Teoría de Números Algebraicos

Luis Arenas

August 4, 2021

Contents

Chapter 1

De los enteros y otros dominios

1.1 Anillos, anillos conmutativos y sus ideales

El conjunto $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ de los *enteros*, o *números enteros*, positivos y negativos es un anillo con las operaciones usuales de suma y producto. A lo largo de estos apuntes encontraremos numerosas estructuras de este tipo, por lo que repasaremos aquí sus propiedades básicas.

Recordemos que un anillo $(A, +, \cdot)$ es un grupo abeliano $(A, +)$ donde la operación conmutativa $+$ recibe el nombre de suma, junto con una segunda operación, usualmente denotada por "$\cdot$", o simplemente por yuxtaposición, denominada producto, que satisface las propiedades siguientes

1. $a(b + c) = ab + ac$, y $(b + c)a = ba + ca$,
2. $(ab)c = a(bc)$.

Si además se cumple que existe un elemento $1 \in A$ tal que $1a = a1 = a$ para todo $a \in A$ se dice que A es un *anillo unitario*. Si $ab = ba$ para todo par de elementos a y b en A, se dice que el anillo A es conmutativo. El anillo $\mathbb{Z}$ es un anillo conmutativo y unitario. En estas notas, utilizaremos la palabra anillo en el sentido de "anillo unitario", lo que es bastante usual en la literatura. Si necesitamos referirnos a un anillo no unitario, o no necesariamente unitario, lo diremos explícitamente. Nos referiremos a él como un ANNU (las iniciales de "anillo no necesariamente unitario"). Por ejemplo, el conjunto $2\mathbb{Z} = \{2t | t \in \mathbb{Z}\}$ de todos los enteros pares es un ANNU. Un ANNU $I \subseteq A$ es un

ideal si $aI = Ia = I$ para todo elemento $a \in A$. Si A es conmutativo basta comprobar que $aI = I$. La mayoría de los ANNU que aparecen en estas notas son ideales, por lo que nos referimos a ellos por ese nombre, "ideales".

Ejemplo 1.1. El conjunto $2\mathbb{Z}$ de números pares, así como el conjunto $n\mathbb{Z}$ de múltiplos de n para cada n, son ideales de $\mathbb{Z}$. Más generalmente, si el anillo A es conmutativo, entonces $aA = \{ab|b \in A\}$ es un ideal para cada elemento a de A. El ideal aA se llama el ideal principal generado por a y se denota también (a). Estos ideales jugarán un papel crucial en todo lo que sigue.

Dados dos ideales I y J, tamto su intersección $I \cap J$ como su suma $I + J = \{a + b|a \in I, J \in b\}$ son ideales. También es un ideal su producto IJ, definido como sigue:

$$IJ = \left\{ \sum_i a_i b_i \Big| a_i \in I, b_i \in J \right\}.$$

En un anillo arbitrario A, los elementos $a \in A$ que tienen un inverso multiplicativo $b \in A$, es decir $ab = ba = 1$, reciben el nombre de unidades. Las únicas unidades del anillo $\mathbb{Z}$ de números enteros son los elementos 1 y -1. Un elemento u en un anillo conmutativo A es una unidad si y sólo si el ideal Au de múltiplos de u es igual al anillo completo A. Otros ejemplos básicos de unidades son los siguientes:

1. En un cuerpo, todo elemento no nulo es una unidad.

2. En el anillo de polinomios $K[x]$, con coeficientes en un cuerpo K, las unidades son las constantes no nulas.

3. En el anillo de matrices $\mathbb{M}_n(K)$, con coeficientes en un cuerpo K, las unidades son las matrices con determinante no nulo. Más generalmente, si consideramos el anillo de matrices $\mathbb{M}_n(C)$, cuyos coeficientes se encuentran en un anillo conmutativo C, las matrices invertibles son aquellas cuyo determinante es invertible.

4. El anillo $K \times K$, con las operaciones por cordenadas, tiene como unidades precisamente a los elementos con tonas sus coordenadas no nulas.

5. En el anillo $\mathbb{Z}[x]$, de polinomios con coeficientes enteros, las unidades son 1 y -1. Más generalmente, para todo "dominio" D, es decir para todo anillo conmutativo sin divisores de cero, las unidades de $D[x]$ son las unidades del anillo D.

6. En el anillo de polinomios $\mathbb{Z}/4\mathbb{Z}[x]$, de polinomios con coeficientes en el anillo $\mathbb{Z}/4\mathbb{Z}$ de enteros módulo 4, el elemento $1+2x$ es una unidad, ya que se tiene la relación

$$(1+2x)(1-2x) = 1 - 4x^2 = 1.$$

En estas notas trabajaremos intensamente con anillos cocientes, por lo que ejemplos como este último nos resultan particularmente interesantes.

1.2 Dominios Euclideanos

Recordemos que un dominio de integridad D se dice un dominio euclideano (DE) si existe una función $g : (D\backslash\{0\}) \to \mathbb{N}$ que satisface la propiedad siguiente:

> Para todo elemento $m \in D$, y para todo $n \in D\backslash\{0\}$, existen elementos q y r en D, llamados el cociente y el resto, que satisfacen las relaciones siguientes:
>
> $$n = qm + r \quad y \quad \Big(g(r) < g(m) \text{ o } r = 0\Big).$$

En este caso se dice que la función g es un algoritmo de Euclides en D. La existencia de un algoritmo de Euclides en D tiene importantes consecuencias en la estructura de D. En el anillo $\mathbb{Z}$, la función $g(n) = |n|$ es un algoritmo de Euclides, lo que hace del anillo $\mathbb{Z}$ un dominio Euclideano. Mas precisamente, se tiene el siguiente resultado:

Proposición 1.2. *Si a y b son enteros con $b \neq 0$, existen enteros q y r únicamente determinados, que satisfagan las propiedades siguientes:*

1. $a = bq + r$,
2. $0 \leq r < |b|$.

Demostración: Sea $b \neq 0$ un entero fijo, pero arbitrario. Probaremos el resultado para $a, b \geq 0$ por inducción completa en a. Suponemos que la conclusión se cumple para todo entero no negativo menor que a. Si $a < b$, basta tomar $q = 0$ y $r = a$. Si a no es menor que b, entonces $a - b \geq 0$ y

podemos utilizar la hipótesis de inducción para escribir $a - b = q'b + r'$ con $0 \leq r' < b$. Ahora definimos $q = q' + 1$ y $r = r'$. Se sigue del siguiente cálculo:

$$qb + r = (q' + 1)b + r' = (q'b + r') + b = (a - b) + b = a,$$

que la conclusión es cierta para a, y por lo tanto para todo entero no negativo por inducción completa. Si a es negativo y b es positivo, escribimos $-a = q'b + r'$ con $0 \leq r' < b$ por lo ya demostrado, y a continuación definimos q y r, en términos de los elementos q' y r', como sigue:

1. Si $r' = 0$, definimos $r = 0$ y $q = -q'$.
2. Si $r' > 0$ definimos $q = -q' + 1$ y $r = b - r'$.

En cada caso se comprueba fácilmente que se cumplen las condiciones $a = bq + r$ y $0 \leq r < b$ (o $r = 0$), de donde se tiene lo pedido. Finalmente, el caso en el que b es negativo se reduce al caso positivo cambiando simplemente el signo del cociente, lo que funciona gracias a la observación siguiente:

$$qb + r = (-q)(-b) + r.$$

□

Nótese que la unicidad en el resultado que precede proviene de la condición de que el resto sea un entero positivo. En la práctica esta condición puede ignorarse, para escribir la división de 312 por 65 como $312 = 65 \times 5 - 8$, en lugar de $312 = 65 \times 4 + 57$ como estamos acostumbrados. Esta observación tiene importantes consecuencias para el algoritmo de Euclides, que estudiaremos en la sección siguiente.

Proposición 1.3. *Si a y b son enteros con $b \neq 0$, existen enteros q y r que satisfacen las propiedades siguientes:*

1. $a = bq + r$,
2. $0 \leq |r| \leq \frac{1}{2}|b|$.

Demostración: Asumamos primero que b e positivo. Escribamos $a = q'b + r'$, donde q' y r' son como en la proposición precedente. En este caso se tiene $q'b \leq a \leq (q' + 1)b$. Sea $r'' = b - r'$. Podemos escribir alternativamente $a = (q' + 1)b + (-r'')$. Afirmamos que, o bien $r' \leq \frac{b}{2}$, o bien $r'' = |-r''| \leq \frac{b}{2}$.

Esto terminará la demostración. Para probar la afirmación, observamos que r' y r'' son ambos positivos y satisfacen $r' + r'' = b$. Si fuesen ambos mayores que $\frac{b}{2}$ su suma debería ser mayor a b, lo que es absurdo. El caso en el que b es negativo se cubre como antes. □

1.3 Máximo común divisor

Un ideal I de un anillo conmutativo A se dice principal si es el ideal principal generado por algún elemento de A, es decir, si existe un elemento $a \in A$ tal que $I = aA = (a)$.

Proposición 1.4. *En un DE todo ideal es principal.*

Demostración Sea I un ideal no nulo en el dominio euclideano D. Sea $m \in I$ un elemento no nulo tal que $g(m)$ es minimal. Sea $n \in I$ un elemento arbitrario. Entonces $n = mq + r$ con $g(r) < g(m)$ o $r = 0$. Nótese que $r \in I$. Por la minimalidad de m, la alternativa $g(r) < g(m)$ es imposible, por lo que solo puede ser $r = 0$, es decir $n = qm$. Como $n \in I$ es arbitrario, $I = (m)$, como se afirmaba. □

Ejemplo 1.5. En el anillo de enteros $\mathbb{Z}$ todo ideal es principal. De hecho, todo ideal de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ para algún $n \in \mathbb{Z}$. Nótese que esto incluye el caso $n = 0$, lo que nos dá el ideal nulo $(0) = \{0\}$, y el caso $n = \pm 1$, lo que nos dá el ideal completo $(1) = (-1) = \mathbb{Z}$.

definición 1.6. Un dominio de integridad D donde cada ideal es principal recibe el nombre de dominio de ideales principales (DIP). En un DIP, para todo par de elementos n y m el ideal $I = (m) + (n)$ es un ideal principal. Un generador d de I recibe el nombre de máximo común divisor de m y n. Todo DE es un DIP por lo ya demostrado. En particular, $\mathbb{Z}$ es un DIP.

Dados elementos m y n en D, diremos que m divide a n o que m es un divisor de n, en simbolos, $m|n$, si existe $t \in D$ tal que $n = mt$. En particular $m|n$ si y sólo si $(n) \subseteq (m)$. Dado que el máximo común divisor d de m y n satisface $(d) = (n) + (m)$, existen r y s en D tales que $d = rn + ms$. En particular, todo divisor común de n y m debe dividir a d. Por otro lado, como (d) contiene a (m) y (n) se tiene que d es efectivamente un divisor común de m y n. De allí su nombre.

Existe un algoritmo sencillo para encontrar el máximo común divisor de dos elementos n y m en un DE arbitrario D, así como para escribirlo como una combinación del tipo $nu+mv$. Para ello, dividimos n por m obteniendo:

$$n = q_0 m + r_0,$$

con $g(r_0) < g(m)$. A continuación dividimos de nuevo e iteramos

$$m = q_1 r_0 + r_1,\ r_0 = q_2 r_1 + r_2, \ldots, r_i = q_{i+2} r_{i+1} + r_{i+2}, \ldots$$

con $g(r_0) > g(r_1) > g(r_2) > \ldots$.

Proposición 1.7. *En el algorithmo precedente, el último resto distinto de* 0 *que se obtiene es el máximo común divisor.*

Demostración Sea I el ideal $(n)+(m)$. Como $n-q_0 m = r_0$ y $m-q_1 r_0 = r_1$, se tiene que r_0 y r_1 están en I. Dado que $r_{i+2} = r_i - q_{i+2} r_{i+1}$, se prueba por inducción que cada nuevo resto está en el ideal I. Por otro lado si r_t es el último resto no nulo, se tiene que $r_{t-1} = q_{t+1} r_t$, de donde $r_{t-1} \in (r_t)$. Como $r_i = q_{i+2} r_{i+1} + r_{i+2}$ se prueba inductivamente que todos los restos anteriores están en (r_t). Como $m = q_1 r_0 + r_1$, se tiene que m está en (r_t). Finalmente, $n = q_0 m + r_0$ implica $n \in (r_t)$. Se concluye que $(r_t) = I$. □

Si se utiliza la notación $(n, m) = (n) + (m)$, como haremos en todo lo que sigue, lo que se demuestra arriba es la relación $(r_t) = (n, m)$. Es posible profundizar esta observación notando que las ecuaciones $r_{t-1} = q_{t+1} r_t$ y $r_{t-2} = q_t r_{t-1} + r_t$ demuestran que $(r_{t-2}, r_{t-1}) \subseteq (r_t)$, mientras que, al despejar $r_t = -q_t r_{t-1} + r_{t-2}$, se obtiene la contención inversa $(r_t) \subseteq (r_{t-2}, r_{t-1})$. Iterando este argumento, se obtiene la cadena de identidades siguiente:

$$(r_t) = (r_{t-2}, r_{t-1}) = (r_{t-3}, r_{t-2}) = \ldots = (m, r_0) = (n, m).$$

Alternativamente, uno puede interpretar las ecuaciones $r_{t-1} = q_{t+1} r_t$ y $r_{t-2} = q_t r_{t-1} + r_t$ como la siguiente identidad matricial:

$$\begin{pmatrix} r_t \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{t+1} \end{pmatrix} \begin{pmatrix} r_{t-1} \\ r_t \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{t+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_t \end{pmatrix} \begin{pmatrix} r_{t-2} \\ r_{t-1} \end{pmatrix}.$$

Iterando esta interpretación obtenemos la identidad

$$\begin{pmatrix} r_t \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{t+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_t \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \begin{pmatrix} n \\ m \end{pmatrix},$$

la que puede utilizarse para encontra los elementos r u y v que satisfacen la relación $r_t = un + vm$. De hecho, son los coeficientes superiores del producto de matrices de arriba. En otras palabras, existen elementos $w, z \in D$ que satisfacen la identidad siguiente:

$$\begin{pmatrix} u & v \\ w & z \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{t+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_t \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}.$$

Ejemplo 1.8. Calcularemos el maximo común divisor de 148 y 256. Comenzamos dividiendo 256 por 148.

$$256 = 1 \times 148 + 108.$$

A continuacuón dividimos el divisor por el resto, e iteramos:

$$148 = 1 \times 108 + 40,\ 108 = 2 \times 40 + 28,\ 40 = 1 \times 28 + 12,$$

$$28 = 2 \times 12 + 4,\ 12 = 3 \times 4 + 0.$$

El último resto distinto de 0 es el máximo común divisor, es decir 4. Para encontrar u y v se procede multiplicando las matrices correspondientes:

$$\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 11 & -19 \\ -37 & 64 \end{pmatrix}.$$

Esto nos da la expresión $4 = 11 \times 256 - 19 \times 148$.

Ejemplo 1.9. Repetimos ahora el cálculo precedente considerando la posibilidad de que los restos sean negativos. La primera división nos da $256 = 2 \times 148 - 40$. Las subsecuentes nos dan

$$148 = (-4) \times (-40) - 12, \qquad -40 = 3 \times (-12) - 4,$$

y finalmente $-12 = 3 \times (-4)$. El producto de matrices queda como sigue:

$$\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} -11 & 19 \\ 37 & -64 \end{pmatrix}.$$

Esto nos da la expresión $(-4) = (-11) \times 256 + 19 \times 148$. Nótese el cambio de signo en el máximo común divisor.

Es posible ahorrar algo de tiempo utilizando la relación

$$\begin{pmatrix} r_{t-1} \\ r_t \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_t \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \begin{pmatrix} n \\ m \end{pmatrix},$$

en la que no se emplea el último resto, ya que esto permite disminuir en uno el número de matrices a multiplicar. En este caso, los elementos u y v aparecen en la fila inferior de la matriz producto.

1.4 Asociados y factorización única

definición 1.10. Sea D un dominio de integridad. Sean $n, n' \in D$. Diremos que n' es asociado de n, si se tienen simultaneamente $n'|n$ y $n|n'$. Equivalentemente, dos elementos, n y n' son asociados si y sólo si generan el mismo ideal principal, es decir $(n) = (n')$. Observese que si $n = tn'$ y $n' = t'n$ entonces $n(tt' - 1) = 0$. Dado que D es un dominio, se puede concluir que $tt' = 1$, por lo que t y t' son unidades del anillo D. Se concluye que dos elementos, n y n' son asociados si y sólo si existe una unidad $u \in D^*$ tal que $n' = un$. Los asociados de 1 son precisamente las unidades del dominio D.

definición 1.11. Sea D un dominio de integridad. Sea $p \in D - \{0\}$. El elemento p se dice primo, si para todo par de lementos a y b en D, la condición $p|ab$ implica $p|a$ o $p|b$. Equivalentemente, $p \neq 0$ es primo si y sólo si el ideal (p) es primo´, es decir $D/(p)$ es un dominio de integridad. En particular, todo asociado de un primo es un primo.

