

Teoría de Números Algebraicos

Luis Arenas

August 24, 2021

Contents

1	De los enteros y otros dominios	3
1.1	Anillos, anillos conmutativos y sus ideales	3
1.2	Dominios Euclidianos	5
1.3	Máximo común divisor	7
1.4	Asociados y factorización única	10
1.5	Ejercicios	12
2	Congruencias	14
2.1	Inversos módulo n	15
2.2	Elementos idempotentes y productos de anillos	18
2.3	El Teorema Chino de los Restos	23
2.4	Elementos nilpotentes y series de potencias	25
2.5	Derivadas formales	27
2.6	El Lema de Hensel	29
2.7	El grupo de unidades módulo n	31
2.8	Ejercicios	35
3	Residuos cuadráticos y reciprocidad	37
3.1	La ley de reciprocidad cuadrática	40
3.2	El Símbolo de Jacobi	44
3.3	Ejercicios	46
4	Polinomios y extensiones de anillos	48
4.1	La propiedad universal y sus consecuencias	49
4.2	El algoritmo de la división	52
4.3	El lemma de Gauss	56
4.4	Cocientes de $\mathbb{Z}[x]$ y $\mathbb{Z}[\alpha]$	60
4.5	Ejercicios	64

5	Anillos de enteros	68
5.1	Elementos enteros sobre un anillo	68
5.2	Enteros en cuerpos cuadráticos	72
5.3	Enteros de Gauss	74
5.4	Enteros de Eisenstein	87
5.5	Ejercicios	98

Chapter 1

De los enteros y otros dominios

1.1 Anillos, anillos conmutativos y sus ideales

El conjunto $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ 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 , tanto su intersección $I \cap J$ como su suma $I + J = \{a + b|a \in I, b \in J\}$ son ideales. También es un ideal su producto IJ , definido como sigue:

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

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 $M_n(K)$, con coeficientes en un cuerpo K , las unidades son las matrices con determinante no nulo. Más generalmente, si consideramos el anillo de matrices $M_n(C)$, 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 coordenadas, tiene como unidades precisamente a los elementos con todas 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 $\bar{1} + \bar{2}x$ es una unidad, ya que se tiene la relación

$$(\bar{1} + \bar{2}x)(1 - \bar{2}x) = \bar{1} - \bar{4}x^2 = \bar{1}.$$

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

1.2 Dominios Euclidianos

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

Para todo elemento $m \in D$, y para todo $n \in D \setminus \{0\}$, existen elementos q y r en D , llamados el cociente y el resto, que satisfacen las relaciones siguientes:

$$n = qm + r \quad \text{y} \quad \left(g(r) < g(m) \text{ o } r = 0 \right).$$

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 Euclideo. 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 es 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 $r'' \leq \frac{b}{2}$.

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. $\square$

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 euclideo 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. $\square$

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 da el ideal nulo $(0) = \{0\}$, y el caso $n = \pm 1$, lo que nos da 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:

$$n = q_0m + r_0,$$

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

$$m = q_1r_0 + r_1, \quad r_0 = q_2r_1 + r_2, \dots, r_i = q_{i+2}r_{i+1} + r_{i+2}, \dots$$

con $g(r_0) > g(r_1) > g(r_2) > \dots$

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

Demostración Sea I el ideal $(n) + (m)$. Como $n - q_0m = r_0$ y $m - q_1r_0 = r_1$, 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 $m = q_1r_0 + r_1$, se tiene que m está en (r_t) . Finalmente, $n = q_0m + r_0$ implica $n \in (r_t)$. Se concluye que $(r_t) = I$. $\square$

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 $r_{t-2} = q_tr_{t-1} + r_t$ demuestran que $(r_{t-2}, r_{t-1}) \subseteq (r_t)$, mientras que, al despejar $r_t = -q_tr_{t-1} + r_{t-2}$, se obtiene la contención inversa $(r_t) \subseteq (r_{t-2}, r_{t-1})$. Iterando este argumento, se obtiene la cadena de identidades siguiente:

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

Alternativamente, uno puede interpretar las ecuaciones $r_{t-1} = q_{t+1}r_t$ y $r_{t-2} = q_tr_{t-1} + r_t$ 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 encontrar los elementos 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 máximo común divisor de 148 y 256. Comenzamos dividiendo 256 por 148.

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

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

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

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

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:

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

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

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

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 simultáneamente $n'|n$ y $n|n'$. Equivalentemente, dos elementos, n y n' son asociados si y sólo si generan el mismo ideal principal, es decir $(n) = (n')$. Obsérvese 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 elementos 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. $\square$

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). $\square$

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 en 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

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

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

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

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. $\square$

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, se concluye la igualdad $(q) = (p)$. $\square$

Proposición 1.16. *Sea D un DIP. Sea*

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

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. Supongámoslo 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 también 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. $\square$

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

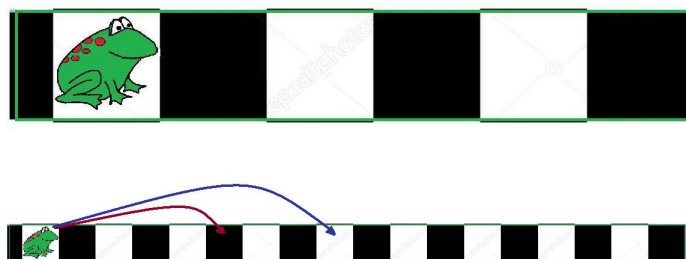


Figure 1.1: Una ranita en una cinta infinita.

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 nombre 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 $a \equiv b \pmod{J}$. En el caso de un ideal principal de la forma $J = nA$, se usa a menudo la forma $a \equiv b \pmod{n}$. 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 . $\square$

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:

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

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

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 tarea de entender por qué este procedimiento es equivalente al algoritmo de Euclides.

