)) = n$ (es decir, que T es cíclico). Si $q(X) \in K[X]$, entonces existen $s(X)$ y $t(X)$ tales que $q(X) = p(X)t(X) + s(X)$, con $\operatorname{grad}(s(X)) < \operatorname{grad}(p(X))$. Luego $s(X) + (p(X)) = q(X) + p(X)$, pues $q(X) - s(X) = p(X)t(X) \in (p(X))$. Por lo tanto,

$$\begin{aligned} K[X]/p(X) &= \{s(X) + (p(X)) \,;\, \operatorname{grad}(s(X)) < n\} \\ &= \{a_0 + a_1 X + \ldots + a_{n-1}X^n + (p(X));\ a_i \in K\} \end{aligned}$$

Por lo tanto $\{\overline{1}, \overline{X}, \overline{X^2}, \ldots, \overline{X^{n-1}}\}$ es base de $K[X]/(p(X))$ como K-espacio vectorial (la distinción es importante: $K[X](p(X))$ es cíclico como $K[X]$-módulo).

¿Cómo actúa la multiplicación de X (es decir, la composición por T en V) en esta base?

$$\begin{aligned} X \cdot \overline{1} &= \overline{X} \\ X \cdot \overline{X} &= \overline{X^2} \\ &\vdots \\ X \cdot \overline{X^{n-1}} = \overline{X^n} &= -a_{n-1}\overline{X^{n-1}} - a_{n-2}\overline{X^{n-2}} - \cdots - a_1\overline{X} - a_0\overline{1}, \end{aligned}$$

y por lo tanto existe $\{v_1, \ldots, v_n\}$ base en V tal que

$$\begin{aligned} Tv_1 &= v_2 \\ Tv_2 &= v_3 \\ &\vdots \\ Tv_{n-1} &= v_n \\ Tv_n &= -a_0 v_1 + \cdots + -a_{n-1} v_n. \end{aligned}$$

Luego la matriz de T en esta base $\mathscr{B}$ es

$$[T]^{\mathscr{B}}_{\mathscr{B}} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix} = C_{p(X)}$$

y se le llama la *matriz compañera* de $p(X)$. Es un ejercicio ver que el polinomio característico de T en este caso es justamente $p(X)$ (basta calcular $\det(XI - [T]^{\mathscr{B}}_{\mathscr{B}})$), y obtenemos que el polinomio característico y el minimal de T son el mismo.

Si $V \cong K[X]/(p_1(X)) \oplus K[X]/(p_2(X)) \oplus \cdots \oplus K[X]/(p_m(X))$ tal que $p_1(X) \mid p_2(X) \mid \cdots \mid p_m(X)$, entonces como la suma de módulos cíclicos es directa, podemos usar lo anterior para encontrar una base $\mathscr{B}$ de V tal que la matriz asociada a T en esta base es

$$[T]^{\mathscr{B}}_{\mathscr{B}} = \begin{pmatrix} C_{p_1(X)} & 0 & 0 & \cdots & 0 \\ 0 & C_{p_2(X)} & 0 & \cdots & 0 \\ 0 & 0 & C_{p_3(X)} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & C_{p_m(X)} \end{pmatrix}.$$

Esta representación matricial de T (que es única y determina unívocamente a T) se llama la *forma normal de Frobenius* de T, o la *forma canónica racional* de T. De ésta se lee que el polinomio característico de T corresponde a $p_1(X)\cdots p_m(X)$ de manera que el polinomio minimal siempre divide al polinomio característico y por lo tanto tienen las mismas raíces en K. Deducimos el *teorema de Cayley-Hamilton*: el polinomio característico de T anula a T.

Observación 4.9. Dos matrices $A, B \in M_n(K)$ son *semejantes* si existe $P \in M_n(K)$ invertible tal que $B = PAP^{-1}$. Notemos que dos matrices $A, B \in M_n(K)$ son semejantes ssi $A = [T]_{\mathscr{B}}^{\mathscr{B}}$ y $B = [T]_{\mathscr{C}}^{\mathscr{C}}$ con $T: V \to V$ lineal donde $\mathscr{B}$ y $\mathscr{C}$ son bases de V.

Dos matrices A, B de la forma

$$A = \begin{pmatrix} C_{p_1} & & & \\ & C_{p_2} & & \\ & & \ddots & \\ & & & C_{p_n} \end{pmatrix} \qquad B = \begin{pmatrix} C_{q_1} & & & \\ & C_{q_2} & & \\ & & \ddots & \\ & & & C_{q_n} \end{pmatrix}$$

con $p_1 \mid p_2 \mid \cdots \mid p_n$ y $q_1 \mid q_2 \mid \cdots \mid q_n$, son semejantes ssi $q_k = p_k$.

Ejemplo 4.7. Sea $T: \mathbb{R}^3 \to \mathbb{R}^3$ cuyo polinomio característico es $(X+1)(X^2+1) = X^3 + X^2 + X + 1$. Como los factores primos del polinomio característico de T y los factores primos del polinomio minimal son los mismos se tiene que el polinomio característico de T es $(X+1)(X^2+1)$. Por lo tanto,

$$C_{(X+1)(X^2+1)} = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix} = [T]_{\mathscr{B}}^{\mathscr{B}}$$

con cierta base $\mathscr{B}$.

Ejemplo 4.8. Si $T: \mathbb{R}^4 \to \mathbb{R}^4$ y el polinomio minimal de T es $(X+1)(X^2+1)$, entonces el característico es $(X+1)^2(X^2+1)$. Por lo tanto, $\mathbb{R}^4 \cong \mathbb{R}[X]/(X+1) \oplus \mathbb{R}[X]/(X+1)(X+1)^2$ y se tiene

$$[T]_{\mathscr{B}}^{\mathscr{B}} = \left(\begin{array}{c|ccc} -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{array}\right)$$

Observación 4.10. Si $V \cong K[X]/(p_1(X)) \oplus K[X]/(p_2(X)) \oplus \cdots \oplus K[X]/(p_n(X))$, sean $\{r_i^{\alpha_i}(X)\}_{i\in[t]}$ sus divisores elementales. Se tiene que $r_1^{\alpha_1}(X) r_2^{\alpha_2}(X) \cdots r_t^{\alpha_t}(X) = p_n(X)$ para ciertos naturales $\alpha_i \geq 1$, y que los r_i son polinomios irreducibles. Supongamos que cada $r_i(X)$ es de grado 1, es decir, existen $\beta_i \in K$ tales que $r_i(X) = (X - \beta_i)$. Como todos los $r_i(X)$ dividen al polinomio característico de T, esta condición es equivalente a decir que K contiene los valores propios de T. Entonces

$$V \cong K[X]/(X-\lambda_1)^{k_1} \oplus K[X]/(X-\lambda_2)^{k_2} \oplus \cdots \oplus K[X]/(X-\lambda_r)^{k_r},$$

con los λ_i no necesariamente distintos entre sí.

Analicemos primero el caso cuando $V = K[X]/(X-\lambda)^k$. Consideremos $\{1, \overline{X}-\lambda, (\overline{X}-\lambda)^2, \ldots, (\overline{X}-\lambda)^{k-1}\}$ base de V como K-espacio vectorial. Tenemos que

$$\begin{aligned} X \cdot 1 &= \overline{X} - \lambda + \lambda \\ X \cdot (\overline{X}-\lambda) &= \overline{X}^2 - \lambda X = \lambda(\overline{X}-\lambda) + (\overline{X}-\lambda)^2 \\ &\vdots \\ X \cdot (\overline{X}-\lambda)^{k-2} &= \lambda(\overline{X}-\lambda)^{k-2} + (\overline{X}-\lambda)^{k-1} \\ X \cdot (\overline{X}-\lambda)^{k-1} &= \lambda(\overline{X}-\lambda)^{k-1} + (\overline{X}-\lambda)^k = \lambda(\overline{X}-\lambda)^{k-1}. \end{aligned}$$

Tomando la base en el orden inverso $\mathscr{B} = \{(\overline{X}-\lambda)^{k-1}, (\overline{X}-\lambda)^{k-2}, \ldots, (\overline{X}-\lambda), 1\}$ y de esta forma

$$[T]^{\mathscr{B}}_{\mathscr{B}} = \begin{pmatrix} \lambda & 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & 0 & \cdots & 0 \\ 0 & 0 & \lambda & 1 & \cdots & 0 \\ 0 & 0 & 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \lambda \end{pmatrix} = J_{\lambda,k}.$$

Esta matriz se llama el *bloque de Jordan de tamaño k para el valor propio* λ. Luego en el caso general tenemos que $V \cong K[X]/(X-\lambda_1)^{k_1} \oplus K[X]/(X-\lambda_2)^{k_2} \oplus \cdots \oplus K[X]/(X-\lambda_r)^{k_r}$ y concluimos que

$$[T]^{\mathscr{B}}_{\mathscr{B}} = \begin{pmatrix} J_{\lambda_1,k_1} & & & \\ & J_{\lambda_2,k_2} & & \\ & & \ddots & \\ & & & J_{\lambda_r,k_r} \end{pmatrix}.$$

La representación de T en una matriz de este tipo (que es única) se llama *forma normal de Jordan* de T.

Ejemplo 4.9. Sea $T : \mathbb{R}^3 \to \mathbb{R}^3$ cuyo polinomio minimal es $(X+1)(X+2)$, entonces el característico es $(X+1)^2(X+2)$ o bien $(X+1)(X+2)^2$. Los factores invariantes en cada caso, son $(X+1)$ y $(X+1)(X+2)$. En una tabla,

Divisores elementales	Particiones de potencias	Segundo factor invariante
$X+1$	1	1
$X+2$	1	0

Por lo tanto, si los divisores elementales son $(X+1)$, $(X+1)$ y $(X+2)$, entonces

$$[T]^{\mathscr{B}}_{\mathscr{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

y si los divisores elementales son $(X+1)$, $(X+2)$ y $(X+2)$,

$$[T]_{\mathscr{B}}^{\mathscr{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Ejemplo 4.10. Sea $T : \mathbb{R}^4 \to \mathbb{R}^4$ y $m_T(X) = (X-1)(X+2)^2$. Entonces el polinomio característico puede ser $c_T(X) = (X+1)^2(X+2)^2$ o bien $c_T(X) = (X+1)(X+2)^3$.

En el primer caso, los factores invariantes serían $(X+1)$ y $(X+1)(X+2)^2$, en el segundo caso, serían $(X+2)$ y $(X+1)(X+2)^2$.

Los divisores elementales en el primer caso serían $(X+2)^2$, $(X+1)$ y $(X+1)$, por lo tanto,

$$[T]_{\mathscr{B}}^{\mathscr{B}} = \left(\begin{array}{cc|c|c} -2 & 1 & & \\ 0 & -2 & & \\ \hline & & -1 & \\ \hline & & & -1 \end{array}\right)$$

y en el segundo caso, los divisores elementales serían $(X+2)^2$, $(X+2)$ y $(X+1)$, por lo tanto

$$[T]_{\mathscr{B}}^{\mathscr{B}} = \left(\begin{array}{c|c|cc} 1 & & & \\ \hline & -2 & & \\ \hline & & -2 & 1 \\ & & 0 & -2 \end{array}\right).$$

4.4. Ejercicios

Ejercicio 4.1. Sea M un R-módulo y N_1, N_2 submódulos de M. N_2 se dice *suplemento* o *complemento* de N_1 si $M = N_1 \oplus N_2$. Muestre que si N_2 es un suplemento de N_1, entonces $M/N_1 \cong N_2$, y concluya que si N_2 y N_2' son suplementos de N_1, entonces $N_2 \cong N_2'$.

Ejercicio 4.2. Veamos algunos contraejemplos que muestran la diferencia entre espacios vectoriales y módulos.

a) Sea $M = \{f : \mathbb{N} \to \mathbb{Z}\}$ el conjunto de sucesiones a valores enteros, dotado de la suma componente a componente y sea $R = \{\phi : M \to M; \phi \text{ morfismo de grupos abelianos}\}$ el anillo de endomorfismos de M. Demuestre que $M^n \cong M^k$ (como R-módulos) para todo $n, k \in \mathbb{N}\backslash\{0\}$.
Indicación: considere $\phi_1, \phi_2 \in M$ definidas por $\phi_1(f)_n = f_{2n+1}$ y $\phi_2(f)_n = f_{2n}$.

b) Muestre que el ideal $(2, x)$ en $\mathbb{Z}[x]$ es un $\mathbb{Z}[x]$-módulo que no tiene base.

c) Encuentre un ejemplo de algún $\mathbb{Z}$-módulo que posea submódulos que no admiten suplemento.

Ejercicio 4.3. Sea F un R-módulo libre y $f : M \to F$ un epimorfismo de R-módulos.

a) Pruebe que f posee una *sección*, es decir una función R-lineal $s : F \to M$ tal que $f \circ s = \mathrm{id}_F$.

b) Demuestre que $\ker(f) \subseteq M$ admite un suplemento isomorfo al módulo libre F.

Ejercicio 4.4. Sea R un anillo, M un R-módulo y $n \in \mathbb{N}$. Sean $\phi_1, \ldots, \phi_n$ R-endomorfismos tales que $\sum_{i=1}^{n} \phi_i = \mathrm{id}$ y $\phi_i \circ \phi_j = 0$ si $i \neq j$. Pruebe que cada ϕ_i es idempotente y que $M \cong \prod_{i=1}^{n} \phi_i(M)$.

Ejercicio 4.5. Sea D un DIP y definamos el rango de un D-módulo finitamente generado como su rango libre. Sea K un R-submódulo de D^n. Pruebe que $\mathrm{rango}(D^n/K) = n - \mathrm{rango}(K)$ y muestre además que si M es un R-módulo finitamente generado y N un R-submódulo de M, se tiene que N y M/N son finitamente generados y $\mathrm{rango}(M) = \mathrm{rango}(N) + \mathrm{rango}(M/N)$.

Ejercicio 4.6. Sea R un anillo, M' , M y M'' R-módulos y

$$0 \xrightarrow{f_1} M' \xrightarrow{f_2} M \xrightarrow{f_3} M'' \xrightarrow{f_4} 0$$

una secuencia exacta, es decir, $\mathrm{im}(f_i) = \ker(f_{i-1})$. Determine la veracidad de las siguientes proposiciones.

1. Si M es finitamente generado (f.g.), entonces M'' es f.g.
2. Si M' y M'' son f.g. es M f.g.

Determine bajo cuáles de las siguientes hipótesis extra M f.g implica M' f.g.

1. M es un módulo libre.
2. R es un DIP.
3. M es un módulo semisimple (ver ejercicio 4.10).
4. Si existe una función $\mu\colon M'' \to M$ tal que $f_4 \circ \mu$ sea la identidad de M.

¿Alguna combinación de éstas permite concluir?

Indicación: el punto 4. es equivalente a que $M = f_2(M') \oplus B$ para algún submódulo B de M.

Ejercicio 4.7. Si R es un anillo, A, B y M son R-módulos, definimos $\mathrm{Hom}_R(A,B) := \{\varphi : A \to B / \ \varphi \text{ es } R\text{-lineal}\}$

a) Pruebe que $\mathrm{Hom}_R(A,B)$ es un R-módulo con la suma y la multiplicación por escalar definida punto a punto, es decir, $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$ y $(r\varphi)(x) = r\varphi(x)$
b) Muestre que $\mathrm{Hom}_R(A \oplus B, M) \cong \mathrm{Hom}_R(A,M) \oplus \mathrm{Hom}_R(B,M)$
c) Si R es conmutativo y M es un R-módulo libre con rango finito, entonces $\mathrm{Hom}_R(M,R) \cong M$. En cierto sentido, esto es probar que los módulos libre de rango finito son autoduales.
d) Pruebe que $\mathrm{Hom}_R(R,M) \cong M$. ¿Es necesario asumir que R es conmutativo o que M sea libre? ¿Qué pasa si R no es unitario?

Ejercicio 4.8.

a) Sea R un anillo, un R-módulo M se dice *simple* (o irreducible) si sus únicos submódulos son 0 y M. Pruebe que un R-módulo M es simple si y solo si $M \cong R/I$ (como R-módulos) con I un ideal maximal. ¿Puede I ser un ideal izquierdo en vez de un ideal?
b) Usando el ejercicio anterior pruebe que si R es un anillo conmutativo, entonces el radical de Jacobson de R (definido en el ejercicio 3.6) es el ideal que aniquila a todos los R-módulos. ¿Se puede relajar la condición de que R sea conmutativo?

Ejercicio 4.9. Demuestre que si R es un anillo y M es un R-módulo simple, entonces el anillo de endomorfismos $\mathrm{End}_R(M)$ es un anillo de división. Este resultado se conoce como el *lema de Schur*.

Ejercicio 4.10. Decimos que un R-módulos es *semisimple* si es que es la suma directa de módulos simples. Pruebe que un R-módulo es semisimple si y solo si todos sus submódulos son sumandos directos (es decir, todo submódulo posee complemento).
Indicación: Si $M = \bigoplus_{i\in I} S_i$ (con cada S_i simple) y B es un submódulo, piense en $S_J = \bigoplus_{i\in J} S_i$ donde J es un subconjunto de índices maximal tal que $S_J \cap B = \varnothing$.

Ejercicio 4.11. Clasifique todos los grupos abelianos de orden 72. ¿Para qué número entre 1 y 72 hay más grupos abelianos con ese orden? ¿Hay alguna heurística para maximizar esta cantidad en general?