Proposición 1.12. *Sea D un DIP. Un elemento $p \in D$ es primo si y sólo si el ideal (p) es maximal.*

Demostración. Recordemos que un ideal es maximal si y sólo si el correspondiente cociente es un cuerpo, como se concluye del hecho de que todo elemento no invertible genera un ideal principal propio (ver apuntes de grupos y anillos para más detalles). Por esta razón, si (p) es maximal, en particular es primo, ya que todo cuerpo es un dominio de integridad. Por otro lado, si (p) no es maximal, entonces está propiamente contenido en un ideal maximal (p'). En particular, p' divide a p. Se sigue que $p = tp'$, y como p no divide a p', debe dividir a t. Luego $t = ps$, de donde $p = tp' = psp'$. Se concluye que $sp' = 1$, pero esto es imposible ya que asumimos que (p') era un ideal propio. □

Proposición 1.13. *Todo elemento de un DIP D que no es una unidad es divisible por un elemento primo.*

Demostración. Esto es inmediato, ya que todo ideal está contenido en un ideal maximal, cómo se demuestra mediante un sencillo razonamiento vía lema de Zorn (esto requiere caracterizar los ideales propios como ideales que no contienen al 1, vea los apuntes de grupos y anillos para más detalles). □

Proposición 1.14. *En un DIP D, cada elemento no nulo es producto de primos y unidades.*

Demostración. Por la proposición precedente, en un DIP todo elemento $n \notin D^*$ puede escribirse en la forma $n = p_1 n_1$. Si n_1 no es una unidad podemos repetir el proceso y escribir $n = p_1 p_2 n_2$. Iterando, si el algún momento se llega a algún $n_r \in D^*$, por lo que se habrá escrito n como producto de primos y unidades. En principio, la otra alternativa sería obtener una cadena infinita estrictamente ascendente de ideales

$$(n) \subset (n_1) \subset (n_2) \subset \ldots,$$

donde cada nuevo elemento n_i divide al anterior n_{i-1} pero no a la inversa. Afirmamos que esto no puede ocurrir. Para ello definimos el conjunto

$$I = \{a \in D | n_t \text{ divide a } a \text{ para algún } t \in \mathbb{N}\}.$$

Afirmamos que I es un ideal. De hecho, si n_t divide a a, entonces divide a ab para todo $b \in D$. Por otro lado, si n_t divide a a, y si n_s divide a b, entonces $n_{\max\{t,s\}}$ divide a ambos a y b, por lo que divide también a $a+b$. Como D es un DIP, debe tenerse $I = (d)$ para algún $d \in D$. En particular, el generador d pertenece a I. Por definición de I, el elemento d debe ser divisible por algún n_t, de donde $n_{t+1} \in I = (d) \subseteq (n_t)$, lo que contradice la construcción de los n_t's. □

La descomposición de un elemento n no es única, dado que siempre es posible remplazar un primo por uno de sus asociados y cambiar las unidades. Por ejemplo, en $\mathbb{Z}$ se tiene

$$4 = 2 \times 2 = (-2) \times (-2) = (-1) \times 2 \times (-2).$$

Sin embargo, esta es la única excepción. Antes de demostrarlo necesitamos un lema.

Lema 1.15. *Si p y q son primos del DIP D, y si p divide a q, entonces p y q son asociados.*

Demostración. Si p divide a q entonces $(q) \subseteq (p)$. Como el ideal (q) es maximal, see concluye la igualdad $(q) = (p)$. □

Proposición 1.16. *Sea D un DIP. Sea*

$$n = up_1^{\alpha_1} \dots p_r^{\alpha_r} = vq_1^{\beta_1} \dots q_s^{\beta_s}, \tag{1.1}$$

donde $p_1, \dots, p_r$ son primos no asociados por pares, y lo mismo ocurre con $q_1, \dots, q_s$. Entonces $s = r$, y existe una permutación σ de $\mathbf{r} = \{1, \dots, r\}$ tal que p_i es asociado a $q_{\sigma(i)}$ y $\alpha_i = \beta_{\sigma(i)}$.

Demostración. Por inducción en t. Si $t = 0$, entonces n es una unidad y no hay nada que probar. Supongamoslo cierto para $t - 1$. Como p_t es primo, éste debe dividir a algún q_j, y por lo tanto debe ser asociado a él. re-enumerando los elementos $q_1, \dots, q_s$ si es necesario, podemos suponer que $j = s$. Digamos $q_s = wp_r$ con $w \in D^*$. Entonces simplificando en (1.1) se tiene

$$up_1^{\alpha_1} \dots p_r^{\alpha_r - 1} = (vw^{-1})q_1^{\beta_1} \dots q_s^{\beta_s - 1}.$$

Si $\alpha_r > 1$, el lado izquierdo es aún divisible por p_1 por lo que tambien lo es el derecho. Se concluye que $\beta_s > 1$. Iterando este procedimiento se tiene $\alpha_r \leq \beta_s$, y por simetría $\alpha_r = \beta_s$. simplificando $p_r^{\alpha_r}$ a ambos lados se tiene:

$$up_1^{\alpha_1} \dots p_{r-1}^{\alpha_{r-1}} = (vw^{-r})q_1^{\beta_1} \dots q_{s-1}^{\beta_{s-1}},$$

por lo que se puede aplicar la hipótesis de inducción. □

1.5 Ejercicios

1. Sean m y n dos enteros positivos y d su máximo común divisor. El mínimo común múltiplo de m y n se define como el generador positivo r del ideal $n\mathbb{Z} \cap m\mathbb{Z}$. Probar que $rd = mn$.

2. Encuentre el máximo común divisor de 6.528 y 3.791.

3. Encuentre enteros positivos t y s tales que $190t + 455s = 5$.

4. Encuentre enteros a y b tales que

$$\frac{a}{155} + \frac{b}{341} = \frac{2}{1705}.$$

5. Probar que si m, n, y t son tres enteros positivos, tales que ningún primo divide simultaneamente a los tres, entonces existen enteros a, b, y c tales que $am + bn + ct = 1$.

6. Una ranita está parada sobre una cinta infinita dividida en casillas, cómo en la Figura 1.1. Asumiendo que la ranita sólo puede dar saltos de largo 5 y 8 (tanto adelante como hacia atrás), demuestre que la ranita es capaz de visitar cualquier casilla del tablero. Si la ranita

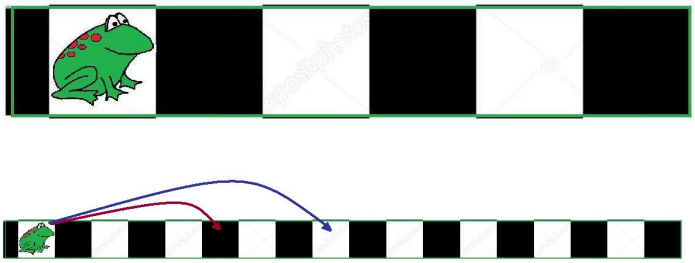

Figure 1.1: Una ranita en una cinta infinita.

puede dar saltos de tamaño n y m, que condición en estos números asegura que la ranita puede visitar cualquier casilla de la cinta?

Chapter 2

Congruencias

Si J un ideal de un anillo conmutativo A, el cociente A/J es un anillo con operaciones derivadas de las operaciones correspondientes de A, por ejemplo

$$(a+J)(b+J) \subseteq ab + aJ + Jb + JJ \subseteq ab + J + J + J = ab + J.$$

lo que muestra que el producto es una operación bien definida en el cociente A/J. Para todo anillo A, el anillo cociente $A/(0)$ es isomorfo al anillo A, mientras que A/A es el anillo trivial con un elemento. Estos son los cocientes triviales del anillo A. Cualquier otro cociente se dice no trivial. Cuando $A = D$ es un DIP, los ideales de D son los ideales principales de la forma nD para algún elemento $n \in D$. En este caso el anillo cociente D/nD recibe el nombre de anillo módulo D. Este uso está particularmente extendido en el caso $D = \mathbb{Z}$, donde el anillo cociente $\mathbb{Z}/n\mathbb{Z}$ recibe el nómbre de anillo de enteros módulo n. Tendremos bastante que decir sobre este tipo de anillo cociente en estas notas. Los elementos de un cociente A/J se denotan a menudo por $\bar{a} = a + J$, En estas notas, emplearemos a menudo la notación alternativa en la que elementos del cociente son considerados elementos del anillo original con una "igualdad modificada", con la que una identidad del tipo $a + J = b + J$ se denota más bien $a \equiv b \,(\mathrm{mod}\, J)$. En el caso de un ideal principal de la forma $J = nA$, se usa a menudo la forma $a \equiv b \,(\mathrm{mod}\, n)$. Estas notaciones están tan extendidas en álgebra y teoría de números, que no serán explicadas mayormente aquí.

A menudo, al escribir un cociente del tipo A/J, se asume tácitamente que se trata de un cociente no trivial. Por ejemplo, si $A = \mathbb{Z}$, al hablar del anillo de enteros módulo n $\mathbb{Z}/n\mathbb{Z}$, se asume que n no es 0 ni ± 1.

2.1 Inversos módulo n

Podemos caracterizar fácilmente los elementos invertibles, o unidades, en el anillo D/nD utilizando los resultados del capítulo precedente. De hecho, tenemos el siguiente resultado:

Proposición 2.1. *Una clase residual $a+nD$ es invertible en el anillo D/nD si y sólo si a es relativamente primo con n.*

Demostración. Si a y n son relativamente primos, entonces existen enteros t y s tales que $at + ns = 1$. Se concluye que

$$(a + nD)(t + nD) = (at + nD) = (at + ns + nD) = (1 + nD).$$

Por otro lado, si se tiene que

$$(a + nD)(t + nD) = (1 + nD)$$

para algún elemento $t \in D$ entonces $at - 1 \in nD$, o en otras palabras $at - 1 = ns$ para algún elemento $s \in D$, de donde se sigue que $at + ns = 1$, y por lo tanto a es relativamente primo con n. □

Podemos utilizar la relación entre el inverso de a módulo n con las soluciones de $at+ns = 1$ para dar un procedimiento alternativo que nos permita escribir 1 como combinación lineal de dos elementos relativamente primos. Este se describe en el siguiente ejemplo:

Ejemplo 2.2. Queremos encontrar enteros s y t tales que $143s + 225t = 1$. Para ello re-escribimos el problema como la congruencia $225t \equiv 1 \pmod{143}$, lo que es equivalente a $82t \equiv 1 \pmod{143}$, puesto que 225 es congruente a 82 módulo 143. Volvemos a re-escribir la ecuación como $82t + 143p = 1$, la cual puede escribirse nuevamente como la congruencia $143p \equiv 1 \pmod{82}$, o, simplificando, como $61p \equiv 1 \pmod{82}$. Iteramos el procedimiento algunas veces más, obteniendo las relaciones siguientes:

$$61p + 82k = 1, \qquad 82k \equiv 1 \pmod{61}, \qquad 21k \equiv 1 \pmod{61},$$

$$61q + 21k = 1, \qquad 61q \equiv 1 \pmod{21}, \qquad -2q \equiv 1 \pmod{21}.$$

De esta última relación se obtiene $q \equiv -11 \equiv 10 \pmod{21}$, y, de la solución $q = 10$, se concluyen fácilmente las soluciones $k = -29$, $p = 39$, y finalmente $t = -68$ y $s = 107$.

Dejamos al lector la terea de entender por qué este procedimiento es equivalente al algoritmo de Euclides.

En álgebra, hay un segundo ejemplo de dominio euclideano tan utilizado como el anillo $\mathbb{Z}$. Es el anillo de polinomios $K[x]$, de polinomios en una indeterminada x y con coeficientes en un cuerpo K. Si A es un álgebra (con 1) sobre K y $a \in A$ es cualquier elemento, el ideal I_a formado por los polinomios que se anulan al evaluarlos en a es un ideal principal generado por el polinomio minimal $m_a(x)$. La función evaluación $\phi_a : K[x] \to A$ es un homomorfismo de anillos, es decir una función que preserva sumas, productos y lleva el 1 de K en el 1 de A. Su imagen es el sub-anillo $K[a] \subseteq A$, mientras que su núcleo es el ideal I_a. El primer teorema de isomorfía de la teoría de anillos establece la existencia de un isomorfismo entre el anillo cociente $K[x]/(m_a)$ y el anillo $K[a]$, el que comunmente recibe el nombre de anillo generado por a. El anillo $K[a]$ es un cuerpo, por lo tanto, precisamente cuando el polinomio minimal $m_a \in K[x]$ es primo (en el caso de polinomios se usa a menudo la palabra irreductible).

Ejemplo 2.3. Queremos encontrar el inverso del complejo $1+i$. Esto puede hacerse de dos maneras. La tradicional es racionalizar, como sigue:

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

Una alternativa es resolver la ecuación $s(x)(1+x) + t(x)(x^2+1) = 1$, para luego evaluar en i. Este segundo procedimiento es enteramente análogo a lo hecho más arriba con enteros. Las división $x^2 + 1 = (x+1)(x-1) + 2$ nos dá la solución $2 = (x^2+1) - (x+1)(x-1)$, de donde se obtiene el resultado precedente.

Ejemplo 2.4. En un ejemplo algo más elaborado, se quiere calcular el inverso de $\eta^3 - 2 \in \mathbb{Q}[\eta]$, donde η es una raiz quinta primitiva de la unidad, cuyo polinomio irreducible es $1+x+x^2+x^3+x^4$. Para esto, buscamos una solución de la ecuación

$$(1 + x + x^2 + x^3 + x^4)t(x) + (x^3 - 2)s(x) = 1.$$

Reduciendo módulo $x^3 - 2$, o, lo que viene a ser lo mismo, evaluando en la raiz $\sqrt[3]{2}$, se obtiene la identidad

$$\left(1 + \sqrt[3]{2} + (\sqrt[3]{2})^2 + (\sqrt[3]{2})^3 + (\sqrt[3]{2})^4\right) t\left(\sqrt[3]{2}\right) = 1.$$

Simplificando esta última expresión nos dá

$$\left(3 + 3\sqrt[3]{2} + (\sqrt[3]{2})^2\right) t\left(\sqrt[3]{2}\right) = 1,$$

lo que es equivalente a la ecuación

$$(3 + 3x + x^2)t(x) + (x^3 - 2)u(x) = 1.$$

Para resolver esta última evaluamos en $\alpha = \frac{-3+\sqrt{-3}}{2}$, una raiz del primer polinomio. Dado que $\alpha^2 = -3(\alpha + 1)$, obtenemos lo siguiente:

$$1 = (\alpha^3 - 2)(\alpha) = \Big(- 3(\alpha + 1)\alpha - 2\Big)u(\alpha) = (-3\alpha^2 - 3\alpha - 2)u(\alpha)$$

$$= (6\alpha - 7)u(\alpha).$$

Una vez más, esta ecuación equivale a

$$(3 + 3x + x^2)w(x) + (6x + 7)u(x) = 1,$$

la que se resuelve evaluando en $-\frac{7}{6}$. Esto dá la condición

$$w\left(-\frac{7}{6}\right) = \left(3 + 3\left(-\frac{7}{6}\right) + \left(-\frac{7}{6}\right)^2\right)^{-1} = \frac{36}{31}.$$

Escogiendo el valor constante para w se tienen las soluciones sucesivas $w(x) = \frac{36}{31}$, $u(x) = \frac{-6x-11}{31}$, $t(x) = \frac{6x^2-7x+3}{31}$ y, finalmente, $s(x) = \frac{-6x^3+x^2-2x-14}{31}$. Esto nos dice que el valor del inverso es $(\eta^3 - 2)^{-1} = s(\eta) = \frac{-6\eta^3+\eta^2-2\eta-14}{31}$.

Dejamos al lector el desafío de repetir el cálculo precedente utilizando el método matricial descrito en el Capítulo 1, para hacerse una idea de qué método es mejor. Lo mismo vale para el cálculo de inversos resolviendo un sistema ecuaciones lineales para los coeficientes de s.