En álgebra, hay un segundo ejemplo de dominio euclideo 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 $\phi_a : K[x] \rightarrow A$ 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 irreducible).

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. La 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 raíz quinta primitiva de la unidad, cuyo polinomio irreducible es $1+x+x^2+x^3+x^4$. Para esto, busquemos 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 raíz $\sqrt[3]{2}$, 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 raíz del primer polinomio. Dado que $\alpha^2 = -3(\alpha + 1)$, obtenemos lo siguiente:

$$\begin{aligned} 1 &= (\alpha^3 - 2)u(\alpha) = \left(-3(\alpha + 1)\alpha - 2\right)u(\alpha) = (-3\alpha^2 - 3\alpha - 2)u(\alpha) \\ &= (6\alpha - 7)u(\alpha). \end{aligned}$$

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:

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

□

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:

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

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. $(1-P)^2 = 1-P-P+P^2 = 1-P-P+P = 1-P$. $\square$

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: $Px = PPy = Py = x$. $\square$

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 $A \cong PA \times P^cA$. $\square$

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

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

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. También 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 $P_1 P_2 = P_1$.

Proposición 2.12. $P_1 < P_2$ si y sólo si $P_1 A \subseteq P_2 A$.

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 $P_1P_2 = P_1$. $\square$

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. $\square$

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

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

Demostración. Inducción en la proposición anterior. $\square$

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

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

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

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

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 ideales 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 $P_2 = ns + nmD$. Observe 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 prueba 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 relativamente 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. $\square$

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*

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

Dos soluciones de dicho sistema son congruentes módulo mn . $\square$

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 $n_1, \dots, n_k$ elementos de D relativamente primos a pares. Entonces el anillo $A = D/nmD$ 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 $n_1, \dots, n_k$ 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. $\square$

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

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

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

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

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

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

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 $A = D/p^r D$ se caracterizan por la existencia de elementos de la forma $\pi = p + p^r D$ que satisfacen $\pi^r = 0$. 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 los elementos que no son múltiplos de π son de la forma $m + p^r D$ 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

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

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

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

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

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

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 $u - n$. $\square$

Más generalmente, toda serie de potencias con coeficientes en un anillo puede ser evaluada en un elemento 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 composición de series de potencias sólo está bien definida, en el contexto algebraico, cuando se evalúa 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 $U_{p,1} = \{1 + pt + p^r\mathbb{Z} \mid t \in \mathbb{Z}\}$ es un grupo multiplicativo 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 $\exp_{p,r} : p\mathbb{Z}/p^r\mathbb{Z} \rightarrow U_{p,1}$ 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 $\log_{p,r} : U_{p,1} \rightarrow p\mathbb{Z}/p^r\mathbb{Z}$ definida por

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

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

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

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 $g_r(u) + g_r(v) = g_r((1+u)(1+v) - 1)$ y $(1 + f_r(u))(1 + f_r(v)) = 1 + f_r(u+v)$. 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 $\phi_u : \mathbb{Z}_{(p)}[[x]] \rightarrow \mathbb{Z}/p^r\mathbb{Z}$ que se anula en x^r . Concluimos que dicha evaluación puede considerarse como una función de B a $\mathbb{Z}/p^r\mathbb{Z}$. Se concluye 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

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

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

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

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 da 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 consecuencia, podemos escribir

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

Evaluable en $y = 0$, se tiene $f_0(x) = f(x)$. Definimos la derivada formal mediante $\frac{d}{dx}(f(x)) = f'(x) = f_1(x)$. 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 difícil comprobar las propiedades

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

Por ejemplo, probaremos la última:

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

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 $\frac{d}{dx}(f(w(x))) = f'(w(x))w'(x)$.*

Demostración. Sea $h = h(x, y) = w(x + y) - w(x)$, de modo que $w(x + y) = w(x) + h$. Obsérvese 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 ahora del siguiente cálculo:

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

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

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

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

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

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 raíces de polinomios módulo p^n para cualquier n dada una raíz módulo p . La única condición necesaria para

esto es que la raíz 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 $f(x) \equiv 0 \pmod{p^n}$, 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 p^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. $f(b_{n+1}) \equiv f(b_n) - kf(b_n)f'(b_n) \pmod{(kf(b_n))^2}$.

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 da

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

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

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

nos da $tp^n = kf(b_n)$ como única solución por los cálculos precedentes. $\square$

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 $f(x) = bx - 1 \equiv 0 \pmod{p^n}$.

Ejemplo 2.29. Si el primo p no es 2, entonces un elemento $b \in \mathbb{Z}/p^n\mathbb{Z}$ 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:

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

Bastará, por lo tanto, calcular la estructura del anillo $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*$. 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 $\text{ord}(a)$ del elemento $a + n\mathbb{Z}$ divide a m si y sólo si $ma + n\mathbb{Z} = 0 + n\mathbb{Z}$. Es decir, $\text{ord}(a)|m$ si y sólo si ma es divisible por n , o, equivalentemente, a es divisible por $m' = n/m$. En particular, $\text{ord}(a) = m$ 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 da $\phi(m)$ elecciones posibles para a módulo $mm' = n$. $\square$

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. $\square$

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 raíces. En particular, se concluye que $x^n - 1$ no puede tener más de n raíces para ningún n . $\square$

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

Un generador del grupo $\mathbb{F}_p^*$ recibe el nombre de raíz 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 $x \in \mathbb{F}_p^*$. $\square$

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:

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

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:

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

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 $(\mathbb{Z}/p_i^r\mathbb{Z})^*$ 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 $(\mathbb{Z}/p^r\mathbb{Z})^*$ 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 $(\mathbb{Z}/2^r\mathbb{Z})^*$ 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 $(\mathbb{Z}/2^r\mathbb{Z})^*$. 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?