Ejercicio 4.12. Sea R un DIP, $v_1,\ldots,v_n \in R^n$ y $A = (v_1 \mid \ldots \mid v_n) \in M_n(R)$ la matriz cuyas columnas son los v_i. Denotemos también $M = \langle v_1,\ldots,v_n\rangle$ el submódulo generado por los v_i.

a) Pruebe que las siguientes afirmaciones son equivalentes.
   1. Los vectores $v_1,\ldots,v_i$ son l.i.
   2. $\ker(A) = \{0\}$ (entendiendo que A es un morfismo de R^n en sí mismo).
   3. Las columnas de $B = PAQ$ son l.i., donde $P,Q \in M_n(R)$ son invertibles.
   4. $\det(A) \neq 0$.
   5. $M \cong R^n$.
   6. El módulo cociente R^n/M es de torsión.

b) Muestre que si $R = \mathbb{Z}$ y los $v_1,\ldots,v_n$ son l.i. en $\mathbb{Z}^n$, entonces $\mathbb{Z}^n/M$ es un grupo abeliano finito de orden $|\mathbb{Z}^n/M| = |\det(A)|$.

c) Muestre que si $R = K[X]$ con K un cuerpo y los $v_1,\ldots v_n$ son l.i. sobre $K[X]^n$, entonces $V \doteq K[x]^n/M$ es un espacio vectorial sobre K de dimensión $\dim_K(V) = \mathrm{grad}(\det(A))$.

Ejercicio 4.13. Dado un anillo R cualquiera, definimos el *centro* de R como el conjunto de elementos que conmutan con todo el resto, es decir $Z(R) = \{a \in R;\ ba = ab\ \forall b \in R\}$ y definimos también el *conmutante* de $a \in R$ como el conjunto de elementos que conmutan con a, esto es $C(a) = \{b \in R;\ ab = ba\}$. El *biconmutante* de a es el conjunto de los elementos que conmutan con todos aquellos que conmutan con a, es decir $B(a) = \{b \in R;\ bc = cb\ \forall c \in C(a)\}$. Dado un módulo M sobre un anillo conmutativo R, escribimos R_M para denotar el subanillo conmutativo de $\mathrm{End}_R(M)$ dado por $R_M = \{\mu_r;\ r \in R\}$ donde $\mu_r : M \to M$ es la multiplicación por el escalar r, es decir $\mu_r(x) = rx$.

En este ejercicio estudiaremos los biconmutantes y conmutantes de una matriz cuadrada a coeficientes en un cuerpo k.

a) Para $A,B \in M_n(k)$, muestre que $B \in C(a)$ ssi $B : M_A \to M_A$ es un morfismo de $k[X]$-módulos.

En vista de lo anterior, estudiemos el anillo $\mathrm{End}_R(M)$ donde M es un módulo finitamente generado sobre un DIP R.

b) Pruebe que si M es un R-módulo cíclico, entonces su anillo de endomorfismos está dado por $\mathrm{End}_R(M) = R_M$.

c) 1. Para un módulo cualquiera sobre un anillo conmutativo R, verifique que $R_M \subseteq Z(\mathrm{End}_R(M))$.

2. Sea M un módulo f.g. sobre un DIP R. De acuerdo con el teorema fundamental de descomposición, escribamos $M \cong Rm_1 \oplus \cdots \oplus Rm_s$ como suma directa de módulos cíclicos con generadores $m_i \in M$ cuyos aniquiladores son los factores invariantes de M. Pruebe que dados $i, j \in [s]$ son $i \geq j$, existe un único endomorfismo $E_{ij} \in \mathrm{End}_R(M)$ tal que $E_{ij}(m_p) = 0$ si $p \neq i$ y $E_{ij}(m_i) = m_j$.
3. Muestre que si M es un módulo f.g. sobre un DIP R, entonces $Z(\mathrm{End}_R(M)) = R_M$.

d) Dados un cuerpo k y $A \in M_n(k)$, muestre que las siguientes proposiciones son equivalentes.
1. A es cíclica.
2. Existe $v \in k^n$ tal que $\{v, Av, A^v, \ldots, A^{n-1}v\}$ es base de k^n.
3. El polinomio minimal de A tiene grado n.
4. El polinomio minimal y el polinomio característico de A difieren, a lo más, en un factor -1.

e) 1. Demuestre que si $A \in M_n(k)$ es una matriz cíclica, entonces su conmutante está formado por los polinomios en A, es decir $C(A) = k[A] = \{p(A);\ p(X) \in k[X]\}$.
2. Determine todas las matrices que conmutan con

$$\begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & 0 \end{pmatrix} \in M_n(k).$$

3. Demuestre que si A es una matriz cualquiera de $M_n(k)$, entonces su biconmutante $B(A) = k[A]$.

Capítulo 5

Cuerpos

5.1. Extensiones de Cuerpo

Recordemos que todo morfismo entre cuerpos es necesariamente inyectivo, según la observación 3.2. Luego no tiene sentido hablar de cocientes en este contexto, y deberemos contentarnos con estudiar lo que ocurre cuando un cuerpo k está contenido en otro cuerpo K. En tal caso diremos que K es una extensión de k y anotaremos $K|k$. Si $a \in K$ es raíz de un polinomio en $k[X]$, entonces diremos que a es *algebraico* sobre k, o que a es algebraico en $K|k$. Si todo elemento de K es algebraico sobre k, diremos que K es *algebraico* sobre k o que $K|k$ es una *extensión algebraica*. Si $a \in K$ y no es algebraico sobre k, diremos que a es *trascendente* sobre k. Si una extensión $K|k$ no es algebraica diremos que es una *extensión trascendente*.

Ejemplo 5.1. El complejo i es algebraico sobre $\mathbb{R}$, pues satisface $X^2+1 \in \mathbb{R}[X]$. Como $X^2+1 \in \mathbb{Q}[X]$, entonces $i \in \mathbb{C}$ también es algebraico sobre $\mathbb{Q}$. Si $z = a+bi \in \mathbb{C}$, entonces $(X-z)(X-\overline{z}) = X^2 - 2aX + (a^2+b^2) \in \mathbb{R}[X]$, entonces todo elemento de $\mathbb{C}$ satisface un polinomio (irreducible de grado a lo más 2) en $\mathbb{R}[X]$, por lo tanto $\mathbb{C}|\mathbb{R}$ es una extensión algebraica. Sin embargo, $\mathbb{C}|\mathbb{Q}$ no es algebraica.

Sea $K|k$ una extensión y $k \subseteq E \subseteq K$, con E un cuerpo, entonces diremos que E es un *cuerpo intermedio* de la extensión $K|k$. Si $a \in K$ es algebraico sobre k, entonces existe un polinomio $p(X) \in k[X]$ tal que $p(a) = 0$, pero como $k \subseteq E$, entonces $k[X] \subseteq E[X]$ por lo tanto $p(X) \in E[X]$, es decir, a es algebraico sobre E. Luego si $K|k$ es algebraica, entonces también $K|E$ es algebraica. Como veremos en la proposición 5.4, $E|k$ resulta ser algebraica.

Si $K|k$ es una extensión, podemos considerar K como un espacio vectorial sobre k, definiendo la suma de vectores en K como la suma usual de K y la multiplicación escalar como la multiplicación usual de K. A la dimensión $\dim_k K$ le llamaremos el *grado* de la extensión $K|k$ y anotaremos $[K:k] = \dim_k K$. Si $[K:k]$ es finito diremos que la extensión $K|k$ es finita, en caso contrario diremos que la extensión es infinita. Por ejemplo la extensión $\mathbb{C}|\mathbb{R}$ es una extensión de grado 2, pues $\{1, i\}$ es base de $\mathbb{C}$ como espacio vectorial sobre $\mathbb{R}$. Notemos que $[K:k] = 1$ ssi $K = k$.

Proposición 5.1. *Toda extensión finita es algebraica.*

Demostración. Si $K|k$ es una extensión finita, digamos $[K:k]=n$ y $a\in K$, entonces el conjunto $\{1,a,a^2,a^3,\dots,a^n\}$ es un conjunto linealmente dependiente sobre k, es decir, existen $a_0,a_1,\dots,a_n\in k$ no todos nulos tales que

$$a_0+a_1a+a_2a^2+\cdots+a_na^n=0$$

por lo tanto el polinomio $p(X)=\sum_{k=0}^{n}a_kX^k$ está en $k[X]$ y $p(a)=0$, es decir, a es algebraico sobre k. □

Ejemplo 5.2. Consideremos un cuerpo k y el anillo de polinomios $k[X]$, en una variable sobre k. Como $k[X]$ es un dominio de integridad, entonces podemos considerar el cuerpo de cuocientes de $k[X]$, denotado por $k(X)=Q(k[X])$, llamado el cuerpo de *funciones racionales sobre* k. Como $k[X]$ es un espacio vectorial de dimensión infinita sobre k y $k[X]\subseteq k(X)$, entonces $k(X)|k$ es una extensión infinita. Además, X es trascendente sobre k.

Ejemplo 5.3 (Un ejemplo importante)**.** Como vimos en el capítulo 3, si k es un cuerpo y $p(X)\in k[X]$ irreducible, entonces $K=k[X]/(p(X))$ es un cuerpo que contiene una raíz de $p(X)$ y a (una copia) de k. Además $\dim_k K=n$, donde n es el grado del polinomio $p(X)$. Es decir, para todo polinomio irreducible $p(X)\in k[X]$ existe una extensión de k que contiene una raíz de $p(X)$. Si $p(X)$ no es irreducible, entonces $p(X)=p_1(X)p_2(X)\cdots p_r(X)$ con $p_i(X)$ irreducible en $k[X]$, por lo tanto el cuerpo $k[X]/(p_1(X))$ es un cuerpo que contiene una raíz de $p(X)$. Luego para todo polinomio de $k[X]$ (no necesariamente irreducible) existe una extensión de k que tiene una raíz de $p(X)$.

Más aún, si $P=\{p_1(X),p_2(X),\dots,p_n(X)\}$ es un conjunto finito de polinomios en $k[X]$, sea $q_1(X)$ un factor irreducible de $p_1(X)$ en $k[X]$ de manera que $F_1=k[X]/(q_1(X))$ es un cuerpo que contiene a k y tiene una raíz de $p_1(X)$. Ahora sea $q_2(X)$ un factor irreducible de $p_2(X)$ en $F_1[X]$, entonces $F_2=F_1[X]/(q_2(X))$ es un cuerpo que contiene una raíz de $p_2(X)$ y que contiene a F_1. Por lo tanto F_2 es un cuerpo que contiene a k y tiene una raíz de $p_1(X)$ y una raíz de $p_2(X)$. Continuando este proceso inductivamente, podemos construir un cuerpo F que contiene a k y tiene una raíz para cada polinomio de P.

Si $K|k$ y E,E' son dos cuerpos intermedios, es decir, $k\subseteq E\subseteq K$ y $k\subseteq E'\subseteq K$, entonces $E\cap E'$ es un cuerpo intermedio de la extensión $K|k$. Mas generalmente, si $\{F_\lambda\}_{\lambda\in\Lambda}$ es una familia de cuerpos intermedios de la extensión $K|k$, entonces

$$F=\bigcap_{\lambda\in\Lambda}F_\lambda$$

es un cuerpo intermedio de la extensión $K|k$. Si $\emptyset\neq S\subseteq K$, entonces $k(S)$ denota la intersección de todos los cuerpos intermedios de la extensión $K|k$ que contienen a S, es decir

$$k(S)=\bigcap_{\substack{k\subseteq F\subseteq K\\ S\subseteq F}}F$$

y es el cuerpo más pequeño F de la extensión $K|k$ tal que $S\subseteq F$. Sigue que si $k\subseteq E\subseteq K$ y $S\subseteq E$, entonces $k(S)\subseteq E$. En el caso particular que $S=\{a_1,a_2,\dots a_n\}$ es un conjunto finito, a $k(S)$ lo denotamos por

$k(a_1, a_2, \ldots, a_n)$ y en el caso en que S es el singleton $\{a\}$, a la extensión $k(a)|k$ la llamamos una extensión *simple* y a a lo llamamos un elemento *primitivo* de la extensión. Por ejemplo, i pertenece a $\mathbb{C}$ y $\mathbb{R}(i) = \mathbb{C}$, de manera que $\mathbb{C}|\mathbb{R}$ es una extensión simple e i es un elemento primitivo. Más aún, todo elemento $z \in \mathbb{C} \setminus \mathbb{R}$ es un elemento primitivo de la extensión $\mathbb{C}|\mathbb{R}$.

Ahora clasificaremos las extensiones simples. Como notación, cuando $K|k$ y $L|k$ son extensiones de cuerpo y $\phi : K \to L$ es un morfismo de cuerpos tal que $\phi(a) = a$ para cada $a \in k$, diremos que ϕ es un k-morfismo.

Teorema 5.1. *Sea $K|k$ una extensión y $a \in K$.*

1. *Si a algebraico sobre k, entonces existe un único polinomio $m(X) \in k[X]$ irreducible y único k-isomorfismo $\sigma : k[X]/(m(X)) \to k(a)$ tal que $\sigma(X + (m(X))) = a$. Además $[k(a) : k] = \text{grad}(m(X))$.*
2. *Si a es trascendente sobre k, entonces existe un único k-isomorfismo $\sigma : k(X) \to k(a)$ tal que $\sigma(X) = a$. Además la extensión $k(a)|k$ es infinita.*

Demostración. Podemos definir la evaluación $\phi : k[X] \to K$ como $\phi(p(X)) = p(a)$. Esta función es un morfismo de anillos tal que $\phi(\alpha) = \alpha$ para cada $\alpha \in k$ y $\phi(X) = a$ y además es único con esas propiedades. A la imagen de ϕ lo denotamos por $k[a] \subseteq k(a) \subseteq K$.

Si a es algebraico sobre k, entonces existe $p(X)$ no nulo en $k[X]$ tal que $p(a) = 0$. En este caso sea $m(X)$ de grado positivo mínimo en $k[X]$ tal que $m(a) = 0$, de manera que $\ker(\phi) = (m(X))$. Además $m(X)$ es irreducible, pues si no lo fuera contradice el hecho de que $m(X)$ es de grado mínimo. Si escogemos $m(X)$ mónico, entonces $m(X)$ es único polinomio mónico irreducible tal que $m(a) = 0$. Por el primer teorema del isomorfismo $k[X]/(m(X)) \cong k[a]$ (de hecho es k-isomorfo), y como $k[X]/(m(X))$ es un cuerpo tenemos que $k[a]$ también lo es. Notando que $k \subseteq k[a] \subseteq k(a)$ obtenemos que $k[a] = k(a)$. Es claro que la dimensión de $k[X]/(m(X))$ es $\text{grad}(m(X))$.

Por otro lado, si a es trascendente, entonces $\ker(\phi) = \{0\}$ y $k[X] \cong k[a]$ y sigue que $k(a) \cong k(X) = Q(k[X])$ (donde el isomorfismo fija k punto a punto). Como la extensión no es algebraica, obtenemos que necesariamente es infinita. □

Al polinomio $m(X)$ del teorema anterior se le llama el *polinomio irreducible de a sobre k* y lo denotamos por $\text{irr}_{a,k}(X)$.

Un resultado muy útil acerca del grado de una extensión es el siguiente.

Proposición 5.2. *Si $k \subseteq L \subseteq K$ es una cadena de cuerpos, entonces $[K : k] = [K : L][L : k]$.*

Demostración. Si $[K : L]$ o $[L : k]$ es infinito, entonces claramente $[K : k]$ es infinito también. Supongamos entonces que $[K : L] = n$ y $[L : k] = m$.

Sea $\{u_1, u_2, \ldots, u_n\}$ base de K sobre L, es decir, para cada $x \in K$ existen únicos $a_i \in L$ tales que

$$x = a_1u_1 + a_2u_2 + \cdots a_nu_n.$$

Pero cada a_i se escribe de forma única como combinación lineal sobre k de $v_1, v_2, \ldots, v_m$ una base de L sobre k, esto es, para cada a_i se tiene que existen (únicos) $b_{ki} \in k$ tales que

$$a_i = b_{1i}v_1 + b_{2i}v_2 + \cdots + b_{mi}v_m = \sum_{k=1}^{m} b_{ki}v_k.$$

Luego

$$x = \left(\sum_{k=1}^{m} b_{k1}v_1\right)u_1 + \left(\sum_{k=1}^{m} b_{k2}v_k\right)u_2 + \cdots + \left(\sum_{k=1}^{m} b_{kn}v_k\right)u_n = \sum_{k\in[m],i\in[n]} b_{ki}v_k u_i$$

y por lo tanto $B = \{v_k u_i;\ k \in [m],\ i \in [n]\}$ es un conjunto generador de K sobre k. Además, si

$$0 = \left(\sum_{k=1}^{m} b_{k1}v_1\right)u_1 + \left(\sum_{k=1}^{m} b_{k2}v_k\right)u_2 + \cdots + \left(\sum_{k=1}^{m} b_{kn}v_k\right)u_n = \sum_{k\in[m],i\in[n]} b_{ki}v_k u_i,$$

como $\{u_i\}$ es base se tiene que para cada i

$$\sum_{k=1}^{m} b_{ki}v_k = 0$$

y como $\{v_k\}$ es base, se tiene que $b_{ij} = 0$ para cada i, j. Concluimos que B es base de K sobre k, de modo que $\dim_k K = nm = [K : k]$. □

Observación 5.1. Si $K|k$ es una extensión de grado p primo, entonces cada elemento $a \in K\backslash k$ genera todo K, pues por la proposición anterior $[K : k(a)]$ divide a $p = [K : k]$ y no es p (de serlo tendríamos que $[k(a) : k] = 1$, es decir $a \in k$) de manera que $[K : k(a)] = 1$.