Otra propiedad de los inversos que ocuparemos a menudo es la siguiente:

Proposición 2.5. *Sea K el cuerpo de cocientes del anillo D y sea $B \subseteq K$ el anillo formado por todas aquellas fracciones de la forma $\frac{r}{s}$ con n y s relativamente primos. Entonces existe un homomorfismo de B a D/nD que lleva cada elemento de D a su clase lateral correspondiente.*

Demostración. Esto no es otra cosa que un ejemplo de la propiedad universal de la localización (ver apuntes de grupos y anillos), pero damos aquí una demostración independiente. El homomorfismo se define por $\phi\left(\frac{r}{s}\right) = \bar{r}\bar{s}^{-1}$. Demostrar que es un homomorfismo de anillos se reduce a las comprobaciones siguientes:

$$\phi\left(\frac{rr'}{ss'}\right) = \left(\overline{rr'}\right)\left(\overline{ss'}^{-1}\right) = \left(\bar{r}\bar{s}^{-1}\right)\left(\bar{r}'\bar{s}'^{-1}\right) = \phi\left(\frac{r}{s}\right)\phi\left(\frac{r'}{s'}\right),$$

$$\phi\left(\frac{rs'+sr'}{ss'}\right) = \left(\overline{rs'+sr'}\right)\left(\overline{ss'}^{-1}\right) = \left(\bar{r}\bar{s}^{-1}\right) + \left(\bar{r}'\bar{s}'^{-1}\right) = \phi\left(\frac{r}{s}\right) + \phi\left(\frac{r'}{s'}\right).$$

□

Cuando $n = p$ es un primo, el anillo B se denota $D_{(p)}$. Estos anillos, llamados anillos locales racionales (como opuesto a los anillos locales completos que aparecen en un capítulo posterior), jugarán un papel importante en todo lo que sigue.

2.2 Elementos idempotentes y productos de anillos

Si A y A' son anillos conmutativos, su producto cartesiano $A \times A'$ es un anillo conmutativo con las operaciones por coordenadas, es decir las siguientes:

$$(a, a') + (b, b') = (a + b, a' + b'), \qquad (a, a')(b, b') = (ab, a'b').$$

Esta definición puede generalizarse a productos arbitrarios y a anillos no conmutativos, pero no la necesitamos aquí. Dado un anillo A, nos gustaría saber si existen anillos A_1 y A_2 tales que $A \cong A_1 \times A_2$ y de cuantas maneras puede, un anillo dado, escribirse como producto. A diferencia de lo que ocurre en las categorías de grupos y grupos abelianos, el número de maneras en que un anillo puede escribirse como un producto está fuertemente restringido por la existencia de un tipo particular de elementos denominados idempotentes.

definición 2.6. Un elemento $P \in A$ se dice idempotente si $P^2 = P$.

Si $A \cong A_1 \times A_2$, los elementos $(0, 1)$ y $(1, 0)$ son idempotentes de A. Inversamente, probaremos en esta sección que si A tiene idempotentes no triviales, entonces A es un producto.

Lema 2.7. *Si P es un idempotente, entonces $P^c := (1 - P)$ es un idempotente.*

Demostración. $(1-P)^2 = 1-P-P+P^2 = 1-P-P+P = 1-P$. □

A P^c se le llama el complemento de P. Tambien se dice que P y P^c son complementarios. Nótese que se satisfacen las relaciones $P + P^c = 1$ y $PP^c = 0$.

Lema 2.8. *Si P es un idempotente de A, entonces PA es un anillo con unidad $1_{PA} = P$.*

Nótese, sin embargo, que PA no se considera un subanillo de A con la convención de que anillo significa anillo unitario, ya que las unidades 1_A y 1_{PA} de ambos anillos son diferentes.

Demostración. Nótese que PA es un subgrupo, dado que $a \mapsto Pa$ es homomorfismo de grupos. Además, la multiplicación es una operación cerrada, como lo muestra el siguiente cálculo:

$$PAPA = P^2AA = PAA \subseteq PA.$$

Finalmente, todo elemento $x \in PA$ puede escribirse en la forma $x = Py$, de donde se concluye lo siguiente: $Px = PPy = Py = x$. □

Lema 2.9. *Si P es un idempotente central, entonces $A \cong PA \times P^cA$.*

Demostración. La cadena de contenciones

$$A \supseteq PA + P^cA \supseteq (P + P^c)A = A$$

nos demuestra que la suma $PA+P^cA$ es igual a A. Si se tiene $x \in PA \cap P^cA$, entonces $x = Px = PP^cx = 0$. Esto prueba que A es la suma directa $PA \oplus P^cA$ como grupos abelianos. Si $a \in PA$ y $b \in P^cA$, entonces $ab = PaP^cb = PP^cab = 0$. De aqui sigue que si $a \in A$ se escribe como $a = a_1 + a_2$ con $a_1 \in PA$ y $a_2 \in P^cA$, y si $b \in A$ se escribe como $b = b_1 + b_2$ con $b_1 \in PA$ y $b_2 \in P^cA$, se tiene lo siguiente:

$$ab = (a_1 + a_2)(b_1 + b_2) = a_1b_1 + a_1b_2 + a_2b_1 + a_2b_2 = a_1b_1 + a_2b_2.$$

De donde se concluye el isomorfismo de anillos $A \cong PA \times P^cA$. □

Nótese que para cada par de elementos a y b de A se tiene $(Pa)(Pb) = Pab$. En párticular, la función $x \mapsto Px$ es un homomorfismo de anillos cuyo núcleo es P^cA. Se concluye del primer teorema de isomorfía para anillos que $PA \cong A/P^cA$. Se sigue que el resultado precedente puede re-escribirse como

$$A \cong \frac{A}{P^cA} \times \frac{A}{PA}.$$

Esta última forma es más útil para calcular.

Ejemplo 2.10. En $\mathbb{Z}/6\mathbb{Z}$ el elemento $3 + 6\mathbb{Z}$ es idempotente. Tambien lo es su complemento $(1 + 6\mathbb{Z}) - (3 + 6\mathbb{Z}) = 4 + 6\mathbb{Z}$. Se concluye que:

$$\mathbb{Z}/6\mathbb{Z} \cong (3 + 6\mathbb{Z})\mathbb{Z}/6\mathbb{Z} \times (4 + 6\mathbb{Z})\mathbb{Z}/6\mathbb{Z}.$$

Por otro lado, se tiene el isomorfismo

$$(4 + 6\mathbb{Z})\mathbb{Z}/6\mathbb{Z} \cong \frac{\mathbb{Z}/6\mathbb{Z}}{3\mathbb{Z}/6\mathbb{Z}} \cong \mathbb{Z}/3\mathbb{Z}.$$

Del mismo modo, si recordamos que la imagen de un subgrupo H en el cociente G/K es $(H + K)/K$, tenemos la siguiente cadena de isomorfismos:

$$(3 + 6\mathbb{Z})\mathbb{Z}/6\mathbb{Z} \cong \frac{\mathbb{Z}/6\mathbb{Z}}{4(\mathbb{Z}/6\mathbb{Z})} = \frac{\mathbb{Z}/6\mathbb{Z}}{(4\mathbb{Z} + 6\mathbb{Z})/6\mathbb{Z}} \cong \mathbb{Z}/(4\mathbb{Z} + 6\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z},$$

ya que $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$, por ser 2 el máximo común divisor de 4 y 6. La conclusión final es la siguiente:

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Esta es una primera instancia del teorema chino de los restos, que se estudiará con más detalle en la sección siguiente.

La principal filosofía en lo que respecta a los idempotentes de un anillo conmutativo, es que estos se comportan como los subconjuntos de un espacio. Más precisamente, el conjunto de idempotentes de un anillo es un álgebra booleana. No entraremos en los detalles de esta teoría en estas notas, pero recordar las propiedades de las operaciones de unión, intersección y complemento es a menudo útil en este estudio.

definición 2.11. Sean P_1 y P_2 idempotentes de A. Diremos que $P_1 < P_2$ si $P_1P_2 = P_1$.

Proposición 2.12. *$P_1 < P_2$ si y sólo si $P_1A \subseteq P_2A$.*

Demostración. Si $P_1 < P_2$, entonces $P_1P_2 = P_1$. Luego $P_1A = (P_1P_2)A = P_2(P_1A) \subseteq P_2A$. Por otro lado, si $P_1A \subseteq P_2A$, entonces $P_1 \in P_2A$, luego $P_1P_2 = P_1$. □

Proposición 2.13. *Sean P_1 y P_2 idempotentes que satisfacen $P_1P_2 = 0$. Si $P = P_1 + P_2$, entonces P es un idempotente, y se tiene la identidad $PA = P_1A \oplus P_2A$ y el isomorfismo $PA \cong P_1A \times P_2A$.*

Demostración. $(P_1 + P_2)^2 = P_1^2 + P_1P_2 + P_2P_1 + P_2^2 = P_1 + P_2$. Las restantes afirmaciones son un caso particular de $A \cong PA \times P^cA$, aplicado al anillo PA, dado que P es la unidad de PA, mientras que $P - P_1 = P_2$, por lo que P_2 y P_1 son complementarios en ese anillo. □

Dos idempotentes que satisfacen $P_1P_2 = 0$ suelen denominarse disjuntos. Si se tiene una familia $\{P_1, \ldots, P_n\}$ en la que cada par de elementos distintos son disjuntos, diremos que $P_1, \ldots, P_n$ son disjuntos a pares.

Proposición 2.14. *Si $P_1, \ldots, P_n$ son idempotentes centrales disjuntos a pares que satisfacen $P_1 + \ldots + P_n = 1$, entonces $A \cong P_1A \times \ldots \times P_nA$.*

Demostración. Inducción en la proposición anterior. □

Nótese que el isomorfismo de la proposición precedente puede escribirse también como sigue:

$$A \cong \frac{A}{P_1^cA} \times \ldots \times \frac{A}{P_n^cA}.$$

Si P_1 y P_2 son dos idempotentes en un mismo anillo, podemos ecribir

$$1 = (P_1 + P_1^c)(P_2 + P_2^c) = P_1P_2 + P_1P_2^c + P_1^cP_2 + P_1^cP_2^c,$$

donde los idempotentes de la derecha son disjuntos a pares. Además cada uno de los idempotentes originales es suma de algunos de los idempotentes de la derecha. Esto nos permite, por iteración, encontrar una descomposición de la unidad como suma de idempotentes que incluya como subsumas a los elementos de cualquier familia finita pre-existente de idempotentes. Si el anillo tiene una cantidad finita de idempotentes, por ejemplo si es finito, es posible encontrar una descomposición en idempotentes que son minimales respecto de la relación "<". En este caso diremos que se tiene un conjunto completo de idempotentes.

Ejemplo 2.15. Consideremos el anillo $A = \mathbb{Z}/30\mathbb{Z}$. Para descomponer este anillo como un producto, debemos encontrar un conjunto completo de idempotentes de A. Como $6^2 = 36 \equiv 6$ es idempotente, también lo es su complemento $1-6 \equiv 25$. Esto nos dá una descomposición de A como producto. De hecho $A = 6A \times 25A$. Por otro lado $25A = A/6A \cong \mathbb{Z}/6\mathbb{Z}$. Como ya sabemos que este anillo todavía puede descomponerse como un producto deben existir idempotentes adicionales. De hecho vimos anteriormente que $3+6\mathbb{Z}$ y $4+6\mathbb{Z}$ son idempotentes de $\mathbb{Z}/6\mathbb{Z}$. Como la imagen de a en PA es Pa, el idempotente correspondiente a 3 es $3 \times 25 \equiv 15$ y el idempotente correspondiente a 4 es $4 \times 25 \equiv 10$. Se sigue que $6 + 30\mathbb{Z}$, $15 + 30\mathbb{Z}$, y $10 + 30\mathbb{Z}$, son los idempotentes minimales de A. Concluimos que $A \cong 6A \times 15A \times 10A$, o en la forma más cómoda para calcular $A \cong A/25A \times A/16A \times A/21A$, dado que $25 + 30\mathbb{Z}$, $16 + 30\mathbb{Z}$ y $21 + 30\mathbb{Z}$ son los complementos de $6 + 30\mathbb{Z}$, $15 + 30\mathbb{Z}$ y $10 + 30\mathbb{Z}$, respectivamente. Cómo se tienen las identidades $25\mathbb{Z} + 30\mathbb{Z} = 5\mathbb{Z}$, $16\mathbb{Z} + 30\mathbb{Z} = 2\mathbb{Z}$ y $21\mathbb{Z} + 30\mathbb{Z} = 3\mathbb{Z}$, el isomorfismo anterior se reduce a

$$A \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Los ejemplos precedentes sugieren que la razón por la que un anillo de la forma $\mathbb{Z}/n\mathbb{Z}$ puede escribirse como un producto es que n se factoriza como producto de dos números relativamente primos. Veremos en la siguiente sección que este es de hecho el caso.

El lector ya estará convencido en este punto de que, en el álgebra booleana de idempotentes, el producto juega el papel de intersección, mientras que el complemento que definimos aquí juega el mismo papel que el complemento de conjuntos. La suma de idempotentes disjuntos vendría a ser la unión disjunta, por lo que faltaría definir la unión en general. Esto puede hacerse mediante las Leyes de De'Morgan del álgebra booleana. Para conjuntos, esta ley se escribe

$$A \cup B = (A^c \cap B^c)^c,$$

por lo que resulta natural definir la unión de idempotentes mediante la fórmula siguiente

$$P_1 \cup P_2 = (P_1^c P_2^c)^c = 1 - (1 - P_1)(1 - P_2) = P_1 + P_2 - P_1 P_2.$$

Dejamos al lector la tarea de probar que esta última expresión define un idempotente, así como probar otros resultados conocidos del álgebra booleana.

Todo lo dicho sobre idempotentes en esta sección se extiende a anillos no conmutativos si se agrega la condición de que sean idempotentes centrales,

es decir que conmuten con cualquier elemento del anillo, como ciertamente lo hacen los elementos $(1_A, 0_B)$ y $(0_A, 1_B)$ en un producto $A \times B$.

2.3 El Teorema Chino de los Restos

Recordemos que en un dominio de ideates principales D, para todo par de elementos relativamente primos a y b, existen elementos t y s tales que $at + bs = 1$. Utilizando este resultado puede probarse que todo anillo de la forma D/nmD con n y m relativamente primos se descompone como un producto.

Proposición 2.16. *Sea D un DIP y sean n y m elementos de D relativamente primos. Entonces el anillo $A = D/nmD$ se descompone como un producto, de hecho*

$$D/nmD \cong D/nD \times D/mD.$$

Demostración. Por los resultados de la sección precedente basta ver que existen elementos idempotentes apropiados. Sean t y s elementos de D que satisfacen $tm + sn = 1$. Sean $P_1 = tm + nmD$ y $P_2 = ns + nmD$. Observese que $P_1 + P_2 = 1 + nmD = 1_A$, mientras que, por otro lado, se tiene la congruencia $tm = tm(tm + ns) \equiv (tm)^2 \pmod{mn}$, la que pruena que el elemento P_1 es un idempotente. Se sigue que P_2 es su idempotente complementario. El resultado se concluye si probamos que P_1A y P_2A son isomorfos a los dos factores del lado derecho. Por un lado

$$P_1A \cong A/P_2A \cong D/(nsD + nmD) = D/nD,$$

donde hemos usado que la relación $tm + sn = 1$ implica que m y s son relativamnete primos, de donde $sD + mD = D$ y por lo tanto $nsD + nmD = nD$. La demostración de la relación $P_1A \cong D/mD$ es similar. □

Nótese que, en la demostración anterior, la imagen de una clase $a + nmD$ en $D/nD \times D/mD$ es el par $(a + nD, a + mD)$. En particular, para cada par de enteros b y c existe una única clase $a + nmD$ tal que $(a + nD, a + mD) = (b + nD, c + mD)$. Se concluye el siguiente resultado:

Proposición 2.17. *Sea D un DIP y sean n y m elementos de D relativamente primos. Entonces para cada par de enteros b y c existe un entero a que satisface las ecuaciones*

$$x \equiv b \pmod{n}, \qquad x \equiv c \pmod{m}.$$

Dos soluciones de dicho sistema son congruentes módulo mn. □

Este último resultado es el que se conoce usualmente como Teorema Chino de los Restos. Los resultados anteriores se generalizan fácilmente a un número mayor de factores. De hecho, se tiene el siguiente resultado:

Proposición 2.18. *Sea D un DIP y sean $n_1, \ldots, n_k$ elementos de D relativamente primos a pares. Entonces el anillo $A = Di/nmD$ se descompone como un producto, de hecho*

$$D/(n_1 \cdots n_k)D \cong D/n_1D \times \cdots \times D/n_kD.$$

Demostración. Basta observar que, si $n_1, \ldots, n_k$ son relativamente primos a pares, entonces el producto $n_1 \cdots n_{k-1}$ es relativamente primo con n_k, de donde se concluye lo siguiente

$$D/(n_1 \cdots n_k)D \cong D/(n_1 \cdots n_{k-1})D \times D/n_kD,$$

y el resultado sigue por inducción. □

Del mismo modo que antes, se tiene la consecuencia siguiente:

Proposición 2.19. *Sea D un DIP, y sean $n_1, \ldots, n_k$ elementos de D relativamente primos. Entonces, dados elementos $a_1, \ldots, a_k$, existe un entero a que satisface las ecuaciones*

$$a \equiv a_i \pmod{n_i},$$

para cada $i = 1, \ldots, k$. Dos soluciones de dicho sistema son congruentes módulo $n_1 \cdots n_k$. □

Sea $n = up_1^{r_1} \cdots p_k^{r_k}$ un elemento de D con sus descomposición en factores primos. Entonces tenemos la descomposición

$$\mathbb{Z}/nD \cong D/p_1^{r_1}D \times D/p_k^{r_k}D.$$

Se sigue de lo anterior que para entender la estructura del anillo D/nD es suficiente con entender la estructura de D/p^rD para cada primo p y cada exponente r. Este estudio se realiza en las secciones siguientes.