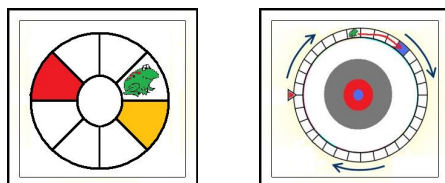


Figure 2.1: Una ranita en una ruleta.

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 raíz cuadrada de 23 módulo 121 y una raíz cuadrada de 7 módulo 243.
6. Resolver el sistema

$$\begin{aligned} x &\equiv 3 \pmod{11}, \\ x &\equiv 2 \pmod{17}, \\ x &\equiv 5 \pmod{23}. \end{aligned}$$
7. Resolver el sistema

$$\begin{aligned} 2x + 4 &\equiv 0 \pmod{11}, \\ 3x + 5 &\equiv 0 \pmod{17}, \\ 6x + 11 &\equiv 0 \pmod{23}. \end{aligned}$$

8. Resolver el sistema

$$\begin{aligned}x &\equiv 3 \pmod{7}, \\3x &\equiv -5 \pmod{11}, \\x^2 &\equiv 1 \pmod{23}.\end{aligned}$$

9. Resolver el sistema

$$\begin{aligned}x^2 + x &\equiv 0 \pmod{11}, \\x^2 + 2x + 1 &\equiv 0 \pmod{17}, \\x^2 - 1 &\equiv 0 \pmod{23}.\end{aligned}$$

10. Resolver la ecuación $x^2 - x \equiv 0 \pmod{11 \cdot 17 \cdot 23}$.
11. Resolver la ecuación $x^2 + x + 1 \equiv 0 \pmod{11 \cdot 17 \cdot 23}$.
12. Resolver la ecuación $x^2 + x + 1 \equiv 0 \pmod{7 \cdot 19 \cdot 39}$.
13. Resolver la ecuación $x^2 + x + 1 \equiv 0 \pmod{7^2 \cdot 19}$.
14. Encontrar una unidad primitiva módulo 7, 19, y 83.
15. Si a es una raíz 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 $f(n) \not\equiv 0 \pmod{p}$. Probar que existen infinitos primos p para los cuales la ecuación $f(x) \equiv 0 \pmod{p}$ tiene al menos una raíz.
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 la 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 la 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 continuación 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 positivo, 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. $\square$

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 búsqueda 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 raíces 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 raíces 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 más 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 raíces 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

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

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

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

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

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

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:

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

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:

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

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 ecuación 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 $a = 1$, $b = \pm K$, $c = \pm L$, y $d = \pm KL$, 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

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

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

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

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

$$\begin{aligned} \left(\frac{181}{211}\right) &= \left(\frac{211}{181}\right) = \left(\frac{30}{181}\right) = \left(\frac{2}{181}\right) \left(\frac{3}{181}\right) \left(\frac{5}{181}\right) = \\ &= -\left(\frac{3}{181}\right) \left(\frac{5}{181}\right) = -\left(\frac{181}{3}\right) \left(\frac{181}{5}\right) = -\left(\frac{1}{3}\right) \left(\frac{1}{5}\right) = -1. \end{aligned}$$

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. $\square$

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

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

$\square$

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:

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

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

Desde aquí, el resultado se concluye utilizando las mismas congruencias de antes. $\square$

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 $(\frac{541}{653})$. Por la ley de reciprocidad, se tiene

$$\begin{aligned} \left(\frac{541}{727}\right) &= \left(\frac{727}{541}\right) = \left(\frac{186}{541}\right) = \left(\frac{2}{541}\right) \left(\frac{93}{181}\right) = - \left(\frac{93}{181}\right) = \\ &- \left(\frac{181}{93}\right) = - \left(\frac{-5}{93}\right) = - \left(\frac{-1}{93}\right) \left(\frac{5}{93}\right) = -(1) \left(\frac{93}{5}\right) = - \left(\frac{3}{5}\right) = 1. \end{aligned}$$

Una precaución, sin embargo, es importante. Si n no es un número primo, el número $(\frac{m}{n})$ 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 $(\frac{3}{35}) = (\frac{3}{5}) (\frac{3}{7}) = (-1)^2 = 1$.

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 $(\frac{495}{177})$, $(\frac{877}{895})$ y $(\frac{3072}{4061})$.

6. Determine si 148 es o no un cuadrado módulo $10379 = 97 \times 107$. 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 explícito 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 $a_0, a_1, \dots, a_n \in C$. Para ciertos fines, es conveniente agregar algunos coeficientes nulos al final de la expresión anterior. Por convención, esto no tiene ningún efecto en 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 $c_t = \sum_{k=0}^t a_k b_{t-k}$. 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 $\phi : C \rightarrow B$ 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 $\tilde{\phi}_a : C[x] \rightarrow B$ 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 $\tilde{\phi}_a : C[x] \rightarrow B$ que lleva a x en a y cuya restricción a C es la identidad.*

En este último caso, la imagen $\tilde{\phi}_a(f(x))$ 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 $\phi : C \rightarrow B$ un homomorfismo. Si $a_1, \dots, a_n$ son elementos arbitrarios de B , entonces existe una función*

$$\tilde{\phi} : C[x_1, \dots, x_n] \rightarrow B$$

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 $f, g \in \mathbb{Z}[x_1, \dots, x_n]$ del tipo $f(a_1, \dots, a_n) = g(a_1, \dots, a_n)$ 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 $M_n(C)$ 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 $\phi_a : C[x] \rightarrow B$. 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 $a_1, \dots, a_n$ son elementos de B , el anillo $C[a_1, \dots, a_n]$ es la imagen del homomorfismo evaluación $\phi_{a_1, \dots, a_n}$ y se tiene $C[a_1, \dots, a_n] \cong C[x_1, \dots, x_n]/\ker(\phi_{a_1, \dots, a_n})$.