Proposición 5.3. *$K|k$ es finita ssi $K = k(a_1, a_2, \ldots, a_n)$ con a_i algebraico sobre k para cada $i \in [n]$.*

Demostración. Consideremos una extensión $K|k$ y $\{a_1, a_2, a_3, \ldots a_n\} \subseteq K$ un conjunto finito de elementos algebraicos sobre k. Podemos considerar una cadena de cuerpos intermedios $E_i = k(a_1, a_2, \ldots, a_i)$ para cada $i \in [n]$ de modo que

$$E_0 = k \subseteq E_1 \subseteq E_2 \subseteq E_3 \subseteq \cdots E_n = k(a_1, a_2, a_3, \ldots a_n).$$

Por la proposición anterior vemos que

$$[E_n : E_{n-1}][E_{n-1} : E_{n-2}][E_{n-1} : E_{n-2}]\cdots[E_1 : k] = [E_n : k]$$

Como cada extensión $E_j|E_{j-1}$ es simple y algebraica, entonces $E_j|E_{j-1}$ es finita y por lo tanto $E_n|k$ es finita. Recíprocamente, si $K|k$ es finita, digamos $[K : k] = n$, sea $\{u_1, u_2, \cdots u_n\}$ una base de K sobre k de modo que $K = k(u_1, u_2, \ldots, u_n)$. Como $K|k$ es finita, entonces cada u_i es algebraico sobre k. □

Proposición 5.4. *Sea $k \subseteq L \subseteq K$ una torre de cuerpos, entonces $K|k$ es algebraica ssi $K|L$ y $L|k$ lo son.*

Demostración. Supongamos que $K|L$ y $L|k$ son algebraicas. Esto quiere decir que si $a \in K$ entonces existe un polinomio $p(X) = a_0 + a_1X + \cdots a_nX^n \in L[X]$ tal que $p(a) = 0$ donde cada a_i es algebraico sobre k, por lo tanto a es algebraico sobre $k(a_0, a_1, a_2, \ldots a_n) = E$ Luego $E(a)|E$ es finita y como $E|k$ es finita, entonces $E(a)|k$ es finita, es decir, como

$$E(a) = k(a, a_0, a_1, a_2, \ldots a_n)$$

tenemos que a es algebraico sobre k. Concluimos notando que la recíproca es directa, y ya fue comentada al definir extensiones algebraicas. □

Observación 5.2. Sea $K|k$ es una extensión de cuerpos y α y β elementos de K algebraicos sobre k. Entonces $k(\alpha, \beta)|k$ es una extensión finita. Notemos que $\alpha+\beta \in k(\alpha, \beta)$ y que por lo tanto $k(\alpha+\beta)|k$ es finita. Luego $\alpha + \beta$ es algebraico sobre k y del mismo modo, $\alpha\beta$ es algebraico sobre k y α/β es algebraico sobre k cuando $\beta \neq 0$. Como $0, 1$ también son algebraicos sobre k, tenemos que el conjunto de los elementos algebraicos de K sobre k forman un cuerpo. Es decir, el conjunto

$$F = \{a \in K;\ a \text{ es algebraico sobre k}\}$$

es un cuerpo intermedio de la extensión $K|k$.

5.2. Cuerpos de Descomposición

Sea k un cuerpo y $p(X)$ un polinomio en $k[X]$. Un cuerpo K es un *cuerpo de descomposición de* $p(X)$ *sobre* k si $K|k$ es una extensión algebraica, $p(X)$ se descompone como $(X-a_1)(X-a_2)(X-a_3)\cdots(X-a_n)$ en $K[X]$ y $K = k(a_1, a_2, a_3, \ldots a_n)$. Es decir, si E es un cuerpo, $k \subseteq E \subseteq K$ y $p(X)$ se descompone como $(X-a_1)(X-a_2)(X-a_3)\cdots(X-a_n)$ en $E[X]$ entonces $E = K$.

Ejemplo 5.4. Si $K|k$ es una extensión de grado 2, entonces la observación **??** muestra que la extensión es simple y generada por cualquier elemento $a \in K\backslash k$. Además, si $p(X) = \text{irr}_{a,k}(X) = X^2 + bX + c \in k[X]$ entonces $(X - a)$ divide a $p(X)$ en $K[X]$ de manera que $p(X) = (X - a)q(X)$ con $q(X) \in K[X]$ de grado 1. Luego $p(X) = (X - a)(X - b) \in K[X]$, es decir, K tiene todas las raíces de $p(X) \in k[X]$. En resumen, si $K|k$ es una extensión de grado 2 entonces $K|k$ es simple y $K = k(a)$ es el cuerpo de descomposición de $p(X) = \text{irr}_{a,k}(X)$ sobre k.

Si suponemos que $\text{char}(k) \neq 2$, como a es raíz de $p(X) = X^2 + bX + c \in k[X]$ notemos que la ecuación $a^2 + ba + c = 0$ se puede escribir como

$$\left(a + \frac{b}{2}\right)^2 + c^2 - \frac{b^2}{4} = 0$$

y entonces vemos que

$$\left(a + \frac{b}{2}\right)^2 = \frac{b^2}{4} - c^2 \in k.$$

Notemos que $a + b/2 \in k$ implica que $a \in k$ lo cual es falso, de modo que $a + b/2 \in K \setminus k$ y $k(a) = k(\beta)$ donde $\beta = a + b/2$. Luego $K = k(\beta)$ con $\beta^2 \in k$. Es decir, si $K|k$ es una extensión de grado 2 con $\text{char}(k) \neq 2$ entonces $K = k(\beta)$ con $\beta^2 \in k$ y K es el cuerpo de descomposición de un polinomio de grado 2 sobre k.

Ejemplo 5.5.

- El cuerpo de los números complejos es cuerpo de descomposición de $X^2 + 1$ sobre $\mathbb{R}$, pero $\mathbb{C}$ no es el cuerpo de descomposición de $X^2 + 1$ sobre $\mathbb{Q}$ pues $\mathbb{Q}(i) = \{a + bi \in \mathbb{C};\ a, b \in \mathbb{Q}\}$ es un cuerpo estrictamente contenido en $\mathbb{C}$ que tiene todas las raíces de $X^2 + 1$.
- El cuerpo $\mathbb{Q}(\sqrt{2})$ es cuerpo de descomposición de $X^2 - 2 \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$. Pero $\mathbb{Q}(\sqrt[3]{2})$ no es cuerpo de descomposición de $X^3 - 2 \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$: en efecto, sea $\zeta = -1/2 + \sqrt{3}i/2 \in \mathbb{C} \setminus \mathbb{R}$ de manera que $\zeta^3 = 1$ y por lo tanto todas las raíces de $X^3 - 2$ en $\mathbb{C}$ son $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$ y $\sqrt[3]{2}\zeta^{-1}$. Luego el cuerpo de descomposición de $X^3 - 2$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt[3]{2}, \zeta)$. Si $\mathbb{Q}(\sqrt[3]{2}, \zeta) = \mathbb{Q}(\sqrt[3]{2})$ significaría que $\zeta \in \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ lo cual es falso. Luego $\mathbb{Q}(\sqrt[3]{2})$ no es c.d.d. de $X^3 - 2$ sobre $\mathbb{Q}$. Además notemos que

  $$[\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

  Como $X^2 + X + 1$ es un polinomio irreducible en $\mathbb{Q}[X]$ (si no lo fuese, tendrá una raíz en $\mathbb{Q}$, lo cual es falso) que tiene como raíz a ζ, entonces $[\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}(\sqrt[3]{2})]$ es 1 o 2, pero si fuese 1 se tendrá que $\zeta \in \mathbb{Q}(\sqrt[3]{2})$ lo cual es falso. Por lo tanto $[\mathbb{Q}(\sqrt[3]{2}, \zeta) : \mathbb{Q}(\sqrt[3]{2})] = 2$ y además $[\mathbb{Q}(\sqrt[3]{2}) : Q] = 3$. Concluimos que el c.d.d de $X^2 - 3$ sobre $\mathbb{Q}$ tiene grado $6 = 3!$ sobre $\mathbb{Q}$.
- Busquemos $K \subseteq \mathbb{C}$ un cuerpo de descomposición de $p(X) = X^3 + X^2 + X + 1 \in Q[X]$ sobre $\mathbb{Q}$. Notamos que $p(X) = X^2(X + 1) + X + 1 = (X^2 + 1)(X + 1)$ implica que $K = \mathbb{Q}(i)$, y entonces $[K : \mathbb{Q}] = 2$ que es menor que $6 = \text{grad}(X^3 + X^2 + X + 1)!$. Lo que si es cierto es que el grado de un c.d.d. K de un polinomio $p(X)$ sobre k no es mayor que $\text{grad}(p(X))!$, y lo probaremos más adelante.

Pese a toda esta discusión aún no demostramos que un cuerpo de descomposición de un polinomio sobre un cuerpo k exista, y es lo que haremos ahora.

Teorema 5.2. *Para cualquier cuerpo k y polinomio $p(X) \in k[X]$ de grado $n \geq 1$ existe K un c.d.d. de $p(X)$ sobre k tal que $[K : k] \leq n!$.*

Demostración. Primero demostraremos que existe un cuerpo E, tal que $E|k$ es extensión y $p(X)$ se descompone en factores lineales en $E[X]$, para lo cual haremos inducción sobre el grado de $p(X)$. Si $\text{grad}(p(X)) = 1$, entonces $p(X) = a(X - b)$ con $a, b \in k$ y $a \neq 0$ y tenemos que $E = k$.

Ahora supongamos que para todo cuerpo F y para todo polinomio $q(X)$ de grado menor que n, existe un cuerpo E en donde el polinomio $q(X)$ se descompone en factores lineales en $E[X]$, y supongamos que $\text{grad}(p(X)) = n$ en $k[X]$. Si $p(X)$ se descompone linealmente en $k[X]$, entonces $E = k$. Si $p(X)$ tiene grado n y al menos uno de sus factores irreducibles $r(X)$ es de grado mayor o igual a 2, entonces $F_1 = k[X]/(r(X))$ es un cuerpo que contiene a k y a α una raíz de $p(X)$. Luego en F_1 podemos descomponer $p(X) = (X - \alpha)q(X)$ con $q(X) \in F_1[X]$ de grado $n - 1$, entonces por hipótesis inductiva, existe un cuerpo E que contiene a F_1 (y por tanto contiene a k) y que en $F_1[X]$ el polinomio $q(X)$ se descompone en factores lineales. Concluimos que en E el polinomio $p(X) = (X - \alpha)q(X)$ se descompone en factores lineales.

Entonces hemos demostrado que para cada cuerpo k y para cada polinomio $p(X)$ en $k[X]$ existe un cuerpo E que contiene a k y $p(X)$ se descompone en factores lineales en $E[X]$.

La construcción anterior muestra que si $p(X)$ tiene grado n, la extensión $F_1 = k[X]/(r(X))$ tiene grado $\leq n$ pues $r(X)$ es un factor de $p(X)$, e inductivamente (usando que $\text{grad}(q(X)) = n-1$) vemos que podemos encontrar un tal cuerpo E que descompone a $p(X)$ tal que $[E : k] \leq n!$. Si $\{a_1, \ldots, a_r\} \subseteq E$ es el conjunto de raíces de $p(X)$ en E, entonces $K = k(a_1, \ldots a_n) \subseteq E$ implica que $[K : k] \leq [E : k] \leq n!$. □

En general, si $p(X)$ es irreducible en $E[X]$ entonces $F_1 = E[X]/p(X)$ es un cuerpo que contiene a E y tiene una raíz de $p(X)$ y además $[F_1 : E] = \text{grad}(p(X))$. Si $p(X)$ no es irreducible, tomemos una factor irreducible de $p(X)$, digamos $q(X)$, entonces $F_1 = E[X]/(q(X))$ es un cuerpo que contiene a E y tiene una raíz de $p(X)$ y $[F_1 : E] = \text{grad}(q(X)) < \text{grad}(p(X))$. Por otra parte, si $E(\alpha)|E$ es una extensión con α algebraico sobre E y $q(X)$ un polinomio de $E[X]$ tal que $q(\alpha) = 0$, entonces $\text{irr}_{\alpha,E}(X)$ divide a $q(X)$ y por lo tanto $[E(\alpha) : E] = \text{grad}(\text{irr}_{\alpha,E}(X)) \leq \text{grad}(q(X)) = [F_1 : E]$.

Demostración. Si $p(X)$ tiene grado 1 entonces $K = k$ y $[K : k] = 1 = 1!$. Supongamos que el resultado es cierto para cualquier cuerpo F y para cualquier polinomio de grado menor que n en $F[X]$, y supongamos que $p(X)$ tiene grado n en $k[X]$ y sea $K = k(a_1, a_2, a_3, \ldots, a_r)$ un c.d.d. de $p(X)$ sobre k. Por el párrafo anterior $[k(a_n) : k] \leq n$, y $p(X) = q(X)(X - a_n)$ con $q(X) \in k(a_n)[X]$ de grado $n-1$. Por la hipótesis inductiva, un c.d.d. de $q(X)$ sobre $k(a_n)$ tiene grado a lo más $(n-1)!$ sobre $k(a)$. Pero $q(X) = (X - a_1)(X - a_2)\cdots(X - a_{n-1})$ en $K[X]$. Luego $k(a_n)(a_1, a_2, \ldots, a_{n-1})$ es c.d.d. de $q(X)$ sobre $k(a_n)$ y entonces $[K : k(a_n)] \leq (n-1)!$ y $[k(a_n) : k] \leq n$. Sigue que $[K : k] \leq n!$. □

Si $\sigma : k \to k'$ es un isomorfismo de cuerpos, entonces podemos considerar $\overline{\sigma} : k[X] \to k'[X]$ definida por

$$\overline{\sigma}\left(\sum_{k=0}^{n} a_k X^k\right) = \sum_{k=0}^{n} \sigma(a_k) X^k$$

el cual es un isomorfismo de anillos y es el único tal que $\overline{\sigma}(X) = X$ y $\overline{\sigma}(a) = \sigma(a)$ para cada $a \in k$. Denotemos $\overline{\sigma}(p(X))$ por $p^\sigma(X)$. Notemos que el grado de $p(X)$ es el mismo que el grado de $p^\sigma(X)$ y que $p(X)$ es irreducible en $k[X]$ ssi $p^\sigma(X)$ lo es en $k'[X]$.

Teorema 5.3. *Sean $\sigma : k \to k'$ es un isomorfismo de cuerpos, $p(X)$ irreducible en $k[X]$ y $p^\sigma(X)$ como en el párrafo precedente. Sean α una raíz de $p(X)$ en alguna extensión de k y β una raíz de $p^\sigma(X)$ en alguna extensión de k'. Entonces existe un k-isomorfismo $\tilde{\sigma} : k(\alpha) \to k'(\beta)$ tal que $\tilde{\sigma}(\alpha) = \beta$ y $\tilde{\sigma}(a) = \sigma(a)$ para cada $a \in k$. Es decir, el siguiente diagrama conmuta:*

$$\begin{array}{ccc} k(\alpha) & \xrightarrow{\cong} & k'(\beta) \\ {\scriptstyle\iota}\uparrow & & \uparrow{\scriptstyle\iota} \\ k & \xrightarrow[\cong]{} & k' \end{array}$$

Demostración. Por lo visto en el párrafo precedente al teorema tenemos que $p^\sigma(X)$ es irreducible en $k'[X]$ cuyo grado es el mismo que el de $p(X)$. Además por teorema 5.1 se tiene que existe un único k-isomorfismo $\tau\colon k[X]/(p(X)) \to k(\alpha)$ tal que $\tau(X + p(X)) = \alpha$. Del mismo modo existe un único k'-isomorfismo $\tau'\colon k'[X]/(p^\sigma(X)) \to k'(\beta)$ tal que $\tau'(X + p^\sigma) = \beta$.

Ahora bien consideremos el isomorfismo $\overline{\sigma}\colon k[X] \to k'[X]$ definido como en el párrafo anterior al teorema, esto es, $\overline{\sigma}\left(\sum_{k=0}^n a_k X^k\right) = \sum_{k=0}^n \sigma(a_k)X^k$ y recordemos que $\overline{\sigma}(X) = X$ y $\overline{\sigma}(a) = \sigma(a)$ para cada $a \in k$. Ahora consideremos la proyección canónica $\pi\colon k'[X] \to k'[X]/(p^\sigma(X))$ definida por $\pi(q(X)) = q(X) + (p^{\sigma(X)})$ la cual es epiyectiva y notemos que $\pi(X) = X + (p^\sigma(X))$ y $\pi(a') = a'$ para cada $a' \in k'$. Por lo tanto $\phi = \pi \circ \overline{\sigma}\colon k[X] \to k'[X]/(p^\sigma(X))$ es un epimorfismo tal que $\phi(X) = X + (p^\sigma(X))$ y $\phi(a) = \sigma(a)$ para cada $a \in k$. El kernel de ϕ es el conjunto $\{q(X) \in k[X]/\ q^\sigma \in (p^\sigma(X))\} = (p(X))$. El primer teorema del isomorfismo muestra que existe un isomorfismo $\tilde{\phi}\colon k[X]/(p(X)) \to k'[X]/(p^\sigma(X))$ tal que $\tilde{\phi}(X + (p(X))) = X + (p^\sigma(X))$ y $\tilde{\phi}(a + p(X)) = \sigma(a) + (p^\sigma(X))$ para todo $a \in k$. Entonces tomemos

$$\tilde{\sigma} = \tau' \circ \tilde{\phi} \circ \tau^{-1} : k(\alpha) \to k'(\beta)$$

el cual es un isomorfismo, pues es la composición de tres isomorfismos y

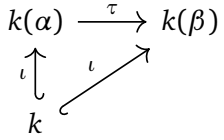
$$\tilde{\sigma}(\alpha) = \tau' \circ \tilde{\phi} \circ \tau^{-1}(\alpha) = \tau' \circ \tilde{\phi}(X + p(X)) = \tau'(X + p^\sigma(X)) = \beta$$

y si $a \in k$, entonces

$$\tilde{\sigma}(a) = \tau' \circ \tilde{\phi} \circ \tau^{-1}(a) = \tau' \circ \tilde{\phi}(a + (p(X))) = \tau'(\sigma(a) + p^\sigma(X)) = \sigma(a)$$

que es lo que queríamos demostrar. □

En el caso particular en que $k = k'$ y $\sigma = \mathrm{id}_k$, tenemos que $p^\sigma(X) = p(X)$ y α, β son raíces de $p(X)$, y entonces existe un isomorfismo $\tau\colon k(\alpha) \to k(\beta)$ tal que $\tau(\alpha) = \beta$ y $\tau(a) = a$ para cada $a \in k$, es decir τ es un k-isomorfismo. Lo podemos ver en el siguiente diagrama conmutativo:



Generalicemos el teorema anterior al caso en que se quiera extender un isomorfismo, no a $k(\alpha)$ sino que a todo un cuerpo de descomposición.