2.4 Elementos nilpotentes y series de potencias

Los anillos de la forma $A = D/p^rD$ se caracterizan por la existencia de elementos de la forma $\pi = p + p^rD$ que satisfacen $\pi^n = 0$. un elemento con una potencia nula se denomina nilpotente. No es difícil comprobar que los elementos nilpotentes del anillo A son precisamente los múltiplos de π. De hecho, $(m\pi)^r = m^r\pi^r = m^r \cdot 0 = 0$, mientras que lo elementos que no son múltiplos de π son de la forma $m + p^rD$ con m relativamente primo a p^r, y por lo tanto invertibles. Se concluye que el conjunto de elementos nilpotentes es el ideal principal $A\pi$, y todo elemento fuera de $A\pi$ es una unidad. En particular $A\pi$ es el único ideal maximal de A. un anillo con un único ideal maximal se denomina local. Los anillos locales racionales son también anillos locales. El Teorema Chino de los Restos nos permite escribir D/nD como un producto de anillos locales. Esta conclusión es útil para lo que viene en capítulos posteriores.

Los elementos nilpotentes de un anillo conmutativo se comportan en muchos aspectos como los elementos infinitesimales del cálculo no-estándar. Por ejemplo, si u es nilpotente, entonces $1 - u$ tiene inverso multiplicativo. De hecho, el inverso de $1 - u$ puede calcularse mediante una serie de potencias

$$(1 - u)^{-1} = 1 + u + u^2 + \cdots$$

donde la suma tiene sentido ya que, despues de un número finito de sumandos, todos los subsecuentes se anulan. De hecho, si $u^n = 0$ entonces se tiene la relación

$$(1 - u)(1 + u + u^2 + \ldots + u^{n-1}) = 1 - u^n = 1,$$

dedonde se deduce la afirmación anterior.

Ejemplo 2.20. En el anillo $\mathbb{Z}/243\mathbb{Z}$, el elemento $4 + 243\mathbb{Z}$ es invertible, ya que $4 = 1 - (-3)$, y su inverso es

$$1 + (-3) + (-3)^2 + (-3)^3 + (-3)^4 + 243\mathbb{Z} = 61 + 243\mathbb{Z}.$$

De hecho tenemos un resultado más general en este sentido.

Proposición 2.21. *Sea A un anillo conmutativo. Sea u una unidad de a, y sea n un elemento nilpotente en A. Entonces el elemento $u + n$ es invertible y su inverso está dado por*

$$(u - n)^{-1} = u^{-1}(1 + nu^{-1} + n^2u^{-2} + \ldots).$$

Demostración. Basta observar que $1 - nu^{-1}$ es nilpotente y por lo tanto invertible, y que $u^{-1}(1 - nu^{-1})^{-1}$ es un inverso de $u - n$. □

Más generalmente, toda serie de potencias con coeficientes en un anillo puede ser evaluada en un elemeneto nilpotente. Esta función evaluación, al igual que la evaluación de polinomios, es un homomorfismo de anillos. Esto implica que identidades que involucran sumas y productos entre series de potencias pueden trasladarse a identidades entre los elementos que se obtienen al evaluar dichas series en un elemento nilpotente dado. Lo mismo ocurre para la composición, con una salvedad. La composión de series de potencias sólo está bien definida, en el contexto algebraico, cuando se evalua una serie de potencias en una serie con término constante nulo. Bajo tales circunstancias, las identidades que involucran composición de series de potencias se preservan bajo la evaluación sin mayor problema.

Como un ejemplo de aplicación de la técnica ya mencionada, probaremos el siguiente resultado:

Proposición 2.22. *Sea $r < p$ un entero positivo. Entonces el conjunto $U_{p,1} = \{1 + pt + p^r\mathbb{Z} | t \in \mathbb{Z}\}$ es un grupo isomorfo al grupo aditivo $p\mathbb{Z}/p^r\mathbb{Z}$.*

Demostración. Basta definir funciones inversas entre los grupos considerados. En este caso, las mismas están dadas por la función exponencial truncada $\exp_{p,r} : p\mathbb{Z}/p^r\mathbb{Z} \to U_{p,1}$ definida por

$$\exp_{p,r}(pt) = 1 + pt + \frac{(pt)^2}{2!} + \frac{(pt)^3}{3!} + \cdots + + \frac{(pt)^{r-1}}{(r-1)!}$$

y la función logaritmo truncada $\log_{p,r} : U_{p,1} \to p\mathbb{Z}/p^r\mathbb{Z}$ definida por

$$\ln_{p,r}(1 + ps) = ps - \frac{(ps)^2}{2} + \frac{(ps)^3}{3} + \cdots + (-1)^r \frac{(ps)^{r-1}}{r-1}.$$

Nótese que estas funciones están bien definidas dado que los denominadores involucrados son unidades en el anillo $\mathbb{Z}/p^r\mathbb{Z}$. Debemos probar que estas funciones son inversas. Para ello consideramos el anillo $\mathbb{Q}[[x]]$ de series de potencias con coeficientes racionales y su cociente $A = \mathbb{Q}[[x]]/(x^r)$. Es fácil ver que la series de potencia usuales $f(x) = e^x - 1$ y $g(x) = \ln(1 + x)$ pueden evaluarse sin problemas en los elementos nilpotentes de A y son inversas allí.

Si se definen las funciones truncadas

$$f_p(x) = x + \frac{x^2}{2} + \ldots + \frac{x^{r-1}}{(r-1)!} \quad \text{y} \quad g_p(x) = x - \frac{x^2}{2} + \ldots + (-1)^r \frac{x^{r-1}}{(r-1)!},$$

es fácil ver que $f(u) = f_r(u)$ y $g(u) = g_r(u)$ para todo elemento nilpotente de A. En particular, estas funciones siguen siendo inversas allí. Por la misma razón se tienen las identidades $g_r(u) + g_r(v) = g_r\Big((1+u)(1+v) - 1\Big)$ y $\Big(1 + f_r(u)\Big)\Big(1 + f_r(v)\Big) = 1 + f_r(u+v)$. Dado que los denominadores de f_r y g_r no contienen potencias de p, estas funciones se pueden restringir sin problemas al subanillo $B = \mathbb{Z}_{(p)}[[x]]/(x^r)$ de series de potencias cuyos coeficientes están en el anillo local racional. Por otro lado, para todo elemento nilpotente $u \in \mathbb{Z}/p^r\mathbb{Z}$ existe una función evaluación $\phi_u : \mathbb{Z}_{(p)}[[x]] \to \mathbb{Z}/p^r\mathbb{Z}$ que se anula en x^r. Concluímos que dicha evaluación puede considerarse como una función de B a $\mathbb{Z}/p^r\mathbb{Z}$. Se conluye que f_p y g_p son inversas en el conjunto de elementos nilpotentes de $\mathbb{Z}/p^r\mathbb{Z}$. Esto es equivalente a la afirmación de que $\exp_{p,r}$ y $\ln_{p,r}$ son inversas. Además se tienen, en B, las identidades

$$g_r(tx) + g_r(sx) = g_r\Big((1+tx)(1+sx) - 1\Big) \qquad \text{y}$$

$$\Big(1 + f_r(tx)\Big)\Big(1 + f_r(sx)\Big) = 1 + f_r(tx + sx),$$

para todo par de enteros s y t. De aquí se concluye que $\exp_{p,r}$ y $\ln_{p,r}$ son homomorfismos de grupos. □

Puede probarse que, si $p \neq 2$, las funciones $f(px)$ y $g(px)$ tienen coeficientes en $\mathbb{Z}_{(p)}$, por lo que truncarlas no es necesario. Esto dá un isomorfismo entre los subgrupos mencionados que es independiente de la condición en r. Veremos más adelante como definir exponenciales y logaritmos en un contexto más general, por lo que esta generalización no es necesaria.

2.5 Derivadas formales

Sea C un anillo conmutativo. y sea $f(x) \in C[x]$ un polinomio con coeficientes en C. Entonces, $f(x+y)$ es un elemento del anillo de polinomios en 2 variables $C[x, y]$. En cosecuencia, podemos escribir

$$f(x+y) = f_0(x) + f_1(x)y + f_2(x)y^2 + f_3(x)y^3 + \ldots.$$

Evaluando en $y = 0$, se tiene $f_0(x) = f(x)$. Definimos la derivada formal mediante $\frac{d}{dx}\Big(f(x)\Big) = f'(x) = f_1(x)$. En otras palabras, $f'(x)$ es el único polinomio en x que satisface la congruencia siguiente:

$$f(x+y) \equiv f(x) + yf'(x) \pmod{y^2}.$$

A esta expresión la llamaremos la expansión de Taylor a primer orden de f.

Ejemplo 2.23. Si $f(x) = x^n$, el teorema del binomio nos dá $(x+y)^n \equiv x^n + nx^{n-1}y \pmod{y^2}$. Se concluye que $f'(x) = nx^{n-1}$.

Con esta definición, no es dificil comprobar las propiedades

$$\frac{d}{dx}[f(x)+g(x)] = f'(x)+g'(x), \qquad \frac{d}{dx}[f(x)g(x)] = f'(x)g(x)+f(x)g'(x).$$

Por ejemplo, probaremos la última:

$$\begin{aligned} f(x+y)g(x+y) &\equiv \Big(f(x)+yf'(x)\Big)\Big(g(x)+yg'(x)\Big) \\ &\equiv f(x)g(x) + \Big(f'(x)g(x)+f(x)g'(x)\Big)y \pmod{y^2}. \end{aligned}$$

Utilizando las propiedades anteriores, se tienen que un polinomio de la forma $f(x) = \sum_{i=0}^{n} a_i x^i$ tiene derivada dada por la fórmula usual $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$. Utilizando el hecho de que los polinomios pueden evaluarse en elementos de C, o, más generalmente, en elementos de cualquier anillo que contiene a C, obtenemos el siguiente resultado:

Proposición 2.24 (Expansión de Taylor a primer orden)**.** *Sea B un anillo conmutativo que contiene a un anillo dado C, y sea $f(x) \in C[[x]]$ un polinomio. Sean $u, \epsilon \in B$ elementos arbitrarios. Entonces se tiene la congruencia siguiente:*

$$f(u+\epsilon) \equiv f(u) + f'(u)\epsilon \pmod{\epsilon^2}. \quad \square$$

Este resultado nos permite demostrar fácilmente la regla de la cadena.

Proposición 2.25 (Regla de la cadena)**.** *Si $f(x), w(x) \in C[x]$, entonces se tiene la identidad $\frac{d}{dx}\Big(f(w(x)\Big) = f'\Big(w(x)\Big)w'(x)$.*

Demostración. Sea $h = h(x,y) = w(x+y) - w(x)$, de modo que $w(x+y) = w(x) + h$. Observese que y divide a h. De la congruencia $w(x+y) \equiv w(x) + yw'(x) \pmod{y^2}$ se deduce que $h \equiv w'(x)y \pmod{y^2}$. El resultado sigue anora del siguiente cálculo:

$$\begin{aligned} f\Big(w(x+y)\Big) &= f\Big(w(x)+h\Big) \\ &\equiv f\Big(w(x)\Big) + hf'\Big(w(x)\Big) \pmod{h^2} \\ &\equiv f\Big(w(x)\Big) + \Big(w'(x)y\Big)f'\Big(w(x)\Big) \pmod{y^2}. \quad \square \end{aligned}$$

Ejemplo 2.26. Mostraremos ahora como la expansión de Taylor puede utilizarse para resolver ecuaciones de congruencias. Tomemos por ejemplo la ecuación $x^2 \equiv 14 \pmod{13^2}$. Claramente la ecuación $x^2 \equiv 14 \pmod{13}$ tiene las soluciones 1 y -1, luego basta buscar soluciones del tipo $1+13t$ o $-1+13t$. Ahora bien, si $f(x) = x^2$, se tiene $f(1+13t) \equiv f(1) + 13tf'(1) \pmod{13^2}$, de donde necesitamos encontrar t tal que $14 \equiv f(1) + 13tf'(1) \equiv 1 + 13t \times 2 \pmod{13^2}$. Juntando las constantes y dividiendo por 13 se obtiene $1 \equiv 2t \pmod{13}$, luego $t \equiv 7 \pmod{13}$ o $x \equiv 1 + 7 \times 13 \equiv 92 \pmod{13^2}$. Del mismo modo se obtiene la solución $x \equiv -1 + 6 \times 13 \equiv 77 \pmod{13^2}$.

Una vez que se ha definido la derivada, podemos definir las derivadas sucesivas por inducción mediante $f^{(n+1)}(x) = \frac{d}{dx} f^{(n)}(x)$. Nótese que, en la relación

$$f(x+y) = f(x) + f'(x)y + f_2(x)y^2 + f_3(x)y^3 + \ldots$$

podemos considerar ambos lados como polinomios en y con coeficientes en el anillo conmutativo $C[x]$, de modo que al derivar ambos lados se tiene

$$f'(x+y) = f'(x) + 2f_2(x)y + 3f_3(x)y^2 + \ldots,$$

y al evaluar en $y = 0$ se tiene $2f_2(x) = f''(x)$. Iterando este procedimiento se obtiene la relación $n!f_n(x) = f^{(n)}(x)$. No es posible despejar $f_n(x)$ de esta relación a no ser que $n!$ sea invertible en el anillo C. Por ejemplo, si $C = \mathbb{Z}/m\mathbb{Z}$, entonces $n!$ es invertible si y sólo si m no es divisible por ningún primo entre 1 y n.

2.6 El Lema de Hensel

El siguiente resultado nos permite encontrar raices de polinomios módulo p^n para cualquier n dada una raiz módulo p. La única condición necesaria para

esto es que la raiz no sea un punto crítico módulo p, es decir que su derivada no se anule:

Proposición 2.27 (Lema de Hensel)**.** *Sea $f(x) \in D[x]$, sea p un primo de D, y sea a un elemento de D que satisface las condiciones siguientes:*

1. $f(a) \equiv 0 \pmod{p}$,
2. $f'(a) \not\equiv 0 \pmod{p}$.

Entonces existe una solución b_n de la ecuación $f(a) \equiv 0 \pmod{p^n}$, que satisface $b_n \equiv a \pmod{p}$, para todo entero n. Además, para cada valor de n, la solución b_n es única módulo n.

Demostración. La condición $f'(a) \not\equiv 0 \pmod{p}$ implica que $f'(a)$ tiene un inverso módulo p. Sea k este inverso. Definimos la sucesión $\{b_n\}_n$ recursivamente,mediante las relaciones siguientes:

1. $b_1 = a$.
2. $b_{n+1} = b_n - kf(b_n)$.

En particular se tienen estas propiedades:

1. $(b_n - b_{n+1}) = kf(b_n)$.
2. $f(b_{n+1}) \equiv f(b_n) - kf(b_n)f'(b_n) \left(\mod \left(kf(b_n)\right)^2\right)$.

Para demostrar la segunda afirmación, aplicamos la fórmula de Taylor a primer orden. Supongamos ahora, como hipótesis de inducción, que $f(b_n) \equiv 0 \pmod{p^n}$ y que $b_n \equiv a \pmod{p}$. Como en particular se tiene $f(b_n) \equiv 0 \pmod{p}$, la propiedad (1) arriba implica que $b_{n+1} \equiv a \pmod{p}$. Por otro lado, dado lo ya probado, la propiedad (2) nos dá

$$f(b_{n+1}) \equiv f(b_n) - kf(b_n)f'(b_n) \equiv f(b_n)\Big(1 - kf'(b_n)\Big) \pmod{p^{2n}}.$$

Aplicando nuevamente la propiedad $b_n \equiv a \pmod{p}$, se obtiene la congruencia $1 - kf'(b_n) \equiv 0 \pmod{p^{n+1}}$, de donde se sigue lo pedido. La unicidad de sigue de que en cada paso, la ecuación

$$f(b_n + tp^n) \equiv 0 \pmod{p^{n+1}}$$

nos dá $tp^n = kf(b_n)$ como única solución por los cálculos precedentes. □

Una consecuencia directa de lo anterior es el siguiente resultado:

Proposición 2.28. *Si b es invertible en $\mathbb{Z}/p\mathbb{Z}$, entonces b es invertible en $\mathbb{Z}/p^n\mathbb{Z}$ para todo entero n.*

Demostración. Basta aplicar el resultado anterior a la ecuación $f(x) = ax - 1 \equiv 0 \pmod{p^n}$.