Ejemplo 4.5. Si $a_1, \dots, a_n$ no satisfacen ninguna ecuación con coeficientes en C , el homomorfismo evaluación $\phi_{a_1, \dots, a_n}$ es inyectivo y en tal caso se dice que $a_1, \dots, a_n$ 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 $e = 2, 7172 \dots$ 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 $\pi = 3, 14159 \dots$ es un ejemplo de número trascendente sobre $\mathbb{Z}$ o $\mathbb{Q}$.

4.2 El algoritmo de la división

En esta sección introduciremos algunas herramientas que resultan cruciales en la demostración de los ejemplos mostrados en la sección anterior. Recuerdese 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 $f(x) = x^n + \dots$, donde los puntos representan términos de grado menor, y $g(x) = ax^m + \dots$. Entonces $f(x)g(x) = ax^{n+m} + \dots$, de donde se sigue el resultado. $\square$

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 $h(x) = ax^n + \dots$, 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 $r(u) = h_1(u) = h(u)$. $\square$

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 $h(x) \in C[x]$ 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

$f(x)(q(x) - q'(x)) = r'(x) - r(x)$. 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. Concluimos que $q(x) = q'(x)$. $\square$

Ejemplo 4.9. El número complejo i satisface la ecuación polinómica $x^2 + 1 = 0$. 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 en la forma $a + bi$ con a y b enteros.

Ejemplo 4.10. El número irracional $\sqrt{2}$ satisface la ecuación polinómica $x^2 - 2 = 0$. 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 $f(x) = a_n x^n + \dots + a_0$, se deduce desarrollando $2^n f(\frac{1}{2})$ 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 $f(x) = a_d x^d + \dots$ 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 $h(x) = bx^m + \dots$, 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

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

Supongamos que $q_0(x) \neq q(x)$. Sea $q_0(x) - q(x) = bx^r + \dots$, con la convención usual. El término de mayor grado en $[q_0(x) - q(x)]f(x)$ 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. $\square$

Ejemplo 4.13. El conjunto $\{0, 1\}$ es un conjunto de representantes 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 $n + \bar{x}^{i_1} + \dots + \bar{x}^{i_s}$ con $n \in \mathbb{Z}$ y enteros positivos $i_1, \dots, i_s$ 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 $(n, F(x))$ en los que la imagen de n en $\mathbb{Z}/2\mathbb{Z}$ es $F(0)$. Para comprobar esto basta considerar el homomorfismo

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

que envía a $f(x)$ en $(f(0), \overline{f(x)})$, 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 $(n, F(x))$ se utiliza un polinomio de la forma $n + x^{i_1} + \dots + x^{i_s}$, donde $F(x) = \bar{n} + \bar{x}^{i_1} + \dots + \bar{x}^{i_s}$. 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, utilizamos 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 $n + \bar{x}^{i_1} + \dots + \bar{x}^{i_s}$ con $n \in \mathbb{Z}$ $i_1, \dots, i_s$ enteros positivos diferentes. En este caso, el mismo razonamiento del ejemplo precedente nos da una representación del tipo

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

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

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

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 converso 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. $\square$

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 $D[x]$. $\square$

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 $K[x]$. $\square$

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, cambiando 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. $\square$

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

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

Un resultado relacionado al lema de Gauss que también utilizaremos bastante en lo que sigue es el siguiente:

Proposición 4.22. (Criterio de irreducibilidad de Eisenstein). Sea C un anillo conmutativo, $u \in C$ un elemento arbitrario, $p \in C$ un elemento primo y $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ un polinomio que satisfice lo siguiente:

1. El cociente $\bar{f}$ módulo p es de la forma $\bar{a}_n(x - \bar{u})^n \neq \bar{0}$.
2. p^2 no divide a $f(u)$.

Entonces $f(x) \in C[x]$ no puede escribirse como el producto de dos polinomios no constantes. En particular, si f es primitivo, entonces es irreducible.

Demostración. Remplazando $f(x)$ por $f(x+u)$ de ser necesario, podemos asumir que u es 0. Asumamos la existencia de una factorización no trivial $f(x) = g(x)h(x)$. Reduciendo módulo p obtenemos $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$. Nótese que $\bar{f}$ es un monomio, y, sobre un dominio de integridad, un monomio no puede factorizarse en polinomios que no sean monomios. Dejamos los detalles al lector. Escribiendo $g(x) = \bar{b}x^m$ y $h(x) = \bar{c}x^s$, es claro que debe tenerse $m + s = n$. Como $m \leq \deg(g)$ y $s \leq \deg(h)$, debe tenerse igualdad en ambos casos. En particular $m, s \geq 1$. Escribiendo $g(x) = bx^m + pg_1(x)$ y $h(x) = cx^s + ph_1(x)$, se obtiene, $f(0) = p^2 g_1(0)h_1(0)$, una contradicción. $\square$

Ejemplo 4.23. El polinomio $\Phi_p(x) = 1 + x + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}$ es irreducible, ya que

$$\bar{\Phi}_p(x) = \frac{x^p - \bar{1}}{x - \bar{1}} = \frac{(x - \bar{1})^p}{x - \bar{1}} = (x - \bar{1})^{p-1},$$

mientras que $\Phi_p(1) = p$.

4.4 Cocientes de $\mathbb{Z}[x]$ y $\mathbb{Z}[\alpha]$

En esta sección introduciremos algunas técnicas que nos permitirán estudiar anillos de la forma $\mathbb{Z}[\alpha]$, donde α es un número complejo. En particular, estudiaremos algunas técnicas para estudiar cocientes de este anillo. Muchos elementos de un anillo pueden estudiarse vía cocientes. Las unidades u de un anillo C se caracterizan por la propiedad $C/(c) \cong \{0\}$. Los primos se caracterizan por la propiedad de que el cociente es un dominio. Ideales comaximales pueden caracterizarse via el Teorema Chino de los Restos. En los cálculos que siguen, utilizaremos a menudo los teoremas de isomorfía como herramienta de cálculo, en particular el segundo. Según este teorema, si tenemos dos ideales $I \subseteq J$ en un anillo conmutativo C , existe un isomorfismo natural

$$\phi : C/J \xrightarrow{\cong} (C/I) / (J/I).$$

Veremos como este resultado permite calcular cocientes en los ejemplos que siguen. El truco común a todos ellos es la interpretación de los cocientes intermedios como un anillo de la forma $\mathbb{Z}[\alpha]$.