Teorema 5.4. *Sean $\sigma\colon k \to k'$ un isomorfismo de cuerpos, $p(X)$ un polinomio en $k[X]$ y $p^\sigma(X)$ como en el teorema anterior. Sean también K un c.d.d. de $p(X)$ sobre k y K' un c.d.d. de $p^\sigma(X)$ sobre k'. Entonces existe un isomorfismo $\tilde{\sigma}\colon K \to K'$ tal que $\tilde{\sigma}(a) = \sigma(a)$ para cada $a \in k$. Es decir, existe $\tilde{\sigma}\colon K \to K'$ isomorfismo tal que el diagrama conmuta:*

$$\begin{array}{ccc} K & \xrightarrow{\cong} & K' \\ {\scriptstyle\iota}\uparrow & & \uparrow{\scriptstyle\iota} \\ k & \xrightarrow[\cong]{} & k' \end{array}$$

Demostración. Haremos inducción sobre el grado de $p(X)$. Si $\text{grad}(p(X)) = 1$, entonces $K = k$ y $K' = k'$ y $\tilde{\sigma} = \sigma$. Si $p(X)$ tiene grado n y se descompone linealmente en $k[X]$, entonces $K = k$, $K' = k'$ y $\tilde{\sigma} = \sigma$. Si $p(X)$ tiene grado n y tiene algún factor irreducible de grado mayor o igual a 2 y sabemos que el teorema se cumple para cualquier $\sigma : k \to k'$ isomorfismo y para cualquier $f(X)$ de grado menor que n entonces sea $r(X) \in k[X]$ un factor irreducible de $p(X)$ con $\text{grad}(r(X)) \geq 2$. Luego $r^{\sigma}(X)$ es un factor irreducible de $p^{\sigma}(X)$. Sea $\alpha \in K$ una raíz de $r(X)$ y $\beta \in K'$ una raíz de $r^{\sigma}(X)$. Por el teorema anterior existe un isomorfismo $\tau : k(\alpha) \to k'(\beta)$ tal que $\tau(\alpha) = \beta$ y el diagrama conmuta:

$$\begin{array}{ccc} k(\alpha) & \xrightarrow{\tau} & k'(\beta) \\ {\scriptstyle\iota}\uparrow & & \uparrow{\scriptstyle\iota} \\ k & \xrightarrow[\sigma]{} & k' \end{array}$$

En $k(\alpha)$ podemos descomponer $p(X) = (X - \alpha)q(X)$ con $q(X)$ de grado $n-1$ y en $k'(\beta)$ podemos descomponer $p(X) = (X - \beta)q'(X)$ donde $q^{\tau}(X) = q'(X)$. Sea E el c.d.d. de $q(X)$ sobre $k(\alpha)$ de manera que $k(\alpha) \subseteq E \subseteq K$ y además $E = k(\alpha)(a_1, a_2, \ldots a_r)$ con los a_i raíces de $q(X)$. Luego $E = k(\alpha, a_1, a_2, \ldots a_r)$ donde $\alpha, a_1, a_2, \cdots a_r$ son raíces de $p(X)$, entonces $E = K$. Del mismo modo K' es el c.d.d. de $q'(X)$ sobre $k'(\beta)$. Entonces por hipótesis inductiva existe un isomorfismo $\tilde{\sigma} : K \to K'$ tal que $\tilde{\sigma}(a) = \tau(a) = \sigma(a)$ para cada $a \in k$. Es decir, podemos extender el diagrama anterior a

$$\begin{array}{ccc} K & \xrightarrow{\tilde{\sigma}} & K' \\ {\scriptstyle\iota}\uparrow & & \uparrow{\scriptstyle\iota} \\ k(\alpha) & \xrightarrow{\tau} & k'(\beta) \\ {\scriptstyle\iota}\uparrow & & \uparrow{\scriptstyle\iota} \\ k & \longrightarrow & k' \end{array}$$

Esto completa la demostración. □

En el caso particular en que $k = k'$ y σ es la identidad, entonces $p^{\sigma}(X) = p(X)$ y tenemos que K y K' son dos cuerpos de descomposición de $p(X)$ sobre k. El teorema anterior garantiza la existencia de un k-isomorfismo $\tilde{\sigma} : K \to K'$. Dejémoslo escrito como corolario.

Corolario 5.1. *Si k es un cuerpo, $p(X)$ es un polinomio en $k[X]$, K y K' son cuerpos de descomposición de $p(X)$ sobre k, entonces K y K' son k-isomorfos.*

Luego el c.d.d. de un polinomio sobre un cuerpo es único salvo isomorfismos, y hablaremos de el cuerpo de descomposición de un polinomio sobre un cuerpo.

Teorema 5.5. *Para cada p primo y n natural, existe un único cuerpo salvo isomorfismos ($\mathbb{F}_p$-isomorfismos) de $q = p^n$ elementos.*

Demostración. Sea K es el cuerpo de descomposición de $p(X) = X^q - X \in \mathbb{F}_p[X]$ sobre $\mathbb{F}_p$. Entonces el conjunto $E = \{a \in \mathbb{F};\ a^q = a\}$ de las raíces de $p(X)$ en K es un cuerpo pues, como K tiene característica p (al contener a $\mathbb{Z}_p$), $a \mapsto a^q$ es morfismo. Por lo tanto $E = K$. Además el polinomio $X^q - X$ tendrá exactamente q raíces en $K = E$ ssi $p(X)$ no tiene raíces múltiples, pero $p'(X) = -1 \in \mathbb{F}_p[X]$ y luego $p(X)$ no tiene raíces múltiples. Entonces $|E| = q = p^n$, es decir, para cada primo p y para cada n natural, existe un cuerpo con p^n elementos. Además, si $\mathbb{F}$ es un cuerpo con $q = p^n$ elementos entonces necesariamente es de característica p y contiene al cuerpo primo de p elementos, es decir $\mathbb{F}_p \subseteq \mathbb{F}$. Notemos que $\mathbb{F}^\times$ es un grupo de $q-1$ elementos y por lo tanto para cada $a \in \mathbb{F}^\times$ se cumple que $a^{q-1} = 1$, o $a^q 0 a$. pero además $a = 0$ también satisface $a^q - a$. Es decir, todo elemento de $\mathbb{F}$ es raíz del polinomio $X^q - X$, de manera que $\mathbb{F}$ es c.d.d. de $X^q - X$. Podemos concluir recordando que el cuerpo de descomposición es único salvo isomorfismos. □

Notemos que en general el morfismo de Frobenius $a \in K \mapsto a^q \in K$ es un $\mathbb{F}_p$-automorfismo cuando K es finito y tiene característica p, de modo que $K^q \doteq \{a^q;\ a \in K\} = K$.

En el teorema anterior usamos el siguiente resultado del capítulo 3, que enunciamos nuevamente por conveniencia. Notemos que la derivada de un polinomio en $k[X]$ es la misma que si consideramos al mismo polinomio en $K[X]$ donde $K|k$ es una extensión de cuerpos.

Teorema 5.6. *Un polinomio $p(X) \in k[X]$ tiene raíces múltiples en E un c.d.d. de $p(X)$ sobre k si y solo si $p(X)$ y $p'(X)$ tienen raíces comunes.*

Ejemplo 5.6. Si $p(X) = X^9 + X^3 + 1$ entonces $p'(X) = 9X^8 + 3X^2$ si consideramos a $p(X)$ en $\mathbb{Q}[X]$, pero $p'(X) = 0$ si consideramos a $p(X) \in \mathbb{F}_3[X]$. De hecho, $p(X) = (X^3 + X + 1)^3 \in \mathbb{F}_3[X]$.

Más generalmente, si K un cuerpo de característica p tal que $K^p = K$, consideremos $p(X) \in K[X]$ tal que $p'(X) = 0$. Escribamos

$$p(X) = a_0 + a_1 X^{r_1} + a_1 X^{r_2} + a_3 X^{r_3} + \cdots a_n X^{r_n}.$$

con $a_k \neq 0$ para cada k y $0 < r_1 < r_2 < r_3 < \cdots r_n$ números naturales. Entonces como $D_K(p(X)) = 0$, se tiene que $a_t r_t = 0$ para cada t y como $a_t \neq 0$ obtenemos que cada r_t es un múltiplo de p. Escribamos $r_t = k_t p$ de manera que

$$p(X) = a_0 + a_1 X^{k_1 p} + a_2 X^{k_2 p} + a_3 X^{k_3 p} + \cdots + a_n X^{k_n p}.$$

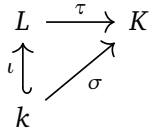
Como $a_i \in K = K^p$ podemos encontrar $b_i \in K$ tal que cada $(b_i)^p = a_i$, entonces

$$p(X) = (b_0)^p + (b_1X^{k_1})^p + (b_2X^{k_2})^p + (b_3X^{k_3})^p + \cdots + (b_nX^{k_n})^p = (q(X))^p$$

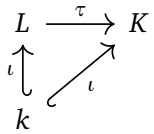
donde $q(X) = b_0 + b_1X^{k_1} + b_2X^{k_2} + b_3X^{k_3} + \cdots + b_nX^{k_n} \in K[X]$. Luego $p(X)$ no puede ser irreducible.

5.3. Inmersiones y Clausura Algebraica

Si k y K son cuerpos y $\sigma : k \to K$ un morfismo de anillos, entonces σ es un monomorfismo. A tal monomorfismo también le llamaremos *inmersión de k en K*. Si $L|k$ es una extensón de cuerpos $\tau : L \to K$ tal que $\tau(a) = \sigma(a)$ para cada $a \in k$ diremos que τ es una inmersión que *extiende* a σ, y también diremos que τ es una *inmersión que va sobre σ*.

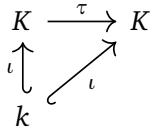


En el caso particular en que $K|k$ es una extensión y σ es la inclusión, tenemos que τ es un k-monomorfismo. En tal caso diremos que τ extiende a la inclusión y que τ *va sobre k*.



A continuación presentamos el primer resultado referente a inmersiones.

Teorema 5.7. *Sea $K|k$ una extensión algebraica y $\sigma : K \to K$ una inmersión que va sobre k, entonces σ es un k-automorfismo.*



Demostración. Basta demostrar que σ es epiyectivo, pues ya sabemos que es un k-monomorfismo.

Sea $a \in K$, como $K|k$ es algebraico podemos tomar $p(X) = \text{irr}_{a,k}(X) = \sum_{k=0}^{n} a_kX^k$ el polinomio irreducible de a en $k[X]$. Dado que $p(a) = \sum_{k=0}^{n} a_ka^k = 0$, aplicando σ se tiene que $\sum_{k=0}^{n} a_k\sigma(a)^k = 0$ pues $\sigma(a_i) = a_i \in k$. Por lo tanto σ transforma raíces de $p(X)$ en raíces de $p(X)$. Entonces si $X = \{a = a_1, a_2, a_3, \ldots, a_n\}$ es

el conjunto de las raíces de $p(X)$ en K, la función $\overline{\sigma} : X \to X$ definida por $\overline{\sigma}(X) = \sigma(X)$ está bien definida y es inyectiva, ya que σ lo es. Como X es finito, se tiene que $\overline{\sigma}$ es biyectiva, y por lo tanto existe $a_j \in X \subseteq K$ tal que $\overline{\sigma}(a_j) = \sigma(a_j) = a_1 = a$. Es decir, $a \in \sigma(K)$ y concluimos que $K = \sigma(K)$, que es lo que queríamos probar. □

Consideremos ahora una inmersión $\sigma : k \to E$ y $a \in K$ algebraico, con $K|k$ una extensión y $p(X) = \text{irr}_{a,k}(X)$, consideremos $p^\sigma(X) \in E[X]$, como en el teorema (5.3). En realidad $p^\sigma(X) \in k'[X]$, donde k' es el cuerpo $\sigma(k) \subseteq E$ que es isomorfo a k, entonces para cada $b \in E$ raíz de $p^\sigma(X)$ existe un isomorfismo $\tilde{\sigma} : k(a) \to k'(b)$ por teorema (5.3), tal que $\tilde{\sigma}(a) = b$ y $\tilde{\sigma}(\alpha) = \sigma(\alpha)$, $\forall \alpha \in k$. Por lo tanto $\tau_b : k(a) \to E$ definida por $\tau_b(X) = \tilde{\sigma(x)}$ es un monomorfismo tal que $\tau_b(a) = b$ y $\tau_b(\alpha) = \sigma(\alpha)$, $\forall \alpha \in k$. Es decir, τ_b es una inmersión de $k(a)$ a E que extiende a σ y manda a a b. Además si $\tau : k(a) \to E$ es una inmersión que va sobre σ, entonces si $p(X) = \sum_{k=0}^{n} a_k X^k$, con $a_k \in k$, entonces $0 = \sum_{k=0}^{n} a_k a^k$ aplicando τ se tiene que

$$0 = \sum_{k=0}^{n} \tau(a_k)\tau(a)^k = \sum_{k=0}^{n} \sigma(a_k)\tau(a)^k = p^\sigma(\tau(a))$$

es decir $\tau(a) = b$ con b raíz de $p^\sigma(X)$. Pero $\tau_b : k(a) \to E$ es una inmersión sobre σ y $\tau_b(a) = b$. ¿Será que $\tau = \tau_b$? Recordemos que como a es algebraico sobre k, entonces $k(a) = k[a]$, entonces si $c \in k(a)$ entonces existen finitos $c_k \in k$ tal que

$$c = \sum_{k=0}^{n} c_k a^k$$

entonces

$$\tau(c) = \sum_{k=0}^{n} \tau(c_k)(\tau(a))^k = \sum_{k=0}^{n} \sigma(c_k) b^k$$

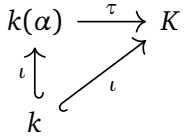
y del mismo modo

$$\tau_b(c) = \sum_{k=0}^{n} \tau_b(c_k)(\tau_b(a))^k = \sum_{k=0}^{n} \sigma(c_k) b^k$$

es decir $\tau = \tau_b$. Entonces tenemos el siguiente teorema:

Teorema 5.8. *Sea $K|k$ una extensión y $\sigma : k \to E$ una inmersión y $a \in K$ algebraico sobre k. Si $p(X) = \text{irr}_{a,k}(X)$, entonces para cada raíz $b \in E$ de $p^\sigma(X)$ existe una única inmersión $\tau_b : k(a) \to E$ que extiende a σ y $\tau_b(a) = b$. Además toda extensión $\tau : k(a) \to E$ de σ es igual a τ_b para cierto b raíz de p^σ en E.*

Observación 5.3. En el caso particular en que $K = E$ y σ es la inclusión, $a \in K$ y $p(X) = \text{irr}_{a,k}(X)$, entonces $p^\sigma(X) = p(X)$. Entonces existen tantas inmersiones τ sobre k como raíces distintas de $p(X)$ hay en K.



Un cuerpo K se dice *algebraicamente cerrado* si todo polinomio $p(X) \in K[X]$ de grado mayor o igual a 1 tiene raíces en K. De hecho, si K es algebraicamente cerrado, entonces K tiene todas las raíces de todos los polinomios de grado mayor o igual a 1 en $K[X]$. La siguiente proposición permite definir de varias maneras esta noción

Proposición 5.5. *Sea K un cuerpo. Las siguientes afirmaciones son equivalentes:*

1. *K es algebraicamente cerrado.*
2. *K no admite extensiones algebraicas salvo la trivial.*
3. *Todo polinomio irreducible $p(X) \in K[X]$ tiene grado 1.*
4. *Todo polinomio $p(X) \in K[X]$ de grado positivo se descompone en factores lineales en $K[X]$.*

Demostración. La equivalencia 3 $\iff$ 4 es directa pues $K[X]$ es un DFU, y la equivalencia 1 $\iff$ 4 también lo es ya que $\alpha \in K$ es raíz de $p(X) \in K[X]$ ssi $(X-\alpha)$ divide a $p(X)$ en $K[X]$. Veamos que 1 $\iff$ 2: si K es algebraicamente cerrado y $F|K$ es una extensión algebraica, entonces para cada $a \in F$, K tiene todas las raíces de $\mathrm{irr}_{a,k}(X) \in K[X]$. Es decir, $a \in K$, y luego $F = K$. Recíprocamente, sea K es un cuerpo que no admite extensiones algebraicas salvo la trivial. Dado $p(X) \in K[X]$, recordemos si E es el c.d.d. de $p(X)$ sobre K, entonces $E|K$ es finita y por lo tanto algebraica. Luego $E = K$ y K contiene todas las raíces de $p(X)$. □

Observación 5.4. Si $K = \{a_1, \ldots, a_n\}$ es un cuerpo finito, entonces el polinomio

$$p(X) = 1 + \prod_{k=1}^{n} (X - a_k) \in K[X]$$

es tal que $p(a) = 1$ para cada $a \in K$ y por lo tanto $p(X)$ no tiene raíces en K. Es decir, de existir cuerpos algebraicamente cerrados, estos son infinitos.