Ejemplo 2.29. Si el primo p no es 2, entonces un elemento $b \in \mathbb{Z}/n\mathbb{Z}$ es un cuadrado si y sólo si es un cuadrado en $\mathbb{Z}/p\mathbb{Z}$. Basta aplicar el Lema de Hensel a la ecuación $f(x) = x^2 - b \equiv 0 \pmod{p^n}$.

Ejemplo 2.30. La ecuación $x^5+3x^2+x = 0$ tiene precisamente una solución de la forma $1 + 5t$ y una de la forma $5k$ en el anillo $\mathbb{Z}/5^n\mathbb{Z}$, para cada entero $n \geq 1$. En este caso, la derivada es congruente, módulo 5, a $x+1$, por lo que no se anula ni en 0 ni en 1.

Ejemplo 2.31. La ecuación $x^5+x^2+3x = 0$ tiene precisamente una solución de la forma $5k$ en el anillo $\mathbb{Z}/5^n\mathbb{Z}$, para cada entero $n \geq 1$. Sin embargo, el lema de Hensel no se pronuncia sobre las soluciones de la forma $1 + 5t$, ya que la derivada se anula, módulo 5, en 1.

2.7 El grupo de unidades módulo n.

En esta sección estudiaremos el grupo de unidades $(\mathbb{Z}/n\mathbb{Z})^*$ del anillo de enteros módulo n. Este es un grupo abeliano finito, por lo que los teoremas de estructura para tales grupos (véase los apuntes de grupos y anillos) nos permiten escribirlo como producto cartesiano de grupos cíclicos. Sin embargo, podemos ser significativamente más explícitos aplicando los resultados vistos en este capítulo. De hecho, si $n = p_1^{r_1} \cdots p_k^{r_k}$, el Teorema Chino de los restos nos permite obtener la descomposición siguiente:

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^* \cong \prod_{i=1}^{k} \left(\mathbb{Z}/p_i^{r_i}\mathbb{Z}\right)^*.$$

Bastará, por lo tanto, calcular la estructura del anillo $\left(\mathbb{Z}/p_i^{r_i}\mathbb{Z}\right)^*$. Para ello, comenzaremos con el caso $n = 1$. Recordemos que el anillo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ es un cuerpo.

La función ϕ de Euler se define como $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$. El teorema chino de los restos implica que $\phi(nm) = \phi(n)\phi(m)$ si n y m son relativamente primos. El número de elementos de un orden dado en un grupo cíclico puede calcularse fácilmente en términos de ϕ. De hecho, tenemos el siguiente resultado:

Lema 2.32. *Si m divide a n, existen $\phi(m)$ elementos de orden m en el grupo cíclico $C_n = \mathbb{Z}/n\mathbb{Z}$.*

Demostración El orden $\mathrm{ord}(a)$ del elemento $a + n\mathbb{Z}$ divide a m si y sólo si $ma + n\mathbb{Z} = 0 + n\mathbb{Z}$. Es decir, $\mathrm{ord}(a)|m$ si y sólo si ma es divisible por n, o, equivalentemente, a es divisible por $m' = n/m$. En particular, $\mathrm{ord}(a) = m$ si y sólo si a es divisible por m' y no por ningún divisor de n mayor a m'. En otras palabras $(a) + (n) = (m')$. Esto es equivalente a decir que $(a/m') + (n/m') = (1)$, por lo que hay $\phi(n/m') = \phi(m)$ elecciones posibles para tal elemento a/m' módulo m, lo que nos dá $\phi(m)$ elecciones posibles para a módulo $mm' = n$. □

El siguiente corolario es inmediato, ya que todo elemento en C_n tiene un orden que divide a n:

Corolario 2.32.1. $\sum_{d|n} \phi(d) = n$.

Lema 2.33. *Si G es un grupo abeliano finito, donde hay a lo más n soluciones de la ecuación $g^n = e$ para cada n entonces G es un grupo cíclico.*

Demostración Sea $N = |G|$. Basta ver que existe un elemento de orden N. Supongamos que G tiene $\psi(n)$ elementos de orden n para cada n. Entonces $\sum_{d|N} \psi(d) = N$. Si $\psi(N) = 0$, existe algún n con $\psi(n) > \phi(n)$. Tomemos un divisor n de N minimal tal que $\psi(n) > \phi(n)$. En particular, G tiene elementos de orden n. Un elemento $g \in G$ de orden n genera un subgrupo isomorfo a $\mathbb{Z}/n\mathbb{Z}$, y por lo tanto $\psi(d) \geq \phi(d)$ para todo divisor d de n. Se concluye que el número de elementos cuyo orden divide a n es $\sum_{d|n} \psi(d) > \sum_{d|n} \phi(d) = n$. Como los elementos cuyo orden divide a n son las soluciones de $g^n = e$, la afirmación precedente contradice la hipótesis. □

Proposición 2.34. *Si K es un cuerpo arbitrario, y si Γ es un subgrupo finito de K^*, entonces Γ es cíclico.*

Demostración La hipótesis del resultado precedente es inmediata, ya que un polinomio de grado n no puede tener mas de n raices. En particular, se concluye que $x^n - 1$ no puede tener más de n raices para ningún n. □

Corolario 2.34.1. *El grupo de unidades de* $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ *es cíclico.* □

Un generador del grupo $\mathbb{F}_p^*$ recibe el nombre de raiz primitiva módulo p. Aplicando ahora los resultados de la sección precedente se obtiene el siguiente resultado:

Corolario 2.34.2. *El grupo* $\mathbb{Z}/p^n\mathbb{Z}$ *contiene un elemento de orden* $p-1$ *para cada entero positivo* n*.*

Demostración basta aplicar el Lema de Hensel al polinomio $f(x) = x^{p-1} - 1$, cuya derivada $f'(x) = (p-1)x^{p-2}$ es no nula para todo $x \in \mathbb{F}_p^*$. □

Lema 2.35. *Sea* k *un entero positivo. Si* p *es un primo y se cumple al menos una de las condiciones siguientes:*

1. p *es impar,*
2. $k > 1$*.*

entonces, para cada entero t *relativamente primo con* p*, se tiene* $(1+tp^k)^p = 1 + sp^{k+1}$*, para algún entero* s *relativamente primo con* p*.*

Demostración Por el teorema del binomio, se tiene lo siguiente:

$$(1 + tp^k)^p = 1 + tp^{k+1} + \binom{p}{2} t^2 p^{2k} + \cdots$$

Basta ver que todos los términos a partir del tercero son divisibles por una potencia de p mayor a $k+1$, y por lo tanto puede factorizarse como sigue:

$$(1 + tp^k)^p = 1 + p^{k+1}\left[t + p\left[\binom{p}{2} t^2 p^{k-2} + \binom{p}{3} t^3 p^{2k-2} + \cdots\right]\right].$$

Para probar la afirmación consideramos dos casos:

1. Si p es impar, entonces $\binom{p}{2}$ es divisible por p por lo que $\binom{p}{2} t^2 p^{k-2}$ es entero. Los terminos subsecuentes no representan un problema, puesto que el exponente de p es claramente no-negativo.

2. Si $k \geq 2$, ningún exponente de p en la expresión anterior puede ser negativo.

□

Corolario 2.35.1. *Si p es un primo impar, entonces $\left(\mathbb{Z}/p_i^r\mathbb{Z}\right)^*$ tiene un elemento de orden p^{r-1} para cada entero positivo r.*

Demostración Basta probar por inducción que $(1+tp^{r-k})$ tiene orden p^k, de modo que $1+p$ tiene orden p^{r-1}. Es claro que $1+tp^{r-1}$ tiene orden p, pues no es congruente a 1, pero sí lo es $(1+tp^{r-1})^p \equiv 1+tp^r \pmod{p^r}$. Si asumimos que $1+tp^{r-j}$ tiene orden p^j, para todo t relativamente primo con p, entonces el lema precedente muestra que $(1+tp^{r-j-1})^p$ tiene orden p^j. Si el orden de $1+tp^{r-j-1}$ es $p^u n_0$, entonces $u \geq j > 0$, por lo que el orden de $(1+tp^{r-j-1})^p$ es $p^{u-1}n_0$, por lo que $u = j+1$ y $n_0 = 1$. El resultado sigue. □

Corolario 2.35.2. *Si p es un primo impar, entonces $\left(\mathbb{Z}/p^r\mathbb{Z}\right)^*$ es cíclico de orden $\phi(p^n) = p^{r-1}(p-1)$.*

Demostración Como tiene un elemento de orden $p-1$ y un elemento de orden p^{r-1} el resultado sigue del isomorfismo $C_{p^{r-1}} \times C_{p-1} \cong C_{p^{r-1}(p-1)}$ (ver apuntes de grupos y anillos). □

Proposición 2.36. *para todo entero $r \geq 2$, el grupo $\left(\mathbb{Z}/2^r\mathbb{Z}\right)^*$ es el producto de dos grupos cíclicos de orden 2 y 2^{r-2} respectivamente. Además, el primer grupo está generado por -1 y el segundo grupo está generado por 5.*

Demostración Se sigue del Lema 2.35, por el mismo argumento de antes, que $5^{2^{r-k}} = (1+4)^{2^{r-k}}$ tiene orden 2^k si $r-k \geq 2$, así que, en particular, 5 tienen orden 2^{r-2}. Además $5 \equiv 1 \pmod 4$, por lo que lo mismo ocurre con cualquier potencia. En particular, -1 no es una potencia de 5 en $\left(\mathbb{Z}/2^r\mathbb{Z}\right)^*$. Se sigue que 5 y -1 generan un grupo isomorfo a $C_{2^{r-2}} \times C_2$. Basta ahora observar que este último grupo tiene orden $2^{r-1} = \phi(2^r)$. □

2.8 Ejercicios

1. Una ranita se ubica en una ruleta con n casillas, como la que se ilustra en la figura 2.1. Esta sólo es capaz de dar saltos en el sentido de las agujas del reloj, saltando k casillas por vez. Para que valores de n y k puede la rana recorrer cada casilla de la ruleta?

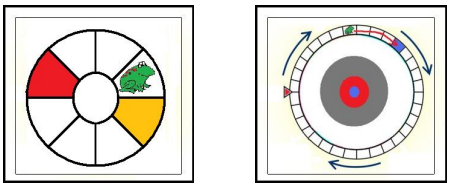

Figure 2.1: Una ranita en una ruleta.

2. Demuestre el teorema de Wilson: *Para todo primo p se tiene* $(p-1)! \equiv -1 \pmod{p}$.

3. Encuentre el inverso de 183 módulo 257.

4. Encuentre el inverso de 257 módulo 1024. Utilice el resultado para encontrar el inverso de 1024 módulo 257.

5. Utilice la serie de taylor de $(1+x)^{1/2}$ para encontrar una raiz cuadrada de 23 módulo 121 y una raiz cuadrada de 7 módulo 243.

6. Resolver el sistema
$$\begin{aligned} x &\equiv 3 \text{ (módulo 11)}, \\ x &\equiv 2 \text{ (módulo 17)}, \\ x &\equiv 5 \text{ (módulo 23)}. \end{aligned}$$

7. Resolver el sistema
$$\begin{aligned} 2x + 4 &\equiv 0 \text{ (módulo 11)}, \\ 3x + 5 &\equiv 0 \text{ (módulo 17)}, \\ 6x + 11 &\equiv 0 \text{ (módulo 23)}. \end{aligned}$$

8. Resolver el sistema
$$\begin{array}{ll} x \equiv 3 & (\text{mod } 7), \\ 3x \equiv -5 & (\text{mod } 11), \\ x^2 \equiv 1 & (\text{mod } 23). \end{array}$$

9. Resolver el sistema
$$\begin{aligned} x^2 + x &\equiv 0 \text{ (módulo 11)}, \\ x^2 + 2x + 1 &\equiv 0 \text{ (módulo 17)}, \\ x^2 - 1 &\equiv 0 \text{ (módulo 23)}. \end{aligned}$$

10. Resolver la ecuación $x^2 - x \equiv 0$ (módulo $11 \cdot 17 \cdot 23$).

11. Resolver la ecuación $x^2 + x + 1 \equiv 0$ (módulo $11 \cdot 17 \cdot 23$).

12. Resolver la ecuación $x^2 + x + 1 \equiv 0$ (módulo $7 \cdot 19 \cdot 39$).

13. Resolver la ecuación $x^2 + x + 1 \equiv 0$ (módulo $7^2 \cdot 19$).

14. Encontrar una unidad primitiva módulo 7, 19, y 83.

15. Si a es una raiz primitiva módulo 257, encuentre todos los posibles valores de a^{16} módulo 257.

16. Sea $f(x) \in \mathbb{Z}[x]$ un polinomio tal que para cada primo p existe algún entero n tal que $f(n) \not\equiv 0$ (módulo p). Probar que existen infinitos primos p para los cuales la ecuación $f(x) \equiv 0$ (módulo p) tiene al menos una raiz.

17. Probar que p divide a $a^p - a$ para todo entero a.

18. Probar que un polinomio f con coeficientes enteros satisface $f(x) = g(x)^p + ph(x)$, donde g y h son polinomios con coeficientes enteros, si y sólo si $f'(x) = ps(x)$, donde s es un polinomio con coeficientes enteros.

19. Sean a, b, c, d números enteros. Probar que existen enteros x, y, z, w tales que
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$
con $r, u \equiv 1 \pmod{n}$ y $s, t \equiv 0 \pmod{n}$, si y sólo si $ad - bc$ es relativamente primo con n.

Chapter 3

Residuos cuadráticos y reciprocidad

En este capítulo estudiaremos la posibilidad de resolver ecuaciones cuadráticas módulo n, es decir ecuaciones del tipo

$$ax^2 + bx + c \equiv 0 \pmod{n}.$$

Por el Teorema Chino de los restos, es suficiente con resolver esta ecuación módulo p^n donde p es un primo. Para ilustrar este procedimiento consideremos el siguiente ejemplo:

Ejemplo 3.1. Se quieren encontrar las soluciones de la ecuación cuadrática

$$x^2 + x + 1 \equiv 0 \pmod{273}.$$

Puesto que $273 = 3 \times 7 \times 13$, es suficiente resolver la ecuación módulo cada uno de los 3 primos. Módulo 3 las solución es $x \equiv 1$. Módulo 7 las soluciones son 2 y 4. Módulo 13 las soluciones son 3 y 9. Esto significa que la solución de la ecuación original se obtiene resolviendo cada uno de los sistemas siguientes:

1. $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{7}$, $x \equiv 3 \pmod{13}$.
2. $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{7}$, $x \equiv 9 \pmod{13}$.
3. $x \equiv 1 \pmod{3}$, $x \equiv 4 \pmod{7}$, $x \equiv 3 \pmod{13}$.
4. $x \equiv 1 \pmod{3}$, $x \equiv 4 \pmod{7}$, $x \equiv 9 \pmod{13}$.

Las soluciones de estos sistemas son, respectivamente, $x \equiv 16, 22, 172, 254$, como se obtiene del Teorema Chino de los restos. Estas son, por lo tanto, la soluciones de la ecuación pedida.

Ejemplo 3.2. Se quieren encontrar las soluciones de la ecuación cuadrática

$$x^2 + x + 1 \equiv 0 \pmod{165}.$$

Puesto que $273 = 3 \times 5 \times 11$, es suficiente resolver la ecuación módulo cada uno de los 3 primos. Módulo 5 las solución no tiene soluciones, por lo que tampoco las tiene la ecuación original.

El Lemma de Hensel, demostrado en el capítulo anterior, permite encontrar soluciones módulo p^r, con tal de que se las conozca módulo p, a condición de que la derivada no se anule módulo p. Probaremos a contiinuación una versión más fuerte que permite encontrar soluciones módulo p^r para todo r con tal de que se las conozca módulo p^{r_0} para un elemento preciso $r_0 = a$ condición de que la derivada no se anule "demasiado":

Proposición 3.3 (Lema de Hensel, segunda versión)**.** *Sea $f(x) \in D[x]$, y sea p un primo de D, a un elemento de D, y t un entero pisitivo, que satisfacen las condiciones siguientes:*

1. $f(a) \equiv 0 \pmod{p^{2t}}$,
2. $f'(a) \not\equiv 0 \pmod{p^t}$

Entonces existe, para todo entero n, una solución b_n de la ecuación $f(a) \equiv 0 \pmod{p^n}$, que satisface $b_n \equiv a \pmod{p}$.