Ejemplo 4.24. El cociente $\mathbb{Z}[x]/(2, x)$ es isomorfo al cuerpo con dos elementos $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. De hecho, como $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, se tiene

$$\mathbb{Z}[x]/(2, x) \cong \left(\mathbb{Z}[x]/(x) \right) / \left((2, x)/(x) \right) \cong \mathbb{Z}/(2) = \mathbb{F}_2.$$

Se sigue que $(2, x)$ es un ideal maximal del anillo $\mathbb{Z}[x]$.

Ejemplo 4.25. El cociente $\mathbb{Z}[x]/(2x+1, x+2)$ se calcula observando que $\mathbb{Z}[x]/(x+2)$ es isomorfo a $\mathbb{Z}$ mediante el homomorfismo de evaluación en -2 .

$$\begin{aligned} \mathbb{Z}[x]/(2x+1, x+2) &\cong \left(\mathbb{Z}[x]/(x+2) \right) / \left((2x+1, x+2)/(x+2) \right) \\ &\cong \mathbb{Z} / \left(2(-2) + 1, (-2) + 2 \right) = \mathbb{Z}/(-3, 0) = \mathbb{F}_3. \end{aligned}$$

Concluimos que $(2x+1, x+2)$ es un ideal maximal. En este ejemplo se aprecia más claramente el paso de la identificación de un ideal con su imagen en el anillo cociente, lo que resulta crítico para cálculos de este tipo.

Nótese que si $\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(f(x))$, el método anterior nos permite, en ocasiones, calcular cocientes en anillos de la forma $\mathbb{Z}[\alpha]$. Ilustraremos esto en los siguientes ejemplos.

Ejemplo 4.26. Calcularemos para que primos $p \in \mathbb{Z}$, el ideal principal (p) es primo en $\mathbb{Z}[i]$. Para ello observamos que $\mathbb{Z}[i]$ se identifica con el cociente $\mathbb{Z}[x]/(x^2 + 1)$. Luego

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[x]/(p, x^2 + 1) \cong \mathbb{F}_p[x]/(x^2 + 1).$$

Se concluye que (p) es primo en $\mathbb{Z}[i]$ si y sólo si $(x^2 + 1)$ es primo en $\mathbb{F}_p[x]$. Veamos que este es el caso si y sólo si -1 no es un cuadrado módulo p . Para esto utilizamos el hecho de que $\mathbb{F}_p[x]$ es un dominio euclideo. En particular, todo polinomio de este anillo es primo si y sólo si es irreducible, lo que para un polinomio cuadrático es equivalente a no tener raíces. Por otro lado, los resultados del Capítulo 3 nos dicen que -1 es un cuadrado módulo p si y sólo si p es congruente a 1 módulo 4. Se sigue que 3, 7 y 11 son primos en $\mathbb{Z}[i]$, mientras que 5 y 13 no lo son. Veremos en el próximo capítulo que $\mathbb{Z}[i]$ es un dominio euclideo, por lo que 5 y 13, así como cualquier otro primo de la forma $4k + 1$, deben ser, de hecho, reducibles. Esto se comprueba fácilmente en casos particulares. Obsérvese que $5 = (2 + i)(2 - i)$ y $13 = (3 + 2i)(3 - 2i)$.

Ejemplo 4.27. Calcularemos el cociente $\mathbb{Z}[i]/(1 + i)$. Primero observamos que una preimagen bajo la evaluación en i de $1 + i$ es el polinomio $1 + x$, por lo que al identificar $\mathbb{Z}[i]$ con $\mathbb{Z}[x]/(1 + x^2)$ se tiene el isomorfismo $\mathbb{Z}[i]/(1 + i) \cong \mathbb{Z}[x]/(1 + x, x^2 + 1)$. Cocientando ahora por $(1 + x)$, es decir evaluando en -1 , se tiene que la imagen de $x^2 + 1$ es 2, y por lo tanto $\mathbb{Z}[x]/(1 + x, x^2 + 1) \cong \mathbb{Z}/(2) = \mathbb{F}_2$. Se concluye que $\mathbb{Z}[i]/(1 + i) \cong \mathbb{F}_2$. En particular, esto demuestra que el ideal principal $(1 + i)$ es maximal en el anillo $\mathbb{Z}[i]$, y que el elemento $1 + i$ es primo.

Dos ideales I y J se dicen comaximales si $I + J = C$. La importancia de este concepto radica en que el Teorema Chino de los restos se extiende a ideales comaximales cualesquiera.

Proposición 4.28. Teorema Chino de los restos, versión general
Sean J e I dos ideales comaximales en un anillo conmutativo C . Entonces se cumplen las identidades $IJ = I \cap J$ y $C/IJ \cong (C/I) \times (C/J)$.

Demostración. Si $I + J = C$, existen elementos $a \in I$ y $b \in J$ tales que $a + b = 1$. Es claro que $IJ \subseteq I \cap J$. Para probar la contención opuesta observamos que $c \in I \cap J$ implica $c = c \cdot 1 = ca + cb$, y cada sumando puede interpretarse como el producto de un elemento en I con uno en J .