Si k es un cuerpo, $\overline{k}$ es un cuerpo algebraicamente cerrado y $\overline{k}|k$ una extensión algebraica, entonces diremos que $\overline{k}$ es una *clausura algebraica* de k.

Observación 5.5. Sea $K|k$ algebraica tal que todo polinomio de grado mayor o igual a 1 en $k[X]$ tiene raíces en K, de manera que todo polinomio de grado mayor o igual a 1 en $k[X]$ tiene todas sus raíces en K. Consideremos $F|K$ una extensión algebraica y notemos que $F|k$ también es una extensión algebraica. Si $a \in F$, entonces a satisface un polinomio $p(X) \in k[X]$, pero K contiene todas las raíces de $p(X)$, es decir $a \in K$. Por lo tanto $F = K$. Es decir, K no admite extensiones algebraicas salvo él mismo y por lo tanto K es algebraicamente cerrado. Es decir K es una clausura algebraica de k.

Ahora sea $K|k$ una extensión y K algebraicamente cerrado. Definamos

$$\overline{k} = \{a \in K;\ a \text{ es algebraico sobre } k\}.$$

Es claro que $\overline{k}$ es un cuerpo y $\overline{k}|k$ es una extensión algebraica. Ahora sea $p(X)$ un polinomio en $k[X]$ de grado mayor o igual a 1. Como K es alg. cerrado, tomemos todas las raíces de $p(X)$ en K, pero todas esas raíces son algebraicas sobre k y entonces están en $\overline{k}$. Por lo tanto $\overline{k}$ es un cuerpo algebraico sobre k y tiene todas las raíces de todos los polinomios de grado mayor o igual a 1 en $k[X]$, y por el párrafo anterior concluimos que $\overline{k}$ es una clausura algebraica de k.

Para que todas estás observaciones no queden en el vacío tenemos que demostrar que las clausuras algebraicas existen, y lo haremos a continuación. Además demostraremos que las clausuras algebraicas son únicas, salvo isomorfismos. Antes de eso probemos el siguiente corolario del teorema 5.8.

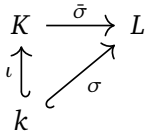
Corolario 5.2. *Si $K|k$ es una extensión algebraica y $\sigma : k \to L$ es una inmersión con L alg.cerrado, entonces existe una inmersión $\tilde{\sigma} : K \to L$ sobre σ. Si además K es alg. cerrado y L es algebraico sobre $\sigma(k)$, entonces $\tilde{\sigma}$ es isomorfismo.*

Demostración. Sea $A = \{(F, \mu); k \subseteq F \subseteq K,\ \mu : F \to L$ inmersión que va sobre $\sigma\}$. Notemos primero que A no es vacío pues $(k, \sigma) \in A$. Definamos un orden parcial en A por $(F_1, \mu_1) \leq (F_2, \mu_2)$ ssi $F_1 \subseteq F_2$ y $(\mu_2)_{|F_1} = \mu_1$. Tomemos una cadena $\mathscr{C} = \{(F_\lambda, \mu_\lambda)\}_{\lambda \in \Lambda}$ en $(A, \leq)$ y definamos

$$E = \bigcup_{\lambda \in \Lambda} F_\lambda.$$

Es directo ver que E es un cuerpo intermedio de la extensión $K|k$. Definamos $\mu : E \to L$ por $\mu(a) = \mu_\lambda(a)$ si $a \in F_\lambda$, que está bien definida ya que los λ están bien ordenados. Como para todo $\lambda \in \Lambda$ se tiene que $(\mu_\lambda)_{|k} = \sigma$, entonces $\mu_{|k} = \sigma$. Luego (E, μ) está en A y es cota superior de $\mathscr{C}$. Por el lema de Zorn, existe un elemento maximal de A.

Sea $(F, \tilde{\sigma})$ elemento maximal de A. Si F está contenido propiamente en K, tomemos $a \in K \setminus F$. Por el teorema 5.3 existe una extensión de $\tilde{\sigma}$ de $K(a)$ a L pues a es algebraico sobre K y L contiene las raíces de $p^{\tilde{\sigma}}$ donde $p(X) = \mathrm{irr}_{a,k}(X)$. Esto contradice la maximalidad de $(F, \tilde{\sigma})$, y concluimos que $K = F$ y $\tilde{\sigma}$ es la extensión que buscábamos.



Ahora bien, notemos que $\sigma(k) \subseteq \tilde{\sigma}(K) \subseteq L$, y si K es algebraicamente cerrado, entonces $\tilde{\sigma}(K)$ es algebraicamente cerrado. Como L es algebraico sobre $\sigma(k)$, entonces L es algebraico sobre $\tilde{\sigma}(K)$, pero un cuerpo algebraicamente cerrado no admite extensiones algebraicas salvo la trivial, y por lo tanto $\tilde{\sigma}(K) = L$. Es decir, $\tilde{\sigma}$ es un isomorfismo que extiende a σ. □

Consideremos el caso particular en que K y $\overline{k}$ son clausuras algebraicas de k, esto es K y $\overline{k}$ son algebraicamente cerrados y tanto $K|k$ como $\overline{k}|k$ son algebraicas. En el teorema anterior tomemos $L = \overline{k}$ y σ como la inclusión $\iota : k \to \overline{k}$, de manera que $\sigma(k) = k$ y $L = \overline{k}$ es algebraico sobre $\sigma(k) = k$. Luego existe $\tilde{\sigma} : K \to \overline{k}$ isomorfismo que extiende a ι, es decir, es k-isomorfismo. Hemos probado el siguiente corolario, y entonces podemos hablar de la clausura algebraica de un cuerpo.

Corolario 5.3. *Dos clausuras algebraicas de k son k-isomorfas.*

Ahora demostremos la existencia. Para ello construyamos un anillo de polinomios con un número cualquiera de variables sobre el cuerpo k. Ya vimos una construcción de este tipo en el capítulo 3, y ahora daremos otra. Consideremos k un cuerpo y $S = \{X_\lambda\}_{\lambda\in\Lambda}$ un conjunto no vacío al cual llamaremos conjunto de variables. Definamos los monomios como

$$\mathscr{F} = \{\mu : \Lambda \to \mathbb{N};\ \mu \text{ de soporte finito}\}$$

es decir, si $\mu \in \mathscr{F}$ entonces $S_\mu \doteq \{\lambda \in \Lambda;\ \mu(\lambda) \neq 0\}$ es finito. Definamos una suma en $\mathscr{F}$ punto a punto, es decir $(\mu + \eta)(\lambda) = \mu(\lambda) + \eta(\lambda)$. Esta suma está bien definida, es asociativa, conmutativa y tiene como neutro a la función identicamente nula. Si $\mu \in \mathscr{F}$, entonces el conjunto $S_\mu = \{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ es finito, y consideremos las variables asociadas a esos elementos $X_{\lambda_1}, X_{\lambda_2}, \ldots X_{\lambda_n}$ en S. Definimos la *palabra* X^μ (que representa a μ) como $X^\mu = X_{\lambda_1}^{\mu(\lambda_1)} X_{\lambda_2}^{\mu(\lambda_2)} \cdots X_{\lambda_n}^{\mu(\lambda_n)}$. Si μ es la función nula entonces X^μ lo denotamos por 1 y en ese caso escribimos $X^0 = 1$. Sea $[S] = \mathscr{F}$ el conjunto de todas las palabras X^μ, entonces definimos $k[S]$ como el espacio vectorial sobre k con base $[S]$. Equivalentemente, $k[S]$ es el conjunto de funciones $\phi : [S] \to k$ de soporte finito.

Si definimos una multiplicación en $[S]$ por $X^\mu X^\lambda = X^{\mu+\lambda}$, podemos extender el producto de $[S]$ a $k[S]$ para obtener una estructura de anillo conmutativo sobre $k[S]$. Consideremos el monomorfismo $\iota : k \to k[S]$ por $a \to a1$ de modo que $\iota(k)$ es una copia isomorfa de k en $k[S]$. Además, para cada $\lambda \in \Lambda$ consideremos $\mu_\lambda \in \mathscr{F}$ tal que $\mu_\lambda = 1$ y 0 en todo el resto de Λ. Denotaremos este X^{μ_λ} como X_λ.

Teorema 5.9. *Si k es un cuerpo, entonces existe una clausura algebraica de k.*

Demostración. Basta con construir una extensión $K|k$ tal que K sea algebraicamente cerrado, pues la observación 5.5 muestra que $\overline{k} = \{a \in K;\ a \text{ algebraico sobre } k\}$ es una clausura algebraica de k.

Sea Λ el conjunto de todos los polinomios de grado mayor o igual a 1 en $k[X]$. Consideremos $S = \{X_\lambda\}_{\lambda\in\Lambda}$ un conjunto de variables y el anillo $R = k[S]$ como en el párrafo anterior. Sea $f(X) \in k[X]$, entonces podemos considerar el polinomio $f(X_f) \in R$. Sea I el ideal generado por $\{f(X_f);\ f \in \Lambda\}$ en R. Por definición $I \neq \{0\}$.

Afirmamos que I tampoco es todo R. Efectivamente, si $I = R$ entonces $1 \in I$ y existen finitos $f_i \in \Lambda$ y finitos g_i en R tales que

$$g_1 f_1(X_{f_1}) + g_2 f_2(X_{f_2}) + g_3 f_3(X_{f_3}) + \cdots + g_n f_n(X_{f_n}) = 1 \tag{5.1}$$

Denotemos cada X_{f_i} por X_i. Como cada g_i involucra solo un número finito de variables, entonces en la relación 5.1 participa un conjunto finito de variables $\{X_1, X_2, \ldots, X_n, X_{n+1}, X_{n+2}, \ldots, X_{n+m}\}$. Sea E el cuerpo

de descomposición de $f(X) = f_1(X)f_2(X)\cdots f_n(X)$ sobre k y sea a_i una raíz de $f_i(X)$ en E. Reemplazando en 5.1 X_i por a_i para $i \in [n]$ y $X_{n+k} = 0$ para $k \in [m]$, la ecuación se reduce a $1 = 0$ en E lo cual es una contradicción. Luego $\{0\} \neq I \neq R$.

Sea M ideal maximal que contiene a I. Entonces $F_1 = R/M$ es un cuerpo que contiene a una copia de k y tal que cada polinomio $p(X) \in k[X]$ de grado mayor o igual a 1 tiene una raíz $X_p + M \in F_1$. Repitiendo la construcción anterior para F_1 e iterando, obtenemos una cadena de cuerpos

$$k = F_0 \subseteq F_1 \subseteq F_2 \subseteq F_3 \ldots \subseteq F_n \subseteq F_{n+1} \subseteq \ldots$$

tal que cada polinomio de grado mayor o igual a 1 sobre F_n tiene raíces en F_{n+1} y además cada F_n contiene a k. Sea

$$K = \bigcup_{n\in\mathbb{N}} F_n,$$

y notemos que es un cuerpo que contiene a k tal que para cada polinomio $p(X) \in K[X]$ existe $n \in \mathbb{N}$ tal que $p(X) \in F_n[X]$, y por lo tanto tiene una raíz en $F_{n+1} \subseteq K$. Es decir, $K|k$ es una extensión y K es algebraicamente cerrado. □

Ejemplo 5.7. Sea $\overline{\mathbb{Q}}$ la clausura algebraica de $\mathbb{Q}$. Si $n \in \mathbb{N}$, entonces el criterio de Eisenstein muestra que $p(X) = X^n - 2$ es irreducible. Sea α_n una raíz de $p(X)$ en $\overline{\mathbb{Q}}$ y notemos que $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\alpha_n) : \mathbb{Q}] = n$. Como esto ocurre para todo n natural, entonces $\overline{\mathbb{Q}}|\mathbb{Q}$ es una extensión algebraica infinita. Además $\overline{\mathbb{Q}}$ es numerable y por lo tanto $\mathbb{R}|\mathbb{Q}$ es trascendente.

5.4. Extensiones Galoisianas

En este apartado estudiaremos extensiones Galosianas finitas. Esto es una extensión $K|k$ finita (por lo tanto algebraica) que es normal y separable. La normalidad tiene que ver con que K es c.d.d. de algún polinomio y la separabilidad tiene que ver con que las raíces de los polinomios irreducibles de $k[X]$ que tienen raíces en K no tengan raíces múltiples. Partamos definiendo separabilidad.

5.4.1. Extensiones Separables

Sea k un cuerpo. Un polinomio irreducible $p(X) \in k[X]$ se dice *separable* si no tiene raíces multiples en la clausura algebraica de k. Un polinomio $p(X) \in k[X]$ se dice separable si los factores irreducibles de $p(X)$ son separables. Ahora sea $K|k$ una extensión y $a \in K$ algebraico sobre k. Diremos que a es separable sobre k si $\mathrm{irr}_{a,k}(X) = p(X)$ es separable en $k[X]$. Lo anterior es equivalente a decir que a satisface un polinomio separable en $k[X]$. Una extensión algebraica $K|k$ se dice separable si todo elemento de K es separable sobre k.

Observación 5.6. Sea k un cuerpo de característica 0 y $K|k$ una extensión algebraica. Sea $a \in K$ y $p(X) = \mathrm{irr}_{a,k}(X)$, vale recordar que $p(X)$ es el polinomio de grado mínimo mónico en $k[X]$, tal que $p(a) = 0$.

Si $p(X)$ no es separable, entonces existe una raíz b (en la clausura algebraica $\overline{k}$ de k) de $p(X)$ que es múltiple. Notemos en tal caso su derivada $p'(X)$ tiene a b como raíz, pero $p'(X)$ es un polinomio no nulo de grado menor que el grado de $p(X)$ que anula a b lo cual es una contradicción. Por lo tanto a es separable sobre k, es decir, toda extensión algebraica sobre un cuerpo de característica cero es separable.

Vimos también en un ejemplo anterior, que si K es un cuerpo de característica p, con p primo y $K = K^p$, entonces todo polinomio irreducible de $K[X]$ es separable. Luego toda extensión algebraica de K es separable. En particular, si K es finito de característica p, entonces $K = K^p$, y toda extensión algebraica de un cuerpo finito es separable. Luego $\mathbb{F}_q|\mathbb{F}_p$ es separable cuando $q = p^n$.

Observación 5.7. Sea $K|k$ es una extensión algebraica y separable, y sea $k \subseteq F \subseteq K$ un cuerpo intermedio. Si $a \in F \subseteq K$ entonces $\operatorname{irr} a, k(X)$ es separable pues $K|k$ es separable. Entonces $F|k$ es separable. Si $a \in K$ entonces $\operatorname{irr}_{a,F}(X)$ divide a $\operatorname{irr}_{a,k}(X)$, y como $\operatorname{irr}_{a,k}(X)$ es separable, entonces $\operatorname{irr}_{a,F}(X)$ también lo es. Por lo tanto $K|F$ también es separable. El recíproco es un ejercicio.

Ejemplo 5.8. Sea k un cuerpo y $K = k(X)$ el cuerpo de las funciones racionales sobre k. Si $(p(X)/q(X))^2 = X$ con $p(X)$ y $q(X)$ polinomios no nulos en $k[X]$, entonces $p^2(X) = Xq^2(X)$ y el grado de $p^2(X)$ es a la vez par e impar, por lo tanto X no es un cuadrado en K. Sea $p(Z) = Z^2 - X \in K[Z]$ de modo que $p(Z)$ es irreducible en $K[Z]$ pues tiene grado 2 y no tiene raíces en K, luego $F = K[z]/(p(z))$ es un cuerpo, $[F : K] = 2$ y hay un elemento α en F tal que $\alpha^2 = X$. Por lo tanto en F el polinomio $p(Z)$ se descompone como $p(Z) = (Z - \alpha)(Z + \alpha)$. Si k tiene característica 2, entonces $p(Z)$ se descompone como $(Z - \alpha)(Z + \alpha) = (Z - \alpha)^2 \in F$ pues en este caso se cumple que $-\alpha = \alpha$, y por lo tanto se tiene que $F|K$ no es separable.

Es fácil generalizar el argumento anterior: si K es un cuerpo de característica p y contiene un elemento a que no es una p-ésima potencia (por ejemplo X en si $K = k(X)$), entonces el polinomio $p(X) = X^p - a$ es irreducible, pero en un c.d.d. de $p(X)$ tenemos que $X^p - a = (X - \alpha)^p$ donde α es tal que $\alpha^p = a$. Luego K no es separable.

5.4.2. Extensiones Normales

Ya definimos el c.d.d. de un polinomio $p(X)$ en $k[X]$ esto es un cuerpo K que contiene a k, contiene a todas las raíces de $p(X)$ y además si $k \subseteq E \subseteq K$ tal que E contiene a todas las raíces de $p(X)$, entonces $E = K$. Es decir, $K = k(a_1, a_2, \cdots, a_n)$, donde $\{a_i\}_{i=1}^n$ es el conjunto de todas las raíces de $p(X)$.