Demostración. La condición $f'(a) \not\equiv 0 \pmod{p^t}$ implica que $f'(a) = p^s u$ con $s < t$ y u invertible módulo p. Sea k el inverso de u. Por otro lado, $f(a) = lp^{2t}$. Sea $\epsilon = -lkp^{2t-s}$. Observemos que

$$f(a + \epsilon) \equiv f(a) + \epsilon f'(a) \equiv 0 \pmod{\epsilon^2},$$

y como $s < t$ se tiene $p^{t+1} | \epsilon$ y por lo tanto $p^{2t+2} | \epsilon^2$. De aquí se siguen las siguientes conclusiones:

- $f(a + \epsilon) \equiv 0 \pmod{p^{2t+2}}$ y
- $f'(a + \epsilon) \equiv f'(a) + \epsilon f''(a) \equiv f'(a) \pmod{p^t}$.

Ahora el resultado se concluye por una inducción, muy similar a la utilizada para demostrar la primera versión. Los detalles se dejar al lector. □

Ejemplo 3.4. Sea a un entero impar. La ecuación $x^2 - a = 0$ tiene una solución módulo 2^r para todo r, con tal de que tenga una solución módulo $16 = 2^4$, ya que $2c \not\equiv 0 \pmod 4$ para todo entero impar c. De hecho una busqueda exhaustiva prueba que los cuadrados impares son 1 y 9, por lo que basta verificar si un entero impar es congruente a 1 módulo 8 para que $x^2 - a = 0$ tenga una solución módulo 2^r para todo r.

Tomemos ahora la ecuación cuadrática general, y veamos que se necesita exactamente para resolverla. Partimos de la ecuación

$$ax^2 + bx + c \equiv 0 \pmod{p^t}.$$

El caso más sencillo se obtiene cuando p no divide a a y $p \neq 2$. En este caso las raices son de la forma

$$x = \frac{-b + \delta}{2a}$$

donde δ satisface $\delta^2 = b^2 - 4ac$. Nótese que el denominador de la fracción debe entenderse en términos de inversos módulo n, como se discutió en el capítulo precedente. Se obtiene de cualquiera de las dos versiones del Lema de Hensel que $b^2 - 4ac$, si es invertible, es un cuadrado módulo p^r si y sólo si es un cuadrado módulo p. Si $b^2 - 4ac \equiv 0 \pmod{p^r}$, las raices son de la forma $p^s u$ con $2s \geq r$. Si p divide a $b^2 - 4ac$, pero p^r no lo hace, la situación es algo más compleja. Podemos escribir $b^2 - 4ac = p^r n_0$, y comparar esto con la ecuación $(p^s m)^2 = p^{2s} m^2$. Concluimos que $b^2 - 4ac$ es un cuadrado precisamente cuando r es par y n_0 es un cuadrado módulo p.

Cuando p divide a a, digamos $a = pa_0$, la ecuación puede re-escribirse como $pa_0x^2 + bx + c \equiv 0 \pmod{p^t}$. Multiplicando por p se tiene la ecuación equivalente $a_0(px)^2 + b(px) + pc \equiv 0 \pmod{p^{t+1}}$. Por lo tanto la ecuación original tendrá soluciones si y sólo si $a_0y^2 + by + pc \equiv 0 \pmod{p^{t+1}}$ tiene soluciones divisibles por p. Este procedimiento puede repetirse las veces que sea necesario, hasta reducirnos a los casos ya analizados.

El caso mas difícil aparece cuando $p = 2$. En este caso, es todavía cierto que $2ax = \delta - b$ donde $\delta^2 = b^2 - 4ac$. Aún en este caso puede procederse como en el caso anterior, encontrando primero los posibles valores de δ y comprobando a posteriori si los valores obtenidos de $\delta - b$ son divisibles por $2a$. El análisis de si un elemento es o no un cuadrado debe realizarse por

separado en los casos 2, 4 y 8. Esto trae algunas dificultades adicionales cuando $b^2 - 4ac$ es par. Por ejemplo, $4n^0$, con n_0 impar, es un cuadrado módulo 32 si y sólo si $n_0 \equiv 1$ módulo 8, pero la misma ecuación módulo 16 sólo requiere el estudio de n_0 módulo 4. Estos detalles suelen ser sencillos y la formulación precisa de todos los casos posibles se le deja al lector interesado.

Nótese que lo anterior nos permite resolver una ecuación cuadrática en todos los casos siempre y cuando seamos capaces de encontrar las raices de cualquier número módulo p. Esto no necesariamente es sencillo para p grande. Pero al menos existe un procedimiento sencillo para determinar si una ecuación de la forma $x^2 \equiv a$ tiene o no soluciones módulo p. Esto es lo que nos dá la ley de reciprocidad cuadrática, la que estudiaremos en la sección siguiente.

3.1 La ley de reciprocidad cuadrática

Sea p un número primo impar y sea a un número entero relativamente primo a p. El símbolo de Legendre $\left(\frac{a}{p}\right)$ es por definición el entero

$$\left(\frac{a}{p}\right) = \left\{ \begin{array}{cc} 1 & \text{si } \ a \text{ es un cuadrado módulo } p \\ -1 & \text{si } \ a \text{ no es un cuadrado módulo } p \end{array} \right\}.$$

Nótese que determinar si a es o no un cuadrado módulo p es equivalente a calcular el símbolo de Legendre correspondiente. Como $(\mathbb{Z}/p\mathbb{Z})^*$ es un grupo cíclico de orden $p-1$ generado por un elemento primitivo η, obtenemos que $\left(\frac{a}{p}\right) = 1$ si y sólo si $a = \eta^r$ es una potencia par de η, o equivalentemente, si $a^{\frac{p-1}{2}} \equiv \eta^{\frac{r(p-1)}{2}} \equiv 1 \pmod{p}$. Se concluye que

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Una consecuencia inmediata de esta última relación es la identidad multipicativa $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$. Nótese que, si $p > 2$, los enteros 1 y -1 no son congruentes módulo p. De otro modo la conclusión no seguiría. También es inmediata la relación siguiente:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

El cálculo de $\left(\frac{2}{p}\right)$ es algo más complejo. La demostración dada aquí requiere calcular congruencias módulo p en el anillo de enteros de Gauss

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}.$$

Las propiedades de este anillo, y otros similares, se estudiarán con más detalle en capítulos subsecuentes. Por el momento, nos basta la definición de arriba. El lector podrá comprobar sin problemas que este conjunto es realmente un anillo.La identidad $p(a + bi) = pa + (pb)i$ nos dice que las congruencias módulo p pueden estudiarse coordenada a coordenada. En particular, como $2 = (-i)(1 + i)^2$, podemos re-escribir

$$2^{\frac{p-1}{2}}(1 + i) = (1 + i)^p(-i)^{\frac{p-1}{2}} \equiv (1 + i^p)(-i)^{\frac{p-1}{2}} \pmod{p},$$

donde la congruencia $(1 + i)^p \cong 1 + i^p$ se justifica porque p divide a cada coeficiente de la expansión binomial. Como p es impar, i^p es siempre un imaginario puro, pero tanto i^p como $(-i)^{\frac{p-1}{2}}$ dependen de la clase de congruencia de p módulo 8. Tomando la parte real a ambos lados de la ecuación

$$2^{\frac{p-1}{2}}(1 + i) \equiv (1 + i^p)(-i)^{\frac{p-1}{2}} \pmod{p},$$

en cada uno de los cuatro casos, se obtienen los resultados siguientes:

- Si $p \equiv 1 \pmod 8$, se tiene $2^{\frac{p-1}{2}} \equiv Re[(1 + i)(1)] \pmod p$, por lo que se concluye que $\left(\frac{2}{p}\right) = 1$.
- Si $p \equiv 5 \pmod 8$, se tiene $2^{\frac{p-1}{2}} \equiv Re[(1 + i)(-1)] \pmod p$, por lo que se concluye que $\left(\frac{2}{p}\right) = -1$.
- Si $p \equiv 3 \pmod 8$, se tiene $2^{\frac{p-1}{2}} \equiv Re[(1 - i)(-i)] \pmod p$, por lo que se concluye que $\left(\frac{2}{p}\right) = -1$.
- Si $p \equiv 7 \pmod 8$, se tiene $2^{\frac{p-1}{2}} \equiv Re[(1 - i)(i)] \pmod p$, por lo que se concluye que $\left(\frac{2}{p}\right) = 1$.

En cada caso podemos escribir $p = 2t + 1$, de modo que un cálculo simple nos muestra que $\frac{p^2-1}{8} = \frac{1}{2} \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} = \frac{t(t+1)}{2}$. Este último número es par

precisamente cuando t es congruente a 3 o 0 módulo 4, es decir cuando p es congruente a 7 o 1 módulo 8. De aquí se deduce la fórmula siguiente:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

El cálculo de los Símbolos de Legendre puede terminarse, en todos los casos, si podemos calcular $\left(\frac{q}{p}\right)$ para cualquier primo impar q. Una herramienta que nos permite hacer esto es la ley de reciprocidad cuadrática:

Proposición 3.5 (Ley de Reciprocidad Quadrática)**.** *Si p y q son enteros primos positivos impares, entonces*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Demostración. La siguiente demostración se debe a Sey Y. Kim. Para cada conjunto finito de enteros T, escribimos $A_T = \prod_{n\in T} n$. Consideremos los tres conjuntos siguientes:

$$\Phi = \left\{ a \middle| 1 \leq a \leq \frac{pq-1}{2},\ (a, pq) = 1 \right\},$$

$$\Psi = \left\{ a \middle| 1 \leq a \leq \frac{pq-1}{2},\ (a, p) = 1 \right\},$$

$$X = \left\{ qt \middle| 1 \leq t \leq \frac{p-1}{2} \right\}.$$

Claramente $\Psi = \Phi \cup X$, y la unión es disjunta, de donde $A_\Psi = A_\Phi A_X$. Nótese que hemos usado la identidad $\frac{pq-1}{2} = p\frac{q-1}{2} + \frac{p-1}{2} = q\frac{p-1}{2} + \frac{q-1}{2}$, que es también importante en lo que sigue.

Para cada entero t definimos dos conjuntos adicionales:

$$\Psi_t = \left\{ n + pt \middle| 1 \leq n \leq p-1 \right\}, \qquad \Psi'_t = \left\{ n + pt \middle| 1 \leq n \leq \frac{p-1}{2} \right\},$$

de modo que, podemos escribir $\Psi = \Psi'_{(q-1)/2} \cup \bigcup_{t=0}^{(q-2)/2} \Psi_t$, y esta unión es disjunta. Concluimos que $A_\Psi = A_{\Psi_0} \cdots A_{\Psi_{(q-2)/2}} A_{\Psi'_{(q-1)/2}}$. Por otro lado, por el teorema de Wilson (Ejercicio 2 del capítulo precedente), se obtiene la

identidad $A_{\Psi_t} \equiv -1 \pmod{p}$ para cada entero t. Concluimos la identidad siguiente:

$$A_\Psi \equiv (-1)^{(q-1)/2} \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Analogamente se obtiene la identidad

$$A_X = q^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{q}{p}\right) \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Combinando estas dos relaciones con $A_\Psi = A_\Phi A_X$, y luego aplicando la simetría en p y q, obtenemos las siguientes relaciones:

$$A_\Phi \equiv (-1)^{(q-1)/2} \left(\frac{q}{p}\right) \pmod{p} \quad \text{y} \quad A_\Phi \equiv (-1)^{(p-1)/2} \left(\frac{q}{p}\right) \pmod{q}.$$

Si $A_\Phi \equiv 1 \pmod{p}$ y $A_\Phi \equiv 1 \pmod{q}$, entonces $A_\Phi \equiv 1 \pmod{pq}$. Del mismo modo, si $A_\Phi \equiv -1 \pmod{p}$ y $A_\Phi \equiv -1 \pmod{q}$, entonces $A_\Phi \equiv -1 \pmod{pq}$. Los restantes casos producen las otras dos soluciones, K y $-K$, de la equación de congruencias $x^2 \equiv 1 \pmod{pq}$. En particular $A_\Phi \equiv \pm 1 \pmod{pq}$ si y sólo si $(-1)^{(q-1)/2}(-1)^{(p-1)/2} = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)$.

Afirmación: *$A_\Phi \equiv \pm 1$ si y sólo si $p \equiv q \equiv 1 \pmod{4}$.*

Para cada elemento $n \in \Phi$ existe un único $n' \in \Phi$ que satisface la congruencia $nn' \equiv \pm 1 \pmod{pq}$. De hecho, para cada clase de congruencia invertible c, exactamente una clase, c o $-c$, tiene un representante en Φ, y esto se aplica, en particular, al inverso de n. Definamos ahora un último conjunto:

$$\Omega = \{n \in \Phi | n = n'\} = \{n \in \Phi | n^2 \equiv \pm 1\}.$$

Como $nn' = \pm 1$, se tiene $A_\Phi \equiv \pm A_\Omega \pmod{pq}$. Cuando $p \equiv q \equiv 1$, $\Omega = \{a, b, c, d\}$ donde $a = 1$, $b = \pm K$, $a = \pm L$, y $b = \pm KL$, para algún L que satisface $L^2 \equiv -1 \pmod{pq}$. En este caso $A_\Omega \equiv \pm K^2 L^2 \equiv \pm 1 \pmod{pq}$. De otro modo $L^2 \equiv -1 \pmod{pq}$ no tiene soluciones, por lo que $\Omega = \{a, b\}$ y $A_\Omega \equiv \pm K \pmod{pq}$. Esto prueba la afirmación.

La demostración se termina ahora si probamos que la identidad

$$(-1)^{(q-1)/2}(-1)^{(p-1)/2} = (-1)^{\frac{(q-1)(q-1)}{4}}$$

es equivalente a $p \equiv q \equiv 1 \pmod{4}$. Esto es inmediato de la Tabla 3.1. □

En el siguiente ejemplo vemos como la ley de reciprocidad permite el cálculo de símbolos de Legendre:

$p \pmod 4$	$q \pmod 4$	$(-1)^{(q-1)/2}$	$(-1)^{(p-1)/2}$	$(-1)^{\frac{(q-1)(q-1)}{4}}$
1	1	1	1	1
3	1	-1	1	1
1	3	1	-1	1
3	3	-1	-1	-1

Table 3.1: El cálculo caso a caso requerido para terminar la demostración de la Ley de Reciprocidad Cuadrática.

Ejemplo 3.6. Calcularemos $\left(\frac{181}{211}\right)$. Por la ley de reciprocidad, se tiene

$$\left(\frac{181}{211}\right) = \left(\frac{211}{181}\right) = \left(\frac{30}{181}\right) = \left(\frac{2}{181}\right)\left(\frac{3}{181}\right)\left(\frac{5}{181}\right) =$$

$$-\left(\frac{3}{181}\right)\left(\frac{5}{181}\right) = -\left(\frac{181}{3}\right)\left(\frac{181}{5}\right) = -\left(\frac{1}{3}\right)\left(\frac{1}{5}\right) = -1.$$

La conclusión es que 181 no es un cuadrado módulo 211.

3.2 El Símbolo de Jacobi

El cálculo al final de la sección precedente fué sencillo sólo porque los primos involucrados eran pequeños. El cálculo de Símbolos de Legendre mediante la Ley de Reciprocidad Cuadrática nos obliga a factorizar en cada paso. A fin de evitar esto se introduce el Símbolo de Jacobi. Si m y n son números impares, este se define como sigue:

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{\alpha_1}\left(\frac{m}{p_2}\right)^{\alpha_2}\cdots\left(\frac{m}{p_r}\right)^{\alpha_r},$$

donde $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ es la descomposición de n en números primos (también impares, por cierto). De hecho los símbolos de Jacobi satisfacen propiedades similares a las de los símbolos de Legendre, por ejemplo, se tiene el siguiente resultado.