Para la segunda afirmación escribimos $\bar{a}$ y $\bar{b}$ para las imágenes de a y b en $R = C/IJ$. Nótese que $\bar{a}\bar{b} = \bar{0}$, dado que el producto está contenido en IJ . Además $\bar{a} = \bar{a} \cdot \bar{1} = \bar{a}(\bar{a} + \bar{b}) = \bar{a}^2$, por lo que $\bar{a}$ y $\bar{b}$ son idempotentes complementarios del anillo R . Se sigue que $R \cong R/(\bar{a}) \times R/(\bar{b})$. Afirmamos que $(\bar{a}) = \bar{I} := I/IJ$ y $(\bar{b}) = \bar{J} := J/IJ$. De la afirmación se deduce $R/(\bar{a}) \cong (C/IJ)/(I/IJ) \cong C/I$, y lo mismo se aplica al segundo factor. Por simetría, es suficiente probar la afirmación para a . Para comprobar esta afirmación, necesitamos probar que $\bar{I} \subseteq (\bar{a})$, pues la converso es inmediata. Sea $\bar{c}$ un elemento de $\bar{I}$, digamos la imagen de cierto elemento $c \in I$. Entonces $\bar{c} = \bar{c} \cdot \bar{1} = \bar{c}(\bar{a} + \bar{b}) = \bar{c}\bar{a}$, dado que, como antes $\bar{c}\bar{b} = \bar{0}$. De aquí se sigue el resultado. $\square$

Ejemplo 4.29. Los ideales $(2, x)$ y $(3, x)$ en $\mathbb{Z}[x]$ son comaximales. Luego

$$\mathbb{Z}[x]/(2, x) \times \mathbb{Z}[x]/(3, x) \cong \mathbb{Z}[x]/((2, x) \cap (3, x)) = \mathbb{Z}[x]/(6, x). \quad (4.2)$$

Nótese que $(2, x)(3, x) = (6, 2x, 3x, x^2) = (6, x)$, ya que $x = 3x - 2x$. Como $\mathbb{Z}[x]/(n, x) \cong \mathbb{Z}/n\mathbb{Z}$, el isomorfismo en (4.2) es el ya conocido isomorfismo $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Ejemplo 4.30. Los ideales (2) y (x) en $\mathbb{Z}[x]$ no son comaximales, aún cuando 2 y x no tienen factores comunes, de hecho son ambos primos. En particular, esto prueba que $\mathbb{Z}[x]$ no es un DIP. De hecho $\mathbb{Z}[x]/(2, x) \cong \mathbb{F}_2$ como se vió en un ejemplo precedente. La imagen del homomorfismo canónico

$$\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[x]/(2) \times \mathbb{Z}[x]/(x) \cong \mathbb{F}_2[x] \times \mathbb{Z},$$

no contiene al elemento $(1 + (2), 2 + (x))$, pues si así fuese tendríamos

$$(g + (2), g + (x)) = (1 + (2), 2 + (x)),$$

de donde $g = 1 + 2r$ y $g = 2 + xs$, es decir $1 = 2r - xs$, por lo que evaluando en 0 se tendría la contradicción $1 = 2r(0)$.

Ejemplo 4.31. En el siguiente ejemplo calcularemos un cociente en el anillo $\mathbb{Z}[1/2] \cong \mathbb{Z}[x]/(2x - 1)$. De hecho, calcularemos el cociente $\mathbb{Z}[1/2]/(5)$. Para esto reescribimos como sigue:

$$\mathbb{Z}[1/2]/(5) \cong \mathbb{Z}[x]/(5, 2x - 1) \cong \mathbb{F}_5[x]/(2x - 1) \cong \mathbb{F}_5,$$

ya que el elemento 2 es invertible en $\mathbb{F}_5$.

Este ejemplo nos ilustra el hecho de que la operación de agregar inversos (o localizar) conmuta con la operación de calcular un cociente. Este es un resultado muy importante en la teoría de anillos conmutativos y justifica el hecho de que los inversos módulo n se comportan de manera muy similar a los inversos racionales, como se mencionó en el Capítulo 2. De hecho, en el ejemplo anterior, $1/2 \equiv 3 \pmod{5}$, pues

$$\frac{1}{2} - 3 = \frac{-5}{2}$$

y por esta razón el inverso de 2 módulo 5 es 3, pero esta última relación es válida ya en $\mathbb{Z}$. El siguiente ejemplo nos muestra como las propiedades de las localizaciones simplifican el cálculo de cocientes:

Ejemplo 4.32. Sea ρ una raíz del polinomio ciclotómico

$$\Phi_5(x) = 1 + x + x^2 + x^3 + x^4 = \frac{x^5 - 1}{x - 1}.$$

No es difícil comprobar que este polinomio es irreducible utilizando el criterio de Eisenstein. Vamos a verificar si el elemento $\rho^2 - 2$ es o no un primo. Para ello observamos que

$$\mathbb{Z}[\rho]/(\rho^2 - 2) \cong \mathbb{Z}[x]/(x^2 - 2, \Phi_5(x)) \cong \mathbb{Z}[\sqrt{2}]/(\Phi_5(\sqrt{2})).$$

Un cálculo nos proporciona $\Phi_5(\sqrt{2}) = 7 + 3\sqrt{2}$. Se sigue que

$$\begin{aligned} \mathbb{Z}[\rho]/(\rho^2 - 2) &\cong \mathbb{Z}[\sqrt{2}]/(7 + 3\sqrt{2}) \cong \\ \mathbb{Z}[x]/(x^2 - 2, 7 + 3x) &\cong \mathbb{Z}[-7/3]/\left(\frac{31}{9}, 0\right), \end{aligned}$$

donde la última identidad se obtiene evaluando en $-7/3$, lo que nos da el isomorfismo $\mathbb{Z}[x]/(7 + 3x) \cong \mathbb{Z}[-7/3] = \mathbb{Z}[1/3]$. Concluimos que el cociente buscado se obtiene agregando un inverso de 3 a $\mathbb{F}_{31} = \mathbb{Z}/31\mathbb{Z}$. Esto último no afecta el cociente, pues 3 ya es invertible en ese cuerpo. Concluimos que $\mathbb{Z}[\rho]/(\rho^2 - 2) \cong \mathbb{F}_{31}$ y por lo tanto $\rho^2 - 2$ es, efectivamente, un primo en el anillo $\mathbb{Z}[\rho]$.