Sea ahora una familia de polinomios $\mathscr{F} = \{f_\lambda(X)\}_{\lambda \in \Lambda} \subseteq k[X]$ de grado mayor o igual a 1 y sea $\overline{k}$ la clausura algebraica de k. Sea $S \subseteq \overline{k}$ el conjunto de todas las raíces de los polinomios de $\mathscr{F}$ en $\overline{k}$, entonces a $k(S)$ le llamamos c.d.d de $\mathscr{F}$ sobre k. Si $k \subseteq E \subseteq K$, y E contiene todas las raíces de los polinomios de $\mathscr{F}$, entonces $K = E$.

Observación 5.8. La clausura algebraica de k es un c.d.d. Dos c.d.d de una misma familia de polinomios sobre k son isomorfos.

El siguiente teorema permite definir extensión normal de una forma cómoda.

Teorema 5.10. *Sea $K|k$ algebraica. Entonces las siguientes propiedades son equivalentes:*

1. *K es c.d.d. de una familia de polinomios irreducibles de $k[X]$.*
2. *Todo polinomio irreducible $p(X)$ que tiene una raíz en K, se descompone linealmente en $K[X]$.*
3. *Si $\overline{k}$ es una clausura algebraica de k que contiene a k y $\sigma: K \to \overline{k}$ una inmersión sobre k, entonces $\sigma(K) = K$.*

Demostración. Probemos $2 \Rightarrow 1$: Sea $\mathscr{F}$ la familia de polinomios irreducibles en $k[X]$ que tienen raíces en K. Entonces K contiene todas las raíces de $\mathscr{F}$. Sea S el conjunto de raíces de los polinomios de $\mathscr{F}$ en K y sea $E = k(S)$. Tenemos que $k \subseteq E \subseteq K$. Si $E \neq K$, entonces existe $a \in K \setminus E$. Como $K|k$ es algebraico, existe un polinomio irreducible $p(X) \in k[X]$ tal que $p(a) = 0$, luego $p(X) \in \mathscr{F}$ y $a \in S \subseteq E$. Entonces $K = E$, el c.d.d. de $\mathscr{F}$.

$3 \Rightarrow 2$: Sea $p(X) \in k[X]$ un polinomio irreducible que tiene una raíz en K, sin restricción podemos suponer que $p(X)$ es mónico. Sea $a \in K$ una de esas raíces de $p(X)$ en K y sean $\{a_1 = a, a_2, a_3 \cdots, a_n\}$ todas las raíces de $p(X)$ en $\overline{K}$, la clausura algebraica de K. Como $K|k$ es algebraica, entonces $\overline{K}$ también es la clausura algebraica de k. El teorema 5.3 muestra que existe una inmersión $\tau_{a_2}: K \to \overline{K}$ sobre k tal que $\tau_{a_2}(a) = a_2$. Como $a \in K$, por hipótesis tenemos que $a_2 = \tau_{a_2}(a) \in K$. Del mismo modo $a_k \in K$ para cada $k \in [n]$. Luego en $K[X]$ el polinomio $p(X)$ se descompone en factores lineales.

$1 \Rightarrow 3$: Sea $\sigma: K \to \overline{k}$ un k-monomorfismo y escribamos $k(X) = K$, donde X es el conjunto de raíces de una familia de polinomios $\mathscr{F}$ en $k[X]$. Probemos primero que $\sigma(K) \subseteq K$, para eso basta demostrar que $\sigma(X) \subseteq X$. Sea $a \in X$, entonces existe polinomio $p(X) \in \mathscr{F}$ tal que $p(a) = 0$. Si $p(X) = \sum_{j=0}^{n} b_j X^j$ con $b_j \in k$, entonces

$$\sigma(0) = 0 = \sigma\left(\sum_{j=0}^{n} b_j a^j\right) = \sum_{j=0}^{n} \sigma(b_j)(\sigma(a))^j = \sum_{j=0}^{n} b_j (\sigma(a))^j.$$

Luego $\sigma(a)$ es raíz de $p(X)$ y $\sigma(a) \in X$, es decir, $\sigma(K) \subseteq K$.

Sea $\overline{\sigma}: K \to K$ definida por $\overline{\sigma}(x) = \sigma(x)$ (es solo la restricción en el conjunto de llegada) y notemos que es una inmersión sobre k. Como $K|k$ es algebraica, y por el teorema 5.7 se tiene que $\overline{\sigma}$ es automorfismo, por lo tanto $\sigma(K) = \overline{\sigma}(K) = K$. □

Una extensión algebraica $K|k$ que satisface alguna (entonces todas) de las condiciones del teorema anterior, se llama *normal*. En particular el cuerpo de descomposición de un polinomio irreducible es normal.

Observación 5.9. Si $K|k$ es una extensión y K es el c.d.d. de un polinomio sobre k, entonces K es el c.d.d. de la familia de polinomios irreducibles que dividen a $p(X)$ y por lo tanto $K|k$ es normal. En particular $\mathbb{F}_q|\mathbb{F}_p$ es normal cuando $q = p^n$ con p un primo y n un natural.

Ejemplo 5.9.

- Si $K|k$ es una extensión de grado 2, entonces $K = k(\alpha)$ donde α satisface un polinomio de grado 2 en $k[X]$. Sea $p(X)$ tal polinomio, entonces $p(X)$ en $K[X]$ se descompone como $p(X) = (X - \alpha)q(X)$

con $q(X)$ de grado 1 en $K[X]$. Digamos que $q(X) = aX + b$ con $a \neq 0$ y $a, b \in K$, entonces b/a es raíz de $q(X)$ en K, y luego K es el c.d.d de $p(X)$. Por lo tanto toda extensión de grado 2 es normal.

- Si $K = \mathbb{Q}(\sqrt[4]{2})$, entonces $K|\mathbb{Q}$ no es normal, pues $X^4 - 2$ es irreducible en $\mathbb{Q}[X]$ que tiene una raíz en K pero no tiene a la raíz $\sqrt[4]{2}i$. Sin embargo, $[K : \mathbb{Q}(\sqrt{2})] = 2$, por lo tanto $K|\mathbb{Q}(\sqrt{2})$ es normal y como $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ es una extensión de grado 2, entonces también es normal.
- Sea $K = \mathbb{Q}(\sqrt[3]{2}), \zeta)$ donde $\zeta = \dfrac{-1}{2} + \dfrac{\sqrt{3}i}{2}$ es tal que $\zeta^3 = 1$. Entonces $K|\mathbb{Q}$ es normal pues K es el c.d.d de $X^3 - 1 = p(X)$ en $\mathbb{Q}[X]$, el cual es irreducible (ya que no tiene raíces en $\mathbb{Q}$). Notemos que $F = \mathbb{Q}(\sqrt[3]{2})$ es un cuerpo intermedio de $K|\mathbb{Q}$ tal que la extensión $F|\mathbb{Q}$ no es normal.

Observación 5.10. Si $K|k$ es normal, entonces $K = k(X)$ donde X son las soluciones de una familia $\mathscr{F} = \{f_\lambda\}_{\lambda\in\Lambda}$ de polinomios irreducibles en $k[X]$. Sea F un cuerpo tal que $k \subseteq F \subseteq K$, entonces $F(X) = K$ y sea $\mathscr{P}$ el conjunto de los divisores irreducibles de elementos de $\mathscr{F}$ en $F[X]$. Entonces $F(X) = K$ es c.d.d de la familia $\mathscr{P}$ de polinomios irreducibles sobre F. Luego $K|F$ es normal. Pero por el ejemplo anterior no es cierto, en general, que $F|k$ es normal.

5.4.3. Grupo de Galois de una extensión

Si K es un cuerpo, entonces el conjunto de todos los automorfismos de K es un grupo (con la composición), al cual lo denotamos por $\mathrm{Aut}(K)$. Es directo ver que

$$\mathrm{Aut}(K) = \{\sigma : K \to K;\ \sigma \text{ es morfismo, y } \sigma(K) = K\}.$$

Observación 5.11. Si k es un cuerpo primo, esto es k no tiene subcuerpos propios, entonces $k \cong \mathbb{Q}$ o $k \cong \mathbb{F}_p$ dependiendo si k es de característica cero, o es de característica p, con p primo. Si $\sigma : k \to k$ es un morfismo (por lo tanto monomorfismo), entonces $\sigma(k)$ es un cuerpo y por lo tanto $\sigma(k) = k$. Luego si k es primo, todo morfismo $\sigma : k \to k$ es automorfismo. Además, si $K|k$ es una extensión, es fácil ver que todo morfismo $\sigma : K \to K$ fija punto a punto a k (como en el ejemplo 3.10), y en particular todo morfismo de k en sí mismo es la identidad. Es decir, $\mathrm{Aut}(k) = \mathrm{End}(k) = \{\mathrm{id}\}$.

Sea $K|k$ una extensión de cuerpos, podemos definir el grupo $\mathrm{Aut}(K|k)$ también denotado por $\mathrm{Gal}(K|k)$ o simplemente $G(K|k)$, como el subgrupo de $\mathrm{Aut}(K)$ tal que deja fijo punto a punto a los elementos de k, es decir, el subgrupo de k-automorfismos. A tal grupo se le llama el *grupo de Galois de la extensión* $K|k$. Tenemos que

$$\mathrm{Aut}(K|k) = \mathrm{Gal}(K|k) = \{\sigma \in \mathrm{Aut}(K);\ \sigma(a) = a\ \forall a \in k\}.$$

Según la observación anterior, se tiene que si k es primo, entonces $\mathrm{Aut}(K|k) = \mathrm{Aut}(K)$.

Ejemplo 5.10.

- Consideremos la extensión $\mathbb{R}|\mathbb{Q}$ y recordemos que esta extensión es infinita. En el ejemplo (3.11) del capítulo de anillos, vimos que el único automorfismo de $\mathbb{R}$ es la identidad. Entonces $\mathrm{Gal}(\mathbb{R}|\mathbb{Q}) = \{\mathrm{id}\}$

- Si $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y $k = \mathbb{Q}$, entonces $\mathrm{Gal}(K|k) = \mathrm{Aut}(K)$. Como $K = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6};\ a, b, c, d \in \mathbb{Q}\}$, tenemos que para conocer un elemento σ de $\mathrm{Gal}(K|k)$ basta conocer el valor de $\sigma(\sqrt{2})$, de $\sigma(\sqrt{3})$ y de $\sigma(\sqrt{6})$. Pero $\sigma(\sqrt{6}) = \sigma(\sqrt{2})\sigma(\sqrt{3})$, entonces para determinar a σ nos basta fijar $\sigma(\sqrt{2})$, y $\sigma(\sqrt{3})$. Pero como $\sigma(q) = q$ para cada $q \in \mathbb{Q}$, en particular

$$2 = \sigma(2) = \sigma((\sqrt{2})^2) = \sigma(\sqrt{2})^2.$$

  Es decir $\sigma(\sqrt{2}) = \sqrt{2}$ o $\sigma(\sqrt{2}) = -\sqrt{2}$. Del mismo modo $\sigma(\sqrt{3}) = \sqrt{3}$ o $\sigma(\sqrt{3}) = -\sqrt{3}$. Luego los siguientes son candidatos a automorfismos de K:

$$\sigma_1, \sigma_2, \sigma_3, \sigma_4 : K \to K$$

  definidos por $\sigma_1 = \mathrm{id}$,

$$\sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

$$\sigma_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

$$\sigma_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$$

  Es fácil ver que efectivamente son automorfismos de K y notamos también que $\sigma^2 = \sigma \circ \sigma = \mathrm{id}$ para todo $\sigma \in \mathrm{Gal}(K|k)$, entonces $\mathrm{Gal}(K|k) \cong V_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Notemos además que $[K : k] = |\mathrm{Gal}(K|k)|$.
- Sea $\alpha = \dfrac{2\pi}{5}$, $\zeta = \cos(\alpha) + i\sin(\alpha) \in \mathbb{C}$ y $K = \mathbb{Q}(\zeta)$. Cualquier elemento del grupo de Galois de la extensión $K|\mathbb{Q}$ está determinado por su acción en ζ. Notemos que $\zeta^5 = 1$ entonces ζ es raíz de $X^5 - 1 = (X-1)(X^4 + X^3 + X^3 + X + 1) \in \mathbb{Q}[X]$ y como $\zeta \neq 1$, entonces ζ también es raíz de $p(X) = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$. Además $(\zeta^2)^5 = (\zeta^5)^2 = 1^2$ y como $\zeta^2 \neq 1$, entonces ζ^2 es raíz de $p(X)$. Del mismo modo ζ^3 y ζ^4 son raíces de $p(X)$. Entonces el conjunto de raíces de $p(X)$ es $\{\zeta, \zeta^2, \zeta^3, \zeta^4\} \subseteq K$, pues son todas distintas, y vemos que

$$p(X) = (X - \zeta)(X - \zeta^2)(X - \zeta^3)(X - \zeta^4) \in K[X].$$

  Además $p(X)$ es irreducible en $\mathbb{Q}[X]$ y por lo tanto $[K : \mathbb{Q}] = 4$.
  Si $\sigma : K \to K$ es un automorfismo, entonces

$$1 = \sigma(1) = \sigma(\zeta^5) = (\sigma(\zeta))^5$$

  y como $\sigma(\zeta) \neq 1$ se tiene que $\sigma(\zeta)$ es raíz de $p(X)$, es decir, $\sigma(\zeta) = \zeta^k$ para cierto $k \in [4]$. Entonces tenemos a lo más 4 automorfismos. Si $\sigma(\zeta) = \zeta^k$ denotaremos tal σ por σ_k, con $\sigma_1 = \mathrm{id}$. Cada uno de ellos es efectivamente un automorfismo de K y $\mathrm{Gal}(K|\mathbb{Q}) = \{\sigma_k;\ k \in [4]\}$. Además $\mathrm{Gal}(K|\mathbb{Q})$ es cíclico, con σ_2 uno de los generadores del grupo. Es decir, $\mathrm{Gal}(K|\mathbb{Q}) \cong \mathbb{Z}_4$ y además $[K : \mathbb{Q}] = |\mathrm{Gal}(K|\mathbb{Q})|$.

Observación 5.12. Sea $K|k$ una extensión algebraica, $a \in K$, $p(X) = \mathrm{irr}_{a,k}(X) = \sum_{i=0}^{n} a_i X^i$ con $a_i \in k$ y sea $\sigma \in \mathrm{Gal}(K|k)$. Entonces $p(a) = 0 = \sum_{i=0}^{n} a_i a^i$, y por lo tanto

$$0 = \sigma(0) = \sigma\left(\sum_{i=0}^{n} a_i a^i\right) = \sum_{i=0}^{n} \sigma(a_i)(\sigma(a))^i = \sum_{i=0}^{n} a_i(\sigma(a))^i = p(\sigma(a)).$$

Es decir, $\sigma(a)$ es raíz del polinomio irreducible de a y $\mathrm{irr}_{a,X}(X) = \mathrm{irr}_{\sigma(a),x}(X)$.

Si K es un cuerpo y G es un subgrupo de $\mathrm{Aut}(K)$, entonces definimos el conjunto de elementos fijos en K por la acción de G como

$$\mathrm{Fix}(G) = \{a \in K;\ \sigma(a) = a\ \forall \sigma \in G\}.$$

Como vimos antes, el cuerpo primo de K está contenido en $\mathrm{Fix}(G)$, y es fácil ver que éste es un cuerpo, llamado el *cuerpo fijo por* G. Las siguientes propiedades son un ejercicio fácil.

Proposición 5.6. *Sea K un cuerpo, $G = \mathrm{Aut}(K)$, F, F_1 y F_2 subcuerpos de K y H, H_1 H_2 subgrupos de G, entonces:*

1. $H_1 \supseteq H_2 \Rightarrow \mathrm{Fix}(H_1) \subseteq \mathrm{Fix}(H_2)$
2. $F_1 \supseteq F_2 \Rightarrow \mathrm{Gal}(K|F_1) \subseteq \mathrm{Gal}(K|F_2)$
3. $\mathrm{Fix}(\mathrm{Gal}(K|F)) \supseteq F$
4. $\mathrm{Gal}(K|\mathrm{Fix}(H)) \supseteq H$

En lo que sigue enlazaremos las tres subsecciones de este capítulo: extensiones normales, extensiones separables y grupo de Galois. El primer teorema es el siguiente:

Teorema 5.11. *Sea K el c.d.d. de de un polinomio separable en $k[X]$, entonces $[K : k] = |\mathrm{Gal}(K|k)|$.*

Antes de dar la demostración haremos una pequeña modificación del enunciado pero que no pierde generalidad.

Sea $p(X)$ el polinomio en $k[X]$ para el cual K es cuerpo de descomposición sobre k, y escribamos $p(X) = p_1^{\alpha_1}(X)p_2^{\alpha_2}(X)\cdots p_n^{\alpha_n}(X)$ con los $p_k(X) \in k[X]$ irreducibles, separables y distintos entre sí, y los α_k naturales positivos. Además sin restricción podemos considerar a cada p_k mónico. Sea $q(X) = p_1(X)p_2(X)\cdots p_n(X)$. Ambos polinomios $p(X), q(X)$ están en $k[X]$. Como el conjunto de raíces $p(X)$ es el mismo que el conjunto de raíces de $q(X)$ en K, entonces podemos considerar K como c.d.d. de $q(X)$ sobre k. Dado que $p(X)$ es separable, entonces también lo es $q(X)$, pero además $q(X)$ no tiene raíces múltiples pues si las tuviera, entonces existirían $k \neq j$ tal que p_k y p_j tienen una raíz en común. Sea a una de esas raíces en común. Como K es c.d.d. de $q(X)$, entonces $a \in K$ y por lo tanto habría dos polinomios mónicos irreducibles p_j y p_k que anulan a a en $k[X]$ lo cual es falso. Es decir, las raíces de $q(X)$ son todas distintas. Entonces sin restricción podemos suponer que K es el c.d.d. de un polinomio sin raíces múltiples en $k[X]$.