Proposición 3.7. *Si n es un entero positivo impar, entonces* $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

Demostración. Un cálculo directo, a partir de la definición, nos dá lo siguiente:

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)^{\alpha_1} \cdots \left(\frac{-1}{p_r}\right)^{\alpha_r} = (-1)^{\alpha_1 \frac{p_1-1}{2} + \cdots + \alpha_r \frac{p_r-1}{2}}.$$

Para concluir la demostración, es suficiente probar la siguiente congruencia:

$$\alpha_1(p_1 - 1) + \cdots + \alpha_r(p_r - 1) \equiv n - 1 \pmod 4.$$

Esto se hace por inducción en $\alpha_1 + \cdots + \alpha_r$. Para esto, se utiliza repetidamente la identidad siguiente:

$$(n_1 - 1) + (n_2 - 1) = n_1 n_2 - 1 - (1 - n_1)(1 - n_2) \equiv n_1 n_2 - 1 \pmod 4,$$

la que es válida para cualquier par de números impares n_1 y n_2, ya que $1 - n_1$ y $1 - n_2$ son pares. Dejamos los detalles al lector. □

Proposición 3.8. *Si n es un entero positivo impar, entonces* $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Demostración. En este caso el razonamiento es análogo al anterior, pero debe usarse la congruencia

$$(n_1^2 - 1) + (n_2^2 - 1) = n_1^2 n_2^2 - 1 - (1 - n_1^2)(1 - n_2^2) \equiv (n_1 n_2)^2 - 1 \pmod{16}.$$

□

En la congruencia de arriba, 16 puede remplazarse por 64, pero no es necesario. El último resultado es la Ley de Reciprosidad cuadrática:

Proposición 3.9 (Ley de Reciprocidad Quadrática Para Simbolos de Jacobi.)**.** *Si n y m son enteros positivos e impares, entonces*

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}.$$

Demostración. Asumiremos que $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ y $m = q_1^{\beta_1} \cdots q_s^{\beta_s}$. Un cálculo directo nos dá lo siguiente:

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left[\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right]^{\alpha_i\beta_j} = \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\left(\alpha_i \frac{p_i-1}{2}\right)\left(\beta_j \frac{q_j-1}{2}\right)}$$

$$= (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\left(\alpha_i \frac{p_i-1}{2}\right)\left(\beta_j \frac{q_j-1}{2}\right)} = (-1)^{\left(\sum_{i=1}^{r}\alpha_i \frac{p_i-1}{2}\right)\left(\sum_{j=1}^{s}\beta_j \frac{q_j-1}{2}\right)}.$$

Desde aquí, el resultado se concluye utilizando las mismas congruencias de antes. □

El principal uso de los Símbolos de Jacobi es que simplifican los cálculos, ya que no es necesario comprobar a cada paso que los números involucrados son primos. Basta con comprobar que son impares, y para ello basta mirar el último dígito.

Ejemplo 3.10. Calcularemos $\left(\frac{541}{653}\right)$. Por la ley de reciprocidad, se tiene

$$\left(\frac{541}{727}\right) = \left(\frac{727}{541}\right) = \left(\frac{186}{541}\right) = \left(\frac{2}{541}\right)\left(\frac{93}{181}\right) = -\left(\frac{93}{181}\right) =$$

$$-\left(\frac{181}{93}\right) = -\left(\frac{-5}{93}\right) = -\left(\frac{-1}{93}\right)\left(\frac{5}{93}\right) = -(1)\left(\frac{93}{5}\right) = -\left(\frac{3}{5}\right) = 1.$$

Una precaución, sin embargo, es importante. Si n no es un número primo, el número $\left(\frac{m}{n}\right)$ puede ser 1 sin que m sea un cuadrado módulo n. El símbolo de Jacobi tiene una utilidad estrictamente computacional.

Ejemplo 3.11. El número 3 no es un cuadrado módulo 5 ni módulo 7. Por un lado, esto prueba que $x^2 \equiv 3 \pmod{35}$ no tiene soluciones. Por otro lado $\left(\frac{3}{35}\right) = \left(\frac{3}{5}\right)\left(\frac{3}{7}\right) = (-1)^2 = 1$.

3.3 Ejercicios

1. Calcule los posibles valores del número de soluciones en $\mathbb{Z}/n\mathbb{Z}$ de la ecuación $x^2 + ax + b = 0$, si n es el producto de siete primos distintos.

2. Determine si 1492 es o no un cuadrado módulo 2017 puede utilizar como conocido el hecho de que 2017 es primo.

3. Probar que 3 es un cuadrado módulo un primo p si y sólo si p es congruente a 1 o -1 módulo 12.

4. Determine para que valores del primo p el polinomio $x^2 + x + 1$ tiene soluciones módulo p.

5. Calcule los símbolos de Jacobi $\left(\frac{495}{177}\right)$, $\left(\frac{877}{895}\right)$ y $\left(\frac{3072}{4061}\right)$.

6. Determine si 148 es o no un cuadrado módulo $10.379 = 97 \times 107$. Justifique.

7. Probar en detalle que el símbolo de Jacobi es multiplicativo, es decir $\left(\frac{k_1 k_2}{n}\right) = \left(\frac{k_1}{n}\right)\left(\frac{k_2}{n}\right)$.

8. Probar que si n y m son enteros impares, y si $\left(\frac{m}{n}\right) = -1$, entonces m no es un cuadrado módulo n.

Chapter 4

Polinomios y extensiones de anillos

En este capítulo introduciremos el concepto de extensión de anillo, con el propósito explicito de definir extensiones del anillo $\mathbb{Z}$ de enteros, y eventualmente introducir el anillo de enteros en un cuerpo de números. Antes de esto, necesitamos repasar las propiedades básicas de los anillos de polinomios.

Por definición, el anillo de polinomios $C[x]$ sobre un anillo conmutativo C (unitario o no), se define como el anillo de todas las sumas formales finitas del tipo:

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + \cdots + a_nx^n,$$

Con $a_0, a_1, \ldots, a_n \in C$. Para ciertos fines, es conveniente agregar algunos coeficientes nulos al final de la expresión anterior. Por convención, esto no tiene ningún efecto rn el polinomio. Esto permite definir la suma de dos polinomios de manera concisa. Específicamente, si $f(x) = a_0 + \cdots + a_nx^n$ y $g(x) = b_0 + \cdots + b_mx^m$, con $m \leq n$, podemos rellenar los coeficientes de g con ceros y escribir

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots (a_n + b_n)x^n,$$

donde $b_{m+1} = b_{m+2} = \cdots = b_n = 0$. Del mismo modo, el producto se define mediante $f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_Nx^N$, donde c_n se define por las formulas $c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$, etcétera. La fórmula general para estos coeficientes es $c_t = \sum_{k=0}^{t} a_kb_{t-k}$. Es fácil ver que $c_N = 0$ si $N > n + m$, por lo que basta tomar la suma hasta $n + m$ en la fórmula que define el

producto. El último coeficiente en tal suma será $c_{n+m} = a_n b_m$, ya que los otros términos en la suma que define c_{n+m} tienen un factor nulo. Por cierto, este coeficiente podría anularse si C no es un dominio de integridad, pero es el último término que no estamos seguros que se anule antes de calcular. Cuando C es un dominio, se tiene siempre $c_{n+m} \neq 0$, en tanto $a_n \neq 0$ y $b_m \neq 0$. En este caso se concluye que el grado de un polinomio satisface la conocida identidad $\deg(fg) = \deg f + \deg g$. En el caso general, sólo podemos afirmar que $\deg(fg) \leq \deg f + \deg g$. Con estas definiciones, el anillo de polinomios es un anillo conmutativo. Si C es unitario, también lo es $C[x]$. La unidad de $C[x]$ es el polinomio constante $1_{C[x]} = 1 = 1 + 0x + 0x^2 + \cdots + 0x^n$. Por lo general, no escribiremos los términos con coeficiente 0, ni los coeficientes 1 que multipliquen una potencia no trivial de x. Estas convenciones están totalmente estandarizadas por lo que esperamos que quien lea esté familiarizado con ellas.

4.1 La propiedad universal y sus consecuencias

Nos queda una última propiedad del anillo de polinomios con la que esperamos que el lector esté familiarizado. Esta es, sin duda, la principal razón por la que el anillo de polinomios es importante para el algebrista:

> **Propiedad Universal del Anillo de Polinomios.** *Si $\phi : C \to B$ es un homomorfismo de anillos, donde C es conmutativo, dado cualquier $a \in B$ que conmuta con cada imagen $\phi(c)$ con $c \in C$, existe un homomorfismo de anillos $\tilde{\phi}_a : C[x] \to B$ que lleva a x en a y cuya restricción a C es ϕ.*

La principal aplicación del principio anterior que utilizaremos en lo sucesivo es la siguiente:

> **Evaluación de Polinomios.** *Si B es un anillo que contiene al anillo conmutativo C como un subanillo, dado cualquier $a \in B$ existe un homomorfismo de anillos $\tilde{\phi}_a : C[x] \to B$ que lleva a x en a y cuya restricción a C es la identidad.*

En este último caso, la imagen $\tilde{\phi}_a\Big(f(x)\Big)$ se denota simplemente $f(a)$, y a la función $\tilde{\phi}_a$ se la denomina evaluación en a. Una consecuencia del

hecho de que ϕ_a sea un homomorfismo es que $f(a)g(a) = g(a)f(a)$ para todo $a \in B$. En otras palabras, polinomios en la misma variable conmutan. El caso no conmutativo no será necesario en estas notas hasta llegar a la teoría de órdenes en un capítulo muy posterior.

Lo anterior puede generalizarse a cualquier número finito de variables. Por simplicidad, damos aquí sólo la versión conmutativa:

> **Propiedad Universal del Anillo de Polinomios en n variables.** *Sea B y C anillos conmutativos, y sea $\phi : C \to B$ un homomorfismo. Si $a_1, \ldots, a_n$ son elementos arbitrarios de B, entonces existe una funcion*
>
> $$\tilde{\phi} : C[x_1, \ldots, x_n] \to B$$
>
> *que lleva a x_i en a_i y cuya restricción a C es ϕ.*

Una aplicación muy importante del resultado anterior, que sigue fácilmente usando expansiones de Taylor de polinomios a coeficientes reales es la siguiente:

> **Principio de extensión de identidades.** *Toda identidad entre polinomios $f, g \in \mathbb{Z}[x_1, \ldots, x_n]$ del tipo $f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$ que se cumple para valores reales de las variables se cumple en cualquier anillo conmutativo.*

Algunos ejemplos de identidades de este tipo son las siguientes:

1. El teorema del binomio.
2. La identidad $A\tilde{A} = \det(A)I_n$, donde A es una matriz de n por n e I_n es la identidad.
3. La multiplicatividad del determinante.

Se sigue del principio de extensión que estas identidades se cumplen en todo anillo conmutativo. En particular, de los ejemplos 2 y 3 se sigue que un elemento de $\mathbb{M}_n(C)$ es invertible si y sólo si su determinante lo es, en cuyo caso su inverso es $[\det C]^{-1}\tilde{C}$.

Ejemplo 4.1. La matrix

$$\begin{pmatrix} \bar{5} & \bar{4} & \bar{8} \\ \bar{7} & \bar{3} & \bar{6} \\ \bar{5} & \bar{5} & \bar{5} \end{pmatrix}$$

con coeficientes en $\mathbb{Z}/3\mathbb{Z}$ es invertible. Dejamos como ejercicio para el lector el cálculo de su inverso.

Sea B un anillo que contiene a C como subanillo. Sea a un elemento de B. el anillo generado por a sobre C es el subanillo más pequeño de B que contiene a C y a a y se le denota por $C[a]$. Puede también caracterizarse como la imagen del homomorfismo evaluación $\phi_a : C[x] \to B$. En particular $C[a] \cong C[x]/\ker(\phi_a)$.

Ejemplo 4.2. Para todo anillo conmutativo C y todo elemento $c \in C$ se tiene $C = C[c] \cong \frac{C[x]}{(x-c)}$.

Ejemplo 4.3. El anillo $\mathbb{Z}[i]$ es el anillo de números complejos de la forma $a + bi$ con a y b enteros, ya que $i^n \in \{1, -1, i, -i\}$ para todo n. Se sigue del resultado anterior que $\mathbb{Z}[i] \cong \mathbb{Z}[x]/I$ donde I es el núcleo de la evaluación en i. De hecho, probaremos más abajo que $I = (x^2 + 1)$.

Ejemplo 4.4. El anillo $\mathbb{Z}[\sqrt{2}]$ es el anillo de números reales de la forma $a + b\sqrt{2}$ con a y b enteros, ya que $(\sqrt{2})^n \in \mathbb{Z} \cup \sqrt{2}\mathbb{Z}$ para todo n. Se sigue del resultado anterior que $\mathbb{Z}[\sqrt{2}] \cong \mathbb{Z}[x]/I$ donde I es el núcleo de la evaluación en $\sqrt{2}$. De hecho, probaremos más abajo que $I = (x^2 - 2)$.

Mas generalmente, si $a_1, \ldots, a_n$ son elementos de B, el anillo $C[a_1, \ldots, a_n]$ es la imagen del homomorfismo evaluación $\phi_{a_1,\ldots,a_n}$ y se tiene $C[a_1, \ldots, a_n] \cong C[x_1, \ldots, x_n]/\ker(\phi_{a_1,\ldots,a_n})$.

Ejemplo 4.5. Si $a_1, \ldots, a_n$ no satisfacen ninguna ecuación con coeficientes en C, el homomorfismo evaluación $\phi_{a_1,\ldots,a_n}$ es inyectivo y en tal caso se dice que $a_1, \ldots, a_n$ son algebraicamente independientes sobre C. El anillo generado por n elementos algebraicamente independientes es isomorfo al anillo de polinomios, ya que el homomorfismo evaluación es inyectivo. Es posible, aunque no sencillo, demostrar que $e = 2,7172\ldots$ y $e^{\sqrt{2}}$ son algebraicamente independientes sobre $\mathbb{Z}$. Si $\{a\}$ es algebraicamente independiente como conjunto unitario, se dice que a es trascendente sobre C. El número real $\pi = 3,14159\ldots$ es un ejemplo de número tascendente sobre $\mathbb{Z}$ o $\mathbb{Q}$.

4.2 El algoritmo de la división

En esta ssección introduciremos algunas herramientas que resultan cruciales en la demostración de los ejemplos mostrados en la sección anterior. Recuérdese que un polinomio mónico es aquel cuyo coeficiente principal (o de mayor grado) es uno.

Proposición 4.6. *Si f y g son dos polinomios en $C[x]$, con f mónico, entonces* $\deg(fg) = \deg f + \deg g$.

Demostración. Asumamos que $f(x) = x^n + \cdots$, donde los puntos representan términos de grado menor, y $g(x) = ax^m + \cdots$. Entonces $f(x)g(x) = ax^{n+m} + \cdots$, de donde se sigue el resultado. □

Proposición 4.7. *Si u satisface un polinomio mónico f de grado d con coeficientes en C, entonces todo elemento a de $C[u]$ puede escribirse en la forma $a = r(u)$ con* $\deg(r) < d$.

Demostración. Basta probar que, para todo polinomio $h(x) \in C[x]$ existe un polinomio r con $\deg(r) < d$ que satisface $h(u) = r(u)$. Si $\deg(h) < d$ no hay nada que probar, por lo que suponemos que $h(x) = ax^n + \ldots$, donde los puntos representan términos de grado menor, y que $\deg(h) = n > \deg(f)$. Entonces $h_1(x) = h(x) - af(x)$ es un polinomio de grado menor a h y que satisface $h_1(u) = h(u)$. Se sigue ahora del principio de inducción completa que existe un polinomio $r(x)$ de grado menor a f tal que $r(u) = h_1(u) = h(u)$. □

Proposición 4.8 (Algoritmo de división para polinomios mónicos)**.** *Si f es un polinomio mónico de grado d con coeficientes en C, entonces todo elemento $h(x) = C[x]$ puede escribirse de manera única en la forma $h(x) = r(x) + q(x)f(x)$ con* $\deg(r) < \deg(f)$.

Demostración. Para probar la existencia consideramos la clase lateral $u = x + (f) \in C[x]/(f)$. Claramente $f(u) = 0$ en el anillo cociente. El resultado precedente nos dice que $h(x)+(f) = h(u) = r(u)$ para algún polinomio r con $\deg(r) < d$. La condición $h(u) = r(u)$ nos dice que $h(x) - r(x) \in (f)$, por lo que podemos escribir $h(x) - r(x) = q(x)f(x)$. Esto prueba la existencia. Para la unicidad observamos que $q(x)f(x) + r(x) = q'(x)f(x) + r'(x)$ implica

$f(x)\Big(q(x)-q'(x)\Big)=r'(x)-r(x)$. Como f no puede dividir a un polinomio no trivial de menor grado, debemos tener $r'(x)=r(x)$. Del mismo modo, la multiplicación por f no puede anular a un polinomio no trivial. Concluímos que $q(x)=q'(x)$. □

Ejemplo 4.9. El número complejo i satisface la ecuación polinomica $x^2+1=0$. Se sigue del resultado anterior que todo elemento de $\mathbb{Z}[x]/(x^2+1)$ se escribe de manera única en la forma $a+b\bar{x}$ con a y b enteros. Como $a+bi\neq 0$ para cada par de enteros a y b, se sigue que (x^2+1) es el núcleo de la evaluación en i y por lo tanto $\mathbb{Z}[i]\cong\mathbb{Z}[x]/(x^2+1)$. En particular, cada elemento del anillo $\mathbb{Z}[i]$ puede escribirse el la forma $a+bi$ con a y b enteros.