No es siempre el caso que la localización tenga un efecto nulo en el cociente. Por ejemplo si agregamos un inverso de 3 al anillo $\mathbb{Z}/6\mathbb{Z}$, teremos

el cociente $\mathbb{Z}[1/3]/6\mathbb{Z}[1/3]$. Como 3 es invertible en este anillo, el cociente precedente coincide con $\mathbb{Z}[1/3]/2\mathbb{Z}[1/3]$, que es isomorfo al cuerpo $\mathbb{F}_2$. Concluimos que parte de la estructura del anillo cociente desaparece durante la localización. Esto sucede en cualquier anillo conmutativo cuando se agregan inversos de elementos que son divisores de 0.

Ejemplo 4.33. En este ejemplo mostramos que existen números algebraicos α para los cuales el anillo $\mathbb{Z}[\alpha]$ no es un dominio factorial, es decir no todo elemento de $\mathbb{Z}[\alpha]$ puede escribirse como un producto de primos. De hecho, 3 no es primo en el anillo $\mathbb{Z}[\sqrt{-5}]$, puesto que

$$\begin{aligned}\mathbb{Z}[\sqrt{-5}]/(3) &\cong \mathbb{Z}[x]/(3, x^2 + 5) \cong \mathbb{F}_3[x]/(x^2 + 5) \\ &= \mathbb{F}_3[x]/\left((x+1)(x+2)\right) \cong \mathbb{F}_3[x]/(x+1) \times \mathbb{F}_3[x]/(x+2) \cong \mathbb{F}_3 \times \mathbb{F}_3.\end{aligned}$$

Sin embargo 3 es irreducible en este anillo, dado que al tomar normas en la ecuación

$$(x + y\sqrt{-5})(w + z\sqrt{-5}) = 3$$

se obtiene

$$(x^2 + 5y^2)(w^2 + 5z^2) = 9.$$

Como $r^2 + 5s^2 = 3$ no tiene soluciones enteras, los dos factores de la izquierda deben ser 1 y 9. Si $x^2 + 5y^2 = (x + y\sqrt{-5})(x - y\sqrt{-5}) = 1$, entonces $x + y\sqrt{-5}$ es una unidad.

Si se quieren encontrar ideales maximales J e I cuya intersección, o producto, sea el ideal (3) , podemos considerar los núcleos de los homomorfismos que se obtienen proyectando el epimorfismo $\mathbb{Z}[\sqrt{-5}] \twoheadrightarrow \mathbb{F}_3 \times \mathbb{F}_3$ en cada uno de sus factores. Estos núcleos están generados por 3 y las imágenes de cada uno de los polinomios $x + 1$ y $x + 2$, es decir $I = (3, \sqrt{-5} + 1)$ y $J = (3, \sqrt{-5} + 2)$. Dejamos como ejercicio para el lector comprobar que estos ideales son realmente maximales, y que su producto es el ideal generado por 3.

4.5 Ejercicios

1. Calcule el inverso en $GL_2(\mathbb{Z}/128\mathbb{Z})$ de

$$\begin{pmatrix} 9 & 96 \\ 48 & 97 \end{pmatrix}.$$

2. Probar que en el anillo $\mathbb{Z}/27\mathbb{Z}[x]$, el polinomio $1 + 3x + 9x^2$ es invertible y calcule su inverso.
3. Encuentre el cociente y el resto de dividir $x^7 + x^2 + x$ por $x^3 + x + 1$.
4. Sea α una raíz del polinomio $x^5 + x + 1$. Utilizar el algoritmo de la división para encontrar un polinomio de grado no mayor a 4 tal que $f(\alpha) = \alpha^6 + \alpha^5 + \alpha$.
5. Encuentre un polinomio g de grado no mayor a 2 y un polinomio h cuyos coeficientes no nulos sean todos unos, tal que

$$(23x^6 + 17x^3 + x + 4) - g(x) + x^3h(x)$$

sea divisible por $2x^3 + 4x + 3$.

6. Sea $f(x) = a_nx^n + \cdots + a_1x + a_0$ un polinomio con coeficientes enteros. Probar que si

$$\frac{\mathbb{Z}[x]}{(f)} = \mathbb{Z} \oplus \bar{x}\mathbb{Z} \oplus \cdots \oplus \overline{x^{n-1}}\mathbb{Z},$$

entonces f es un polinomio mónico.

7. Probar que si a y b son relativamente primos, entonces $\mathbb{Z}[x]/(ax + b) \cong \mathbb{Z}[1/a]$.
8. Probar que $\mathbb{Z}[x]/(2x)$ es isomorfo al subanillo de $\mathbb{Z} \times \mathbb{F}_2[x]$ formado por aquellos pares $(n, f(x))$ que satisfacen $n \equiv f(0) \pmod{2}$.
9. Probar que un polinomio $f(x)$ con coeficientes enteros satisface $f(1/2) = 0$ si y sólo si es divisible por $2x + 1$.
10. Sea

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

Probar que cada clase en $\mathbb{Z}[x]/(f)$ tiene un único representante de la forma $r(x) + x^n g(x)$ donde r tiene grado a lo más $n - 1$ y g tiene coeficientes en $\{0, 1, 2, \dots, n - 1\}$.