Demostración. Notemos que $[K : k]$ es finito, pues es el cuerpo de descomposición de un polinomio. Hagamos inducción sobre $[K : k]$. Si $[K : k] = 1$, entonces $K = k$ y $\mathrm{Gal}(K|k) = \{\sigma : k \to k;\ \sigma(a) = a\ \forall a \in k\} = \{\mathrm{id}\}$, de modo que $[K : k] = |\mathrm{Gal}(K|k)| = 1$.

Supongamos que si $E|F$ es cualquier extensión de grado menor que n, $r(X) \in F[X]$ es un polinomio con raíces distintas y E c.d.d de $r(X)$ entonces $[E : F] = |\mathrm{Gal}(K|k)|$, y tomemos $K|k$ una extensión de grado n tal que K es c.d.d. de $q(X) \in k[X]$ un polinomio con raíces distintas.

Sea a una raíz de $q(X) = p_1(X)p_2(X)\dots p_r(X)$, donde los p_i son distintos e irreducibles. Si todos los p_i son de grado 1, entonces $K = k$ y estaríamos en el caso $n = 1$ que ya conocemos. Supongamos entonces que existe p_i de grado mayor que 1 y sin restricción supongamos que a es raíz de p_1 y p_1 es de grado mayor que 1. El teorema 5.8 muestra que existen tantas inmersiones $\tau : k(a) \to K$ sobre k como raíces de $p_1(X)$ hay en K, pero en K hay tantas raíces de p_1 como el grado de p_1 por hipótesis. Sea $\mathrm{Inm}(k(a)|k)$ el conjunto de inmersiones $\tau : k(a) \to K$ sobre k, de modo que

$$[K : k(a)][k(a) : k] = n = [K : k(a)]\,\mathrm{grad}(p_1(X)) = [K : k(a)]|\,\mathrm{Inm}(k(a)|k)|.$$

Sea $\tau \in \mathrm{Inm}(k(a)|k)$ y sea $\sigma_\tau : K \to K$ la inmersión sobre τ que entrega el teorema 5.4, y recordemos que además es isomorfismo. Notemos que $\sigma_\tau(\alpha) = \tau(\alpha) = \alpha$ para cada α en k y por lo tanto $\sigma_\tau \in \mathrm{Gal}(K|k)$. Reciprocamente, si $\sigma \in \mathrm{Gal}(K|k)$ entonces $\sigma_{|k(a)} \in \mathrm{Inm}(k(a)|k)$, por lo tanto si definimos $\mathrm{Ext}(K|k(a)$ como el conjunto de los σ_τ para todo $\tau \in \mathrm{Inm}(k(a)|k)$, entonces $\mathrm{Ext}(K|k(a)) = \mathrm{Gal}(K|k)$. Esto último está diciendo, entre otras cosas, que para cada b raíz de $p_1(X)$, existe $\sigma \in \mathrm{Gal}(K|k)$ tal que $\sigma(a) = b$. Sea $q_1(X)$ el producto de los factores irreducibles de $q(X)$ en $k(a)[X]$. Como $q_1(X)$ divide a $q(X)$ se tiene que las raíces de $q_1(X)$ son todas distintas, K es c.d.d. de $q_1(X)$ sobre $k(a)$ y $[K : k(a)] < n$. Entonces por hipótesis inductiva, se tiene que $[K : k(a)] = |\mathrm{Gal}(K|k(a))|$ y concluimos que

$$[K : k] = |\mathrm{Gal}(K|k(a))||\,\mathrm{Inm}(k(a)|k)|.$$

Por otra parte, si $\mathrm{grad}(p_1) = t$, entonces $[k(a) : k] = |\mathrm{Inm}(k(a)|k)| = |T| = t$, donde T es el conjunto de raíces de $p_1(X)$ en K. Hagamos actuar $G = \mathrm{Gal}(K|k)$ en T, vía evaluación:definimos la acción $G \times T \to T$ por $(\sigma, c) \to \sigma(c)$. Notemos que $\mathrm{Orb}(a) = T$, y entonces $|T| = |G|/\,\mathrm{Stab}(a)|$ donde

$$\mathrm{Stab}(a) = \{\sigma \in \mathrm{Gal}(K|k) = \mathrm{Ext}(K|k(a));\ \sigma(a) = a\} = \mathrm{Gal}(K|k(a)).$$

Por lo tanto $|T||\,\mathrm{Gal}(K|k(a))| = |G|$ pero $|\,\mathrm{Inm}(k(a)|k)| = |T|$, y como $[K : k] = |\mathrm{Gal}(K|k(a))||\,\mathrm{Inm}(k(a)|k)|$ concluimos que $[K : k] = |G|$. □

Un resultado recíproco, en algún sentido, al anterior dice que si G es un subgrupo finito de $\mathrm{Aut}(K)$ y $\mathrm{Fix}(G) = k$, entonces $[K : k] = |G|$. Para ello probemos primero el siguiente lema debido a Artin.

Teorema 5.12 (Lema de Artin)**.** *Si K es un cuerpo, G un subgrupo finito de* $\mathrm{Aut}(K)$ *y* $k = \mathrm{Fix}(G)$*, entonces* $[K : k] \leq |G|$.

Demostración. Sea $G = \{\eta_1 = \mathrm{id}, \eta_2, \eta_3, \ldots, \eta_n\}$ con $n = |G|$, sea $k = \mathrm{Fix}(G)$ y sea $\{u_1, u_2, \ldots, u_m\}$ un conjunto de m elementos de K donde $m > n$. Consideremos el siguiente sistema homogéneo de ecuaciones lineales a coeficientes en K:

$$\begin{aligned}
\eta_1(u_1)x_1 + \eta_1(u_2)x_2 + \eta_1(u_3)x_3 + \cdots + \eta_1(u_m)x_m &= 0 \\
\eta_2(u_1)x_1 + \eta_2(u_2)x_2 + \eta_2(u_3)x_3 + \cdots + \eta_2(u_m)x_m &= 0 \\
&\vdots \\
\eta_n(u_1)x_1 + \eta_n(u_2)x_2 + \eta_n(u_3)x_3 + \cdots + \eta_n(u_m)x_m &= 0
\end{aligned}$$

Tenemos un sistema homogeneo de n ecuaciones y m incognitas con $m > n$, por lo tanto el conjunto de soluciones $(b_1, b_2, b_3, \ldots, b_m) \in K^m$ es un espacio vectorial no trivial de K^m. Entre las soluciones no nulas del sistema, escojamos una de aquellas que tiene la mayor cantidad de coordenadas nulas, digamos $b = (b_1, b_2, b_3, \ldots, b_m)$. Intercambiando las incógnitas si es neccesario, podemos suponer que $b_1 \neq 0$, además como λb también es solución del sistema para cada $\lambda \in K$, tomando $\lambda = (b_1)^{-1}$ podemos suponer que $b_1 = 1$.

Afirmamos que todas las coordenadas de b son elementos de k. Si así no fuera, existiría algún i tal que $b_i \notin k$. Sin restricción supongamos que $b_2 \notin k$. Como $\mathrm{Fix}\, G = k$, entonces existe j tal que $\eta_j(b_2) \neq b_2$. Apliquemos ese η_j al sistema de ecuaciones evaluado en b para obtener

$$\begin{aligned}
\eta_j \circ \eta_1(u_1)1 + \eta_j \circ \eta_1(u_2)\eta_j(b_2) + \eta_j \circ \eta_1(u_3)\eta_j(b_3) + \cdots + \eta_j \circ \eta_1(u_m)\eta_j(b_m) &= 0 \\
\eta_j \circ \eta_2(u_1)1 + \eta_j \circ \eta_2(u_2)\eta_j(b_2) + \eta_j \circ \eta_2(u_3)\eta_j(b_3) + \cdots + \eta_j \circ \eta_2(u_m)\eta_j(b_m) &= 0 \\
&\vdots \\
\eta_j \circ \eta_n(u_1)1 + \eta_j \circ \eta_n(u_2)\eta_j(b_2) + \eta_j \circ \eta_n(u_3)\eta_j(b_3) + \cdots + \eta_j \circ \eta_n(u_m)\eta_j(b_m) &= 0
\end{aligned}$$

Pero como $\{\eta_j \circ \eta;\ \eta \in G\} = G$ se tiene que este sistema es igual al primer sistema evaluado en $b^{\eta_j} \doteq (1, \eta_j(b_2), \eta_j(b_3), \ldots, \eta_j(b_m))$ y entonces b^{η_j} es solución del sistema también es solución de éste. Por lo tanto $b - b^{\eta_j}$ también lo es. Pero $b - b^{\eta_j} = (0, b_2 - \eta_j(b_2), b_3 - \eta_j(b_3), \ldots, b_m - \eta_j(b_2))$, y como $b_i - \eta_j(b_i)$ es 0 si b_i lo es y $b_2 - \eta_j(b_2)$ no es nulo, vemos que $b - b^{\eta_j}$ no es 0 y tiene más coordenadas nulas que b, contradiciendo la minimalidad de éste. Entonces efectivamente todas las coordenadas de b están en k.

Por otra parte notamos que la primera ecuación del sistema es

$$u_1x_1 + u_2x_2 + u_3x_3 + \cdots + u_mx_m$$

pues $\eta_1 = \mathrm{id}$. Evaluando en b resulta que $b_1u_1 + b_2u2 + \cdots + b_mu_m = 0$ es una combinación lineal nula con coeficientes no todos nulos en k. Por lo tanto el conjunto $\{u_1, u_2, \ldots, u_m\}$ es l.d. sobre k. Es decir, todo conjunto de K con $m > n$ elementos es l.d. sobre k. Luego $\dim_k K \leq n$, o lo que es lo mismo $[K : k] \leq |G|$. □

Ahora estamos en condiciones de relacionar más precisamente el grupo de Galois de una extensión, la normalidad y la separabilidad.

Teorema 5.13. *Sea $K|k$ una extensión de cuerpos. Entonces las siguientes condiciones son equivalentes:*

1. *K es el cuerpo de descomposición de un polinomio $p(X) \in k[X]$ el cual es separable.*
2. *$k = \mathrm{Fix}(G)$ para cierto subgrupo finito G de $\mathrm{Aut}(K)$.*
3. *$K|k$ es finita, normal y separable.*

Demostración. $1 \Rightarrow 2$: Sea $G = \mathrm{Gal}(K|k) \leq \mathrm{Aut}(K)$. Como $K|k$ satisface las condiciones del teorema 5.11 entonces $|G| = [K : k]$ es finito. Tenemos que demostrar que $\mathrm{Fix}(G) = k$. Sea $F = \mathrm{Fix}(G)$, entonces $k \subseteq F \subseteq K$ de manera que $\mathrm{Gal}(K|F) \supseteq G$. Además $\mathrm{Gal}(K|F) \subseteq G$ ya que $F = \mathrm{Fix}(G)$, y obtenemos que $\mathrm{Gal}(K|F) = G$. Notando que además K es el cuerpo de descomposición de $p(X)$ sobre F, el teorema 5.11 implica que $[K : F] = |G| = [K : k]$, y como $[K : k] = [K : F][F : k]$ entonces $[F : k] = 1$ y $k = F$, que es lo que queríamos probar.

$2 \Rightarrow 3$: Sea G un grupo finito de automorfismos de K y $k = \mathrm{Fix}(G)$. Por el lema de Artin se tiene que $[K : k] \leq |G|$ y luego $K|k$ es una extensión finita. Sea $q(X) \in K$ un polinomio irreducible que tiene una raíz a en K y sea $X = \mathrm{Orb}(a) = \{\sigma(a);\ \sigma \in G\}$. Luego tenemos que $X \subseteq K$ es un conjunto de raíces de $q(X)$. Escribamos $X = \{a = a_1, a_2, a_3 \ldots, a_r\}$ con $a_i \neq a_j$ si $i \neq j$ de modo que el polinomio

$$g(X) = (X - a_1)(X - a_2)(X - a_3) \cdots (X - a_r) \in K[X]$$

es separable y divide a $q(X)$. Además, para cada $\sigma \in G$ consideremos $\tilde{\sigma} \colon K[X] \to K[X]$ definida por $\sum_{i=0}^{m} c_i X^i \to \sum_{i=0}^{m} \sigma(c_i) X^i$. En particular, para cada $\sigma \in G$ se tiene que

$$\tilde{\sigma}(g(X)) = (X - \sigma(a_1))(X - \sigma(a_2))(X - \sigma(a_3)) \cdots (X - \sigma(a_r)) = g(X)$$

Por lo tanto si $g(X) = \sum_{i=0}^{r} d_i X^i$, entonces $\sigma(d_i) = d_i$ para cada $\sigma \in G$. Es decir, $g(X) \in \mathrm{Fix}(G)[x] = k[X]$. Pero como $q(X)$ es irreducible (y $g(X)$ divide a $q(X)$), se tiene que $g(X) = q(X)$. Entonces K tiene todas las raíces de $q(X)$ y de lo anterior concluimos que $K|k$ es normal. Además, como $K|k$ es finita entonces es algebraica, y por lo tanto el mismo argumento que antes prueba quepara cada $a \in K$ se tiene que $\mathrm{irr}_{a,k}(X)$ es separable en $k[X]$. Luego $K|k$ es finita, normal y separable.

$3 \Rightarrow 1$: Como $[K : k]$ es finito, entonces podemos escribir $K = k(a_1, a_2, \ldots, a_n)$ con cada a_i algebraico sobre k. Consideremos los polinomios $p_i(X) = \mathrm{irr}_{a_i,k}(X)$ para cada $i \in [n]$ y notemos que como $K|k$ es normal, cada $p_i(X)$ se descompone linealmente en $K[X]$ y como $K|k$ es separable, cada $p_i(X)$ es separable. Entonces K es c.d.d. de $p(X) = p_1(X)p_2(X)p_3(X) \cdots p_n(X)$ el cual es separable. □

Si $K|k$ es una extensión que cumple cualquiera (entonces todas) de las condiciones del teorema anterior, diremos que $K|k$ es una extensión *galoisiana* finita o que es una extensión finita de *Galois*.

Notemos que si $K|k$ es finita y de Galois entonces en la demostración de $1 \Rightarrow 2$ demostramos que $\mathrm{Fix}(\mathrm{Gal}(K|k)) = k$. Recíprocamente, si $K|k$ es finita y $\mathrm{Fix}(\mathrm{Gal}(K|k)) = k$, entonces por 2 se tiene que $K|k$ es de Galois. Por otro lado, si $K|k$ es finita y de Galois y $\mathrm{Gal}(K|k) = G$, entonces 1 dice que K es el c.d.d. de un polinomio $p(X) \in k[X]$ separable y el teorema 5.11 muestra que $[K : k] = |\mathrm{Gal}(K|k)|$. Además, si $K|k$ es finita y $[K : k] \neq |\mathrm{Gal}(K|k)|$, entonces $K|k$ no es de Galois. Por último, si $K|k$ es finita tal que $[K : k] = |\mathrm{Gal}(K|k)|$, entonces escribamos $G = \mathrm{Gal}(K|k)$ y $F = \mathrm{Fix}(G)$. Por 2 tenemos que $K|F$ es de Galois, luego $\mathrm{Gal}(K|F) = G$ y $[K : F] = |G| = [K : k]$. Por lo tanto $k = F$, es decir $\mathrm{Fix}(\mathrm{Gal}(K|k) = k$ y $K|k$ es galoisiana. Luego tenemos el siguiente teorema.

Teorema 5.14. *Si $K|k$ es una extensión finita, entonces las siguientes condiciones son equivalentes:*

1. *$K|k$ es de Galois.*
2. $\mathrm{Fix}(\mathrm{Gal}(K|k)) = k$.
3. $[K : k] = |\mathrm{Gal}(K|k)|$.

El siguiente teorema es el más importante de la teoría de Galois.

Teorema 5.15 (Teorema de correspondencia de Galois)**.** *Sea $K|k$ una extensión finita de Galois, y sea $G = \mathrm{Gal}(K|k)$. Para cada H subgrupo de G se cumple que $\mathrm{Gal}(K|\mathrm{Fix}(H)) = H$, y para cada cuerpo intermedio F de la extensión $K|k$ se cumple que $\mathrm{Fix}(\mathrm{Gal}(K|F)) = F$. Es decir, las aplicaciones $\mathrm{Fix}(\cdot)$ y $\mathrm{Gal}(K|\cdot)$ son inversas entre sí y biyectan los subgrupos de G y los cuerpos intermedios de la extensión $K|k$. Además se cumple que*

1. $H_1 \supseteq H_2 \iff \mathrm{Fix}(H_1) \subseteq \mathrm{Fix}(H_2)$.
2. $|H| = [K : \mathrm{Fix}(H)]$.
3. $[G : H] = [\mathrm{Fix}(H) : k]$.
4. *H es normal en $G \iff \mathrm{Fix}(H)$ es normal sobre k. En este caso* $\mathrm{Gal}(\mathrm{Fix}(H)|k) \cong G/H$.

Antes de dar la demostración recordemos que si $K|k$ es normal y F es un cuerpo intermedio, entonces $K|F$ es normal pero no necesariamente $F|k$ es normal. Además, si $K|k$ es separable y F es un cuerpo intermedio, entonces $K|F$ y $F|k$ son separables. Luego si $K|k$ es de Galois y F es un cuerpo intermedio, entonces $K|F$ es de Galois y $F|k$ no es necesariamente de Galois, más aún $F|k$ es de Galois ssi $F|k$ es normal.