Ejemplo 4.10. El número irracional $\sqrt{2}$ satisface la ecuación polinomica $x^2-2=0$. Se sigue del resultado anterior que todo elemento de $\mathbb{Z}[x]/(x^2-2)$ se escribe de manera única en la forma $a+b\bar{x}$ con a y b enteros. Se sigue como en el ejemplo precedente que (x^2-2) es el núcleo de la evaluación en $\sqrt{2}$ y por lo tanto $\mathbb{Z}[\sqrt{2}]\cong\mathbb{Z}[x]/(x^2-2)$, mientras que cada elemento de $\mathbb{Z}[\sqrt{2}]$ tiene la forma $a+b\sqrt{2}$ con a y b enteros.

Los resultados y ejemplos de esta sección motivan la siguiente definición que será crucial en lo que sigue. Un elemento b de un anillo B, que contiene a un subanillo C, se dice entero sobre C, si satisface un polinomio mónico con coeficientes en C.

Ejemplo 4.11. El anillo $\mathbb{Z}[\frac{1}{2}]$ es el anillo de números racionales de la forma $\frac{n}{2^t}$ con n entero. En este caso, es imposible escribir $\frac{1}{2^t}$ como un polinomio en $\frac{1}{2}$ de grado menor a t. Sea $f(x)$ un polinomio con coeficientes enteros tal que $f(\frac{1}{2})=0$. Si $f(x)=a_nx^n+\ldots+a_0$, se deduce desarrollando $2^nf(\frac{1}{2})$ que 2 divide a a_n. Luego $f(x)-(2x-1)\frac{a_n}{2}x^{n-1}$ es un polinomio de grado menor que f que cumple la misma propiedad. Se concluye por inducción que $f(x)$ es divisible por $2x-1$. Luego $\mathbb{Z}[\frac{1}{2}]\cong\mathbb{Z}[x]/(2x-1)$.

El anterior es un ejemplo típico de anillo generado por un elemento no entero. Para tratar anillos como este, probaremos una generalización del resultado anterior:

Proposición 4.12. *Si $f(x)=a_dx^d+\ldots$ es un polinomio de grado d con coeficientes en C, y si S es un conjunto completo de representantes de $C/(a_d)$ que incluye al 0, entonces todo elemento $h(x)\in C[x]$ de grado m puede*

escribirse en la forma $r(x) + x^d g(x) + q(x)f(x)$ *donde* $\deg(r) < \deg(f)$ *y* $g(x)$ *es un polinomio de grado no mayor a* $m - d$ *con coeficientes en* S*. Si* a_d *no es un divisor de* 0 *esta representación es única.*

Demostración. Supongamos que $h(x)$ es un elemento de $C[x]$ con $h(x) = bx^m + \ldots$, con las convenciones anteriores. Entonces existe $s \in S$ con $b - s = ta_d$ para algún $t \in C$. Luego $h(x) - sx^m - tx^{m-d}f(x)$ tiene grado menor que h y se concluye por inducción completa como en la proposición anterior. Para probar la unicidad, supongamos que

$$h(x) = r(x) + x^d g(x) + q(x)f(x) = r_0(x) + x^d g_0(x) + q_0(x)f(x),$$

donde los elementos de $\{r, r_0\}$ tienen grado menor a d ,mientras que los de $\{g, g_0\}$ tienen grado no mayor a $m-d$ y coeficientes en S. Entonces tenemos

$$[q_0(x) - q(x)]f(x) = [r(x) - r_0(x)] + x^d[g(x) - g_0(x)]. \tag{4.1}$$

Supongamos que $q_0(x) \neq q(x)$. Sea $q_0(x) - q(x) = bx^r + \ldots$, con la convención usual. El término de mayor grado en $[q_0(x) - q(x))](x)$ es abx^{r+d}. El polinomio $g(x) - g_0(x)$ no puede tener ningún coeficiente no nulo divisible por a, y los términos de grado mayor o igual a d en el lado derecho de (4.1) son exactamente los términos de $x^d[g(x) - g_0(x)]$. Se concluye, por contradicción, que $q_0(x) = q(x)$, luego

$$r(x) - r_0(x) = -x^d[g(x) - g_0(x)].$$

Como el lado izquierdo tiene sólo términos de grado menor que d y el lado derecho tiene sólo términos de grado mayor o igual a d, deben ser ambos 0. El resultado sigue. □

Ejemplo 4.13. El conjunto $\{0, 1\}$ es un conjunto de repreentantes de $\mathbb{Z}/2\mathbb{Z}$. Se sigue que, en el anillo $\mathbb{Z}[x]/(2x)$, cada elemento tiene una única representación de la forma $n + \bar{x}^{i_1} + \ldots + \bar{x}^{i_s}$ con $n \in \mathbb{Z}$ y enteros positivos $i_1, \ldots, i_s$ distintos. Este elemento no puede representarse por un polinomio de grado inferior al máximo de los i_t. De hecho, este anillo es isomorfo al subanillo de $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}[x]$ formado por los pares $\Big(n, F(x)\Big)$ en los que la imagen de n en $\mathbb{Z}/2\mathbb{Z}$ es $F(0)$. Para comprobar esto basta considerar el homomorfismo

$$\phi : \mathbb{Z}[x] \to \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}[x]$$

que envía a $f(x)$ en $\Big(f(0), \overline{f(x)}\Big)$, donde la barra horizontal indica reducción módulo 2. Es evidente que cada imagen es un par de la forma dada, y para encontrar una pre-imagen de uno de estos pares $\Big(n, F(x)\Big)$ se utiliza un polinomio de la forma $n + x^{i_1} + \ldots + x^{i_s}$, donde $F(x) = \bar{n} + \bar{x}^{i_1} + \ldots + \bar{x}^{i_s}$. Sólo queda probar que el núcleo es el ideal $(2x)$, para lo que observamos lo siguiente:

- $\overline{f(x)} = 0$ si cada coeficiente de f es par.
- $f(0) = 0$ si y sólo si f no tiene coeficiente libre.

Sólo nos queda observar que un polinomio que cumple estas condiciones es divisible por $2x$.

Ejemplo 4.14. Al igual que en el ejemplo anterior, utillizamos el conjunto de representantes $\{0, 1\}$, esta vez para analizar el anillo $\mathbb{Z}[x]/(2x+1) \cong \mathbb{Z}[1/2]$. Nuevamente, cada elemento tiene una única representación de la forma $n + \bar{x}^{i_1} + \ldots + \bar{x}^{i_s}$ con $n \in \mathbb{Z}$ $i_1, \ldots, i_s$ enteros positivos diferentes. En este caso, el mismo razonamiento del ejemplo precedente nos dá una representación del tipo

$$\frac{a}{b} = n + \frac{1}{2^{i_1}} + \frac{1}{2^{i_2}} + \cdots + \frac{1}{2^{i_s}}.$$

Ejemplo 4.15. Sea $C = \mathbb{Z}/6\mathbb{Z}$. Tomando $f(x) = 3x+1 \in C[x]$, y utilizando que $\{\bar{0}, \bar{1}, \bar{2}\}$ es un conjunto completo de representantes de $\mathbb{Z}/3\mathbb{Z} \cong C/(\bar{3})$, vemos que x tiene al menos dos representaciones diferentes del tipo $x = r(x) + x^d g(x) + q(x)f(x)$, a saber:

- $x = \bar{2}(\bar{3}x + \bar{1}) - \bar{2}$, con $\Big(q(x), g(x), r(x)\Big) = (\bar{2}, \bar{0}, -\bar{2})$.
- $x = x$, donde $\Big(q(x), g(x), r(x)\Big) = (\bar{0}, \bar{1}, \bar{0})$.

Por cierto $\bar{3}$ es un divisor de cero en el anillo C.

Ejemplo 4.16. Sea $C = \mathbb{Z}$. Tomamos $f(x) = 3x + 1 \in C[x]$ y el conjunto de representantes $\{1, 2, 3\}$ de $\mathbb{Z}/3\mathbb{Z}$, el cual no contiene al 0. En este caso, el elemento $3x^2$ tiene al menos dos representaciones diferentes, a saber:

- $3x^2 = (x-1)(3x+1)+x(2)+1$, donde$\Big(q(x), g(x), r(x)\Big) = (x-1, 2, 1)$.
- $3x^2 = -(3x+1)+x(3x+3)+1$, con $\Big(q(x), g(x), r(x)\Big) = (-1, 3x+3, 1)$.

4.3 El lemma de Gauss

Para tratar con más facilidad anillos generados por elementos no enteros, necesitaremos herramientas más especializadas. La principal es el Lema de Gauss, el que también nos permite describir los elementos primos de un dominio de factorización única (DFU).

En lo que sigue, diremos que un dominio D es un dominio de factorización única si cada elemento no nulo puede escribirse en la forma

$$d = up_1^{\alpha_1} \dots p_r^{\alpha_r},$$

donde u es una unidad, mientras que $p_1, \dots, p_r$ son primos no asociados, es decir $p_i \neq vp_j$ para cada par de índices (i, j) y cada unidad v. En particular, todo DIP es un DFU, pero la conversa no se cumple. Por ejemplo, el anillo de polinomios con coeficientes enteros es un DFU, como se verá mas abajo, pero no es un DIP. Específicamente, es fácil ver que el ideal $(3, x)$ no contiene al 1, por lo que es un ideal propio. No obstante, el hecho de que 3 y x son primos diferentes, y por lo tanto relativamente primos, muestra que este ideal no puede tener un generador que no sea una unidad.

En general un polinomio $f(x) \in D[x]$ se dice primitivo si ningún primo de D lo divide. Equivalentemente, $f(x)$ es primitivo si ningún primo de D divide simultaneamente a todos sus coeficientes. Nótese que los polinomios mónicos son primitivos.

Proposición 4.17. ***(Lemma de Gauss).*** *El producto de polinomios primitivos es primitivo.*

Demostración. Sean $f(x)$ y $g(x)$ dos polinomios primitivos y sea $p \in D$ un elemento primo. Por definición, ninguna de las imágenes $\overline{f(x)}$, ni $\overline{g(x)}$ se anula en el anillo cociente $D[x]/(p)$. Nótese que este último es isomorfo al anillo $(D/(p))[x]$ de polinomios con coeficientes en el anillo de cocientes. Como el anillo de polinomios sobre un dominio es un dominio, por la multiplicatividad del grado, se concluye que $D[x]/(p)$ es un dominio. Se concluye que la clase $\overline{f(x)g(x)} \in D[x]/(p)$ es no nula. Como p es arbitrario, concluimos que $f(x)g(x)$ es primitivo. □

Obsérvese que cualquier polinomio $f(x)$ en $D[x]$ puede escribirse en la forma $f(x) = nf_0(x)$ donde $n = c(f)$ es un elemento de D, al que llamaremos el contenido de f, y f_0 es un polinomio primitivo, al que llamaremos la parte

primitiva de f. El contenido es, de hecho, el máximo común divisor de los coeficientes de f, por lo que está definido sólo salvo unidades. En lo sucesivo, hablaremos del contenido $c(f)$, y de la parte primitiva de f, como si estuviesen bien definidos, pero debe tenerse presente la existencia de esta "unidad libre". Se sigue de lo anterior que si se escribe un polinomio en la forma $f(x) = nf_0(x) = mf_1(x)$, donde f_0 y f_1 son primitivos, entonces $m = un$ para alguna unidad u de D. El contenido de f es n o m, indistintamente.

Denotemos por $K = \text{Quot}(D)$ al cuerpo de cocientes del dominio D, es decir el cuerpo formado por todas las fracciones $\frac{a}{b}$ con a y b en el dominio D. Los conceptos de parte primitiva y contenido se pueden extender al cuerpo de cocientes K como sigue:

> Si $f(x)$ es un polinomio con coeficientes en K, podemos escribirlo en la forma $\frac{\tilde{f}(x)}{q}$, donde $\tilde{f}(x) \in D[x]$, sacando un denominador común q. Entonces, se define el contenido mediante $c(f) = \frac{c(\tilde{f})}{q}$, mientras la parte primitiva se define por $f(x)/c(f)$, o, equivalentemente, como la parte primitiva de $\tilde{f}$.

Tal como en el anillo D, el contenido y la parte primitiva en $K[x]$ están bien definidos salvo unidades, ya que cualquier identidad del tipo $\frac{\tilde{f}(x)}{q} = \frac{\tilde{f}_1(x)}{q_1}$ implica una identidad $q_1\tilde{f}(x) = q\tilde{f}_1(x)$ en $D[x]$, la que puede utilizarse para probar que las partes primitivas de $\tilde{f}(x)$ y $\tilde{f}_1(x)$ coinciden.

Proposición 4.18. ***(Lemma de Gauss, segunda versión).*** *Todo polinomio irreducible en $D[x]$ es irreducible en $K[x]$.*

Demostración. Sean $f(x)$ un polinomio irreducible en $D[x]$. Supongamos que f tiene una factorización $f(x) = g(x)h(x)$ en $K[x]$. Utilizamos las descomposiciones $h(x) = c(h)h_0(x)$ y $g(x) = c(g)g_0(x)$, escribimos

$$f(x) = c(h)c(g)h_0(x)g_0(x).$$

Como el polinomio $h_0(x)g_0(x)$ es primitivo, debe ser la parte primitiva de f, mientras que $c(h)c(g) = c(f)$ es su contenido. Se concluye que $f(x) = c(f)h_0(x)g_0(x)$, lo que es una factorización en $D[x]$. □

Proposición 4.19. *Todo polinomio $f(x) \in D[x]$ es irreducible si y sólo si satisface las dos condiciones siguientes:*

- $f(x)$ *es primitivo.*
- $f(x)$ *es irreducible como elemento de* $K[x]$*.*

Demostración. La factorización $f(x) = c(f)f_0(x)$ muestra que la primera condición es necesaria, mientras que la segunda lo es por la proposición precedente. Por otro lado, la primera condición sirve para evitar factorizaciones del tipo $f(x) = dh(x)$ donde $d \in D$ es una constante no trivial. Cualquier otra factorización es también una factorización no trivial en $K[x]$. □

Para lo que sigue es conveniente recordar que las unidades del anillo $D[x]$, cuando D es un dominio, son precisamente las constantes invertibles.

Proposición 4.20. ***(Lemma de Gauss, tercera versión).*** *Si* D *es un DFU, entonces* $D[x]$ *es un DFU.*

Demostración. Basta ver que cada elemento $f(x) \in D[x]$ es producto de primos. De hecho, en $K[x]$, tenemos una factorización

$$f(x) = up_1(x)^{\alpha_1}, \cdots, p_r(x)^{\alpha_r},$$

donde u es una constante y cada $p_i(x)$ es un polinomio primo que, cambiándo la constante de ser necesario, podemos suponer primitivo en $D[x]$. Se sigue que estos polinomios son irreducibles en $D[x]$ y su producto es la parte primitiva de f. Se sigue que u es el contenido de f, y por lo tanto está en D. Podemos, por lo tanto, escribir u como un producto de primos de D, los que siguen siendo primos en $D[x]$, como se prueba más arriba. Para terminar la demostración, basta ver que los polinomios irreducibles en $D[x]$ son primos.

Sea $g(x) \in D[x]$ un polinomio irreducible, y por lo tanto primitivo. Supongamos que $g(x)h(x) = G(x)H(x)$, donde h, G y H son polinomios en $D[x]$. Se sigue que g divide a G o H, digamos G, en $K[x]$. Digamos $G(x) = g(x)q(x)$. Basta ver que $q(x)$ tiene coeficientes en D. Tomando contenidos, obtenemos $c(G) = c(g)c(q)$. Como g es primitivo, $c(g)$ es una unidad, y $c(G) \in D$, pues G tiene coeficientes en D. Se concluye que $c(q) \in D$, por lo que q tiene coeficientes en D. El resultado sigue. □

Ejemplo 4.21. El polinomio $4x^2 + 1$ es primitivo e irreducible en $\mathbb{Q}[x]$, por lo que es un elemento primo de $\mathbb{Z}[x]$. Además, cada polinomio que cumple $f(i/2) = 0$ en $\mathbb{Q}[x]$ es un múltiplo de $4x^2 + 1$. Se sigue del Lemma de Gauss que lo mismo ocurre en $\mathbb{Z}[x]$. Concluimos que

$$\mathbb{Z}[i/2] \cong \mathbb{Z}[x]/(4x^2 + 1).$$

****