11. Determine cuales de los siguientes pares de ideales en $\mathbb{Z}[x]$ son comaximales:

- (a) $(3x)$ y (2) .
 - (b) $(3x - 1)$ y $(3x - 2)$.
 - (c) $(3x - 1)$ y $(9x^2 + 1)$.
12. Determine cuales de los siguientes ideales del anillo $\mathbb{Z}[x]$ coinciden con el anillo completo:
- (a) $(x, 2)$.
 - (b) $(x^2, x + 1)$.
 - (c) $(x^2 - 1, x^2 + x + 1)$.
13. Determine cuantos elementos tiene el anillo cociente $\mathbb{Z}[x]/I$ en cada uno de los siguientes casos:
- (a) $I = (x, 2)$.
 - (b) $I = (x^3, x - 3)$.
 - (c) $I = (x^2 - 4, x^2 + x + 1)$.
14. Determine la estructura de los siguientes anillos:
- (a) $\mathbb{Z}[i]/(i - 3)$.
 - (b) $\mathbb{Z}[\sqrt{2}]/(\sqrt{2} - 3)$.
 - (c) $\mathbb{Z}[\sqrt[3]{2}]/(3)$.
 - (d) $\mathbb{Z}[\sqrt[3]{2}]/(3 - \sqrt[3]{2})$.
 - (e) $\mathbb{Z}[\sqrt[3]{2}]/(3 - \sqrt[3]{4})$.
 - (f) $\mathbb{Z}[\rho]/(\rho^2 - 2)$, donde $\rho = e^{2\pi i/5}$.
 - (g) $\mathbb{Z}[i]/(3)$.
15. Determine que primos enteros son primos en el anillo $\mathbb{Z}[\sqrt{7}]$.
16. Demuestre que existen infinitos primos enteros que son primos en $\mathbb{Z}[\sqrt{D}]$ para cada D entero.
17. Determine si 7, 13, y 19 son o no primos en el anillo $\mathbb{Z}[\sqrt[3]{2}]$.
18. Probar que ningún primo entero de la forma $3k + 2$ puede ser primo en el anillo $\mathbb{Z}[\sqrt[3]{2}]$.

19. Sea C un anillo conmutativo arbitrario. Sea $\wp$ un ideal arbitrario de C . Sea f un polinomio con coeficientes en C y sea

$$D = \frac{C[x]}{(f)}$$

el anillo que se obtiene al agregarle a C una raíz de f . Probar que el anillo obtenido al cocientar D por el ideal que genera $\wp$ es isomorfo al anillo obtenido al agregarle a $C/\wp$ una raíz de la reducción módulo $\wp$ de f .

20. Encuentre dos ideales primos I, J en $\mathbb{Z}[\sqrt{-5}]$ tales que $(7) = I \cap J = IJ$. Justifique.
21. Probar que los ideales $(x^4 + x^3 + x^2 + x + 1)$ y $(x^{11} - 6)$ no son comaximales.
22. Encuentre dos enteros n y m tales que

$$\mathbb{Z}[\sqrt[4]{11}]/(\sqrt{11} - 2) \cong \mathbb{Z}/(n) \times \mathbb{Z}/(m).$$

23. Determine si 93 es o no un primo en el anillo $\mathbb{Z}(\frac{\sqrt{11}}{3})$. Justifique.
24. Probar que $x^2 - m$ es irreducible en $\mathbb{Z}[x]$ para todo m que no es un cuadrado perfecto.
25. Probar que $x^n - p$ es irreducible en $\mathbb{Z}[x]$ para todo entero n y todo primo p .
26. Probar que $x^4 + x + 1$ es irreducible en $\mathbb{Z}[x]$ (sugerencia: probar módulo 2).

Chapter 5

Anillos de enteros

En los capítulos precedentes encontramos algunos anillos de la forma $\mathbb{Z}[\alpha]$ donde α satisfacía una única ecuación polinómica de la forma $f(\alpha) = 0$. Vimos que tal anillo puede identificarse con el cociente $\mathbb{Z}[x]/(f)$. Si el polinomio f es mónico, la estructura de este anillo es más sencilla, de hecho se tiene

$$\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\alpha^2 \oplus \cdots \oplus \mathbb{Z}\alpha^n.$$

Más generalmente, si masumimo sólomente que se satisface la identidad $f(\alpha) = 0$, el anillo $\mathbb{Z}[\alpha]$ es un cociente del anillo $\mathbb{Z}[x]/(f)$, por lo que al menos se tiene la relación

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 + \cdots + \mathbb{Z}\alpha^n.$$

Elementos de este tipo reciben el nombre de enteros algebraicos. En este capítulo estudiaremos con mas generalidad el concepto de elemento entero sobre un anillo y el concepto de extensión entera. Este puede verse como una versión para anillos del concepto de extensión algebraica.

5.1 Elementos enteros sobre un anillo

Sean $A \subseteq B$ anillos conmutativos. Un elemento b de B se dice entero sobre A si b es raíz de un polinomio mónico con coeficientes en A . Si $B \subseteq \mathbb{C}$, un elemento de B que es entero sobre $\mathbb{Z}$ se dice un entero algebraico.

Proposición 5.1. *Sean $A \subseteq B$ anillos conmutativos, y sea b un elemento de B . Si b satisface una ecuación del tipo $f(b) = 0$, donde $f(x) \in A[x]$ es un*

polinomio mónico de grado n , entonces $\{1, b, b^2, \dots, b^{n-1}\}$ genera $A[b]$ como A -módulo.

Demostración Si $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$, entonces $f(b) = 0$ implica $b^n = -\sum_{i=0}^{n-1} a_i b^i$. Si M es el A -módulo generado por $\{1, b, b^2, \dots, b^{n-1}\}$, entonces b^n pertenece a M . Multiplicando la identidad precedente por b^k se tiene $b^{n+k} = -\sum_{i=0}^{n-1} a_i b^{i+k}$, lo que permite probar por inducción que todas las potencias de b están en dicho módulo. Tenemos así las contenciones $M \subseteq A