Demostración. Sea $H \leq G$ y escribamos $F = \mathrm{Fix}(H)$. Como G es finito, entonces H es finito y por lo tanto $K|F$ es Galois. Luego $\mathrm{Gal}(K|F) = H$ y tenemos que $|H| = [K : F]$ por el teorema anterior. Además $|G| = [K : k] = [K : F][F : k] = |H|[F : k]$, luego $[F : k] = |G|/|H| = [G : H]$. Ahora sea F cuerpo intermedio de $K|k$, entonces $K|F$ es de Galois y por lo tanto $\mathrm{Fix}(\mathrm{Gal}(K|F)) = F$. Hasta ahora hemos demostrado 2, 3 y lo afirmado antes de 1.

Probemos 1: ya tenemos que si $H_1 \supseteq H_2$, entonces $\mathrm{Fix}(H_1) \subseteq \mathrm{Fix}(H_2)$. Recíprocamente, si $\mathrm{Fix}(H_1) \supseteq \mathrm{Fix}(H_2)$, entonces $H_1 = \mathrm{Gal}(K|\mathrm{Fix}(H_1)) \supseteq \mathrm{Gal}(K|\mathrm{Fix}(H_2) = H_2)$, donde las igualdades ocurren pues $K|\mathrm{Fix}(H_i)$ es de Galois para cada i.

Nos falta demostrar 4. En general, si $H \leq G$ y $\eta \in G$, entonces $\mathrm{Fix}(\eta H \eta^{-1}) = \eta(\mathrm{Fix}(H))$. Entonces H es normal en G ssi $\eta(\mathrm{Fix}(H)) = \mathrm{Fix}(H)$ para cada $\eta \in G$. Supongamos que $\eta(\mathrm{Fix}(H)) = \mathrm{Fix}(H) = F$ para todo $\eta \in G$, y sea $p(x) \in k[X]$ irreducible en $k[X]$ con $a \in F$ una raíz de $p(X)$. Como $K|k$ es normal y $a \in K$, entonces $p(X) = \lambda(X - a_1)(X - a_2)(X - a_3)\cdots(X - a_n)$ con $\lambda \in k$, los $a_i \in K$ y $a = a_1$. Pero además tenemos que $\{a_1, a_2, a_3 \ldots, a_n\} = \mathrm{Orb}(a) = \{\sigma(a);\ \sigma \in G\}$ bajo la acción de G en K. Por lo tanto para cada a_i existe $\sigma \in G$ tal que $\sigma(a) = a_i$, pero como $\sigma(F) = F$ para cada $\sigma \in G$, se tiene que $a_i \in F$ para $i \in [n]$. Luego $F|k$ es normal.

Recíprocamente, si $F|k$ es normal con $F = \mathrm{Fix}(H)$, sea $\eta \in G$ y sea $\overline{K}$ la clausura algebraica de K. Como $K|k$ es algebraica, entonces $\overline{K}$ es clausura algebraica de k. Sea $\iota : K \to \overline{K}$ la inclusión, entonces $\iota \circ \eta : K \to \overline{K}$ es un monomorfismo, por lo tanto $(i \circ \eta)_{|F}$ es un monomorfismo de F a $\overline{K}$, pero como $F|k$ es normal

tenemos que $(\iota \circ \eta)_{|F}(F) = F$, es decir $\eta(F) = F$. Es decir, para cada $\eta \in G$ se tiene que $\eta(\text{Fix}(H)) = \text{Fix}(H)$. Luego H es normal en G.

Por lo anterior, tenemos que si $\eta \in \text{Gal}(K|k)$ entonces $\eta_{|F} \in \text{Gal}(F|k)$. Definamos en este caso $\phi\colon \text{Gal}(K|k) \to \text{Gal}(F|k)$ por $\phi(\eta) = \eta_{|F}$, el cual es un morfismo. Además si $\sigma\colon F \to F$ podemos considerar $\overline{\sigma}\colon F \to K$ dada por $\overline{\sigma}(a) = \sigma(a)$ y $\tilde{\sigma}\colon K \to K$ una extensión sobre $\overline{\sigma}$, de manera que $\phi(\tilde{\sigma}) = \sigma$. Luego ϕ es epimorfismo. Por el primer teorema del isomorfismo se tiene que $G/\ker(\phi) \cong \text{Gal}(F|k)$.

Nos basta conocer el $\ker(\phi)$. Tenemos que $\eta \in G$ está en el $\ker(\phi)$ ssi $\eta_{|F} = \text{id}_F$, es decir, $\eta(a) = a$ para todo $a \in F$ y concluimos que $\ker(\phi) = \text{Gal}(K|F)$. Como $K|F$ es de Galois y $F = \text{Fix}(H)$ se tiene que $\text{Gal}(K|k) = H$ y entonces $G/H \cong \text{Gal}(F|k)$. □

Una primera aplicación del teorema de correspondencia de Galois es el teorema fundamental del álgebra. Para demostrar esto, primero notemos que $\mathbb{C}$ no admite extensiones de grado 2, pues si $F|\mathbb{C}$ es tal que $[F : \mathbb{C}] = 2$, entonces $F = \mathbb{C}(\alpha)$ con $\alpha^2 \in \mathbb{C}$. Como $\mathbb{C}$ contiene todas las raíces cuadradas de sus elementos, obtenemos que $\alpha \in \mathbb{C}$. Además, el teorema del valor medio muestra que cada polinomio de grado impar en $\mathbb{R}[X]$ tiene al menos una raíz en $\mathbb{R}$, de modo que todo polinomio irreducible en $\mathbb{R}[X]$ es de grado par salvo los polinomios de grado 1. Por lo tanto si $F|\mathbb{R}$ tiene grado impar, entonces para cada $a \in F$ se tiene que $[\mathbb{R}(a) : \mathbb{R}]$ divide a $[F : \mathbb{R}]$ y luego $[\mathbb{R}(a) : \mathbb{R}]$ es impar. Como $[\mathbb{R}(a) : \mathbb{R}] = \text{grad}(\text{irr}_{a,\mathbb{R}})(X)$ tenemos que $\text{irr}_{a,\mathbb{R}}(X)$ es un polinomio irreducible de grado impar y entonces $\text{irr}_{a,\mathbb{R}}$ es de grado 1. Luego $\mathbb{R}$ no admite extensiones de grado impar salvo la trivial. Con estas observaciones podemos dar una demostración del teorema fundamental del álgebra.

Teorema 5.16 (Teorema Fundamental del álgebra)**.** *El cuerpo de los números complejos $\mathbb{C}$ es algebraicamente cerrado.*

Demostración. Tenemos que demostrar que $\mathbb{C}$ no admite extensiones algebraicas, salvo la trivial, que es equivalente a decir que $\mathbb{C}$ no admite extensiones finitas. Sea entonces $F|\mathbb{C}$ una extensión finita, de manera que $F|\mathbb{R}$ es finita. Sea $F = \mathbb{R}(a_1, a_2, a_3, \ldots, a_r)$ con a_i algebraico sobre $\mathbb{R}$ y sea $K \supseteq F \supseteq \mathbb{C}$ el cuerpo de descomposición de $p(X) = p_1(X)p_2(X)p_3(X)\cdots p_r(X)$, donde $p_i(X) = \text{irr}_{a,\mathbb{R}}(X)$. Como $\mathbb{R}$ es de característica cero, entonces $K|\mathbb{R}$ es separable. Luego $K|\mathbb{R}$ es de Galois, y si $G = \text{Gal}(K|\mathbb{R})$ tenemos que $[K : \mathbb{R}] = |G| = [K : \mathbb{C}][\mathbb{C} : \mathbb{R}]$. Obtenemos que 2 divide a $|G|$. Escribamos $|G| = 2^n m$ con m impar.

Demostraremos que $m = 1$. Por el teorema de Sylow existe un subgrupo P de orden 2^n en G. Por el teorema de correspondencia de Galois $L = \text{Fix}(P)$ es un cuerpo intermedio de la extensión $K|\mathbb{R}$ tal que $[G : P] = [L : \mathbb{R}] = m$, y como m es impar se cumple que $m = 1$ (ya que las únicas extensiones de grado impar de $\mathbb{R}$ son las triviales). Por lo tanto $G = P$ un 2-grupo de orden 2^n. Entonces $[K : \mathbb{R}] = 2^n = |G|$ y concluimos que $[K : \mathbb{C}] = 2^t = 2^{n-1}$. Como $K|\mathbb{R}$ es de Galois, entonces $K|\mathbb{C}$ es de Galois. Si $t \geq 1$, entonces existe un subgrupo normal H de orden 2^{t-1} en G. Para ese H se tiene que $\text{Fix}(H) = E$, entonces $[E : \mathbb{C}] = [G : H] = 2$, es decir $E|\mathbb{C}$ es una extensión de grado 2, lo cual es falso. Por lo tanto $t = 0$ y $K = \mathbb{C}$, y concluimos que $F = \mathbb{C}$. □

5.5. Ejercicios

Ejercicio 5.1. Usando el teorema de estructura de grupos abelianos finitamente generados, pruebe que si k es un cuerpo entonces cualquier subgrupo finito de $k^\times$ es cíclico, y que el grupo aditivo de F_q (donde $q = p^n$ con p un primo) es isomorfo a $\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$.

Ejercicio 5.2. Sean α y β dos números complejos trascendentes sobre $\mathbb{Q}$. Muestre que $\alpha\beta$ y $\alpha + \beta$ no pueden ser ambos algebraicos sobre $\mathbb{Q}$.

Ejercicio 5.3. Un cuerpo k se dice cuerpo ordenado si existe $P \subset k$ (llamado el conjunto de los positivos) tal que es cerrado bajo la suma y el producto de k y satisface la ley de tricotomía, esto es, para cada $x \in k$ se tiene una y solo una de las siguientes condiciones: $x = 0$, o bien $x \in P$, o bien $-x \in P$. En lo que sigue k es un cuerpo ordenado y P es el conjunto de positivos de k.

a) Muestre que k contiene una copia isomorfa de $\mathbb{Q}$.
b) Si $x, y \in k$, y se cumple que $y - x \in P$ escribimos $x < y$. Definimos $x \leq y$ de la forma obvia y $|x| = \text{máx}\{x, -x\}$. Muestre que se cumple que $|x| = 0$ ssi $x = 0$, y que para $x, y \in k$ se tiene que $|xy| = |x||y|$ e $|x + y| \leq |x| + |y|$.
c) Dado $S \subset k$ diremos que $u \in k$ es una cota superior de S si $s \leq u$ para todo $s \in S$. Si u es cota superior de S y $u \leq z$ para toda cota superior z de S, entonces decimos que u es supremo de S. Si k es tal que todo conjunto acotado superiormente tiene supremo, diremos que k es un cuerpo ordenado completo. Demuestre que si k es un cuerpo ordenado completo, entonces es arquimediano, esto es, para todo $x \in k$ existe $n \in \mathbb{N}$ tal que $x < n$ (aquí nos referimos a la copia de los naturales dentro de la copia de los racionales que está en k).
d) Si k es un cuerpo ordenado completo, entonces la copia de $\mathbb{Q}$ es denso en k (es decir, para cada $p \in P$ y $x \in k$ existe $q \in \mathbb{Q}$ tal que $|x - q| \leq p$).
e) Sean k_1 y k_2 cuerpos ordenados completos, $\mathbb{Q}_i$ la copia de $\mathbb{Q}$ en k_i para $i = 1, 2$ y τ el único isomorfismo de $\mathbb{Q}_1$ en $\mathbb{Q}_2$. Para cada $x \in k_1$ definimos $\psi(x) = \sup\{\tau(q) \in \mathbb{Q}_2; q < x\} \in k_2$. Muestre que ψ es un isomorfismo de anillos que preserva el orden.

Ejercicio 5.4. Pruebe que un cuerpo ordenado no puede ser algebraicamente cerrado.

Ejercicio 5.5. Sea $K|k$ una extensión algebraica donde k es un cuerpo infinito. Pruebe que existe una cantidad finita de cuerpos intermedios $k \subseteq M \subseteq K$ ssi $K|k$ es una extensión simple.
Indicación: piense en extensiones del tipo $k(\alpha + \gamma\beta)$ con $\gamma \in k$.

Ejercicio 5.6. Pruebe que toda extensión finita y separable es simple.

Ejercicio 5.7. Sea $K|k$ una extensión finita de grado n y $\alpha \in K$. Pruebe que:

a) La función de K en K dada por $l(x) = \alpha x$ es una función lineal.
b) El polinomio minimal de α divide al polinomio característico de la matriz representante de l.
c) Las matrices de $n \times n$ contienen una copia isomorfa de cualquier extensión de grado n y de cualquier extensión de grado d con d un divisor de n.

Usando lo anterior, calcule el polinomio minimal de $\sqrt[3]{2}+\sqrt[3]{4}$ sobre $\mathbb{Q}$.

Ejercicio 5.8. Sea k un cuerpo de característica prima p, $n \geq 1$ un natural, $a \in k$ y sea $f(X) = X^{p^n} - a \in k[X]$, con K su cuerpo de descomposición sobre k.

a) Muestre que $f(X)$ tiene una sola raíz $c \in K$ (¿ de qué multiplicidad?).

Ahora queremos mostrar que $f(X)$ no es irreducible en $k[X]$ ssi $a = b^p$ para algún $b \in k$.

b) Pruebe la implicancia $\Leftarrow$.

Supongamos ahora que $f(X)$ no es irreducible en $k[X]$ y que $g(X) \in k[X]$ es un factor mónico de grado m (con $0 < m < p^n$) de $f(X)$.

c) Para la raíz c de $f(X)$ de la parte a), muestre que $g(X) = (X-c)^m$ en $K[X]$, y que $c^m, c^{p^n} \in k$.

d) Muestre que para algún natural $l < n$, se tiene que $c^{p^l} \in k$.
Indicación: Muestre que hay un natural $l < n$ y enteros $r,s \in \mathbb{Z}$ tales que $p^l = rm + sp^n$.

e) Concluya la implicancia $\Rightarrow$.

Ejercicio 5.9. Sean p primo, F cuerpo de característica p y $K = F(\alpha) \neq F$ donde α es raíz del polinomio $q(X) = X^p - X - 1 \in F[X]$. Muestre que K es cuerpo de descomposición de $q(X)$ sobre F, y que $|\mathrm{Gal}(K|F)| = p$.

Ejercicio 5.10. Sea $\eta \in \mathbb{C}$ tal que $\eta^6 + \eta^3 + 1 = 0$, sea $K = \mathbb{Q}(\eta)$ y sea $\overline{\mathbb{Q}}$ la clausura algebraica de $\mathbb{Q}$ contenida en $\mathbb{C}$.

a) Sea $G = \{z \in \mathbb{C};\ z^9 = 1\}$. Muestre que G es un subgrupo finito de $K^\times$.

b) Muestre que si $\sigma : K \to \overline{\mathbb{Q}}$ es un morfismo, entonces $\sigma(K) = K$.

c) Sea m un entero positivo primo relativo con 9. Demuestre que existe un automorfismo de K tal que $\sigma(\eta) = \eta^m$.

d) Demuestre que $p(X) = X^6 + X^3 + 1$ es irreducible en $\mathbb{Q}[X]$.

e) Pruebe que $\mathrm{Gal}(K|\mathbb{Q}) \cong \mathbb{Z}_9^\times$.

Ejercicio 5.11. Sean p primo, n un entero positivo no divisible por p y $q = p^n$. Sea además $G = \mathrm{Aut}(\mathbb{F}_q)$.

a) Demuestre que $\mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p) = G$ y que G es cíclico de orden n.

b) Demuestre que $\sum_{\sigma\in G} \sigma(x) \in \mathbb{F}_p$ para cada $x \in \mathbb{F}_q$.

c) Pruebe que $T : \mathbb{F}_q \to \mathbb{F}_p$ definida por $T(x) = \sum_{\sigma\in G} \sigma(x)$ es $\mathbb{F}_p$-lineal y no nula.

d) Pruebe que si $v \in \mathbb{F}_q$, entonces $T(v - v^p) = 0$.

e) Pruebe que existe $w \in \mathbb{F}_q$ tal que $T(w) = 1$.

f) Sea $u \in \mathbb{F}_q$ tal que $T(x) = 0$ y $w \in \mathbb{F}_q$ tal que $T(w) = 1$. Defina v por

$$v = uw + (u+u^p)w^p + (u+u^p+u^{p^2})w^{p^2} + \cdots + (u+u^p+u^{p^2}+\cdots+u^{p^{n-2}})w^{p^{n-2}}.$$

Muestre que $u = v - v^p$.

Bibliografía

[DF04] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[Gol93] Eric Goles, *Álgebra*, first ed., Ediciones Dolmen, 1993.

[Hal60] Paul R. Halmos, *Naive set theory*, The University Series in Undergraduate Mathematics, D. Van Nostrand Co., Princeton, N.J.-Toronto-London-New York, 1960.

[HK71] Kenneth Hoffman and Ray Kunze, *Linear algebra*, second ed., Prentice-Hall, Inc., Englewood Cliffs, N.J., 1971.

[Hun03] Thomas Hungerford, *Algebra*, eighth ed., Springer, 2003.

[Jac09] Nathan Jacobson, *Basic algebra i*, second ed., Basic Algebra, Dover Publications, 2009.

[Lan05] Serge Lang, *Algebra*, Graduate Texts in Mathematics, Springer New York, 2005.

[Ros78] John S. Rose, *A course on group theory*, Cambridge University Press, 1978.

[Rud64] Walter Rudin, *Principles of mathematical analysis*, second ed., McGraw-Hill Book Co., New York, 1964.

[Ste89] Ian Stewart, *Galois theory*, second ed., Chapman and Hall, Ltd., London, 1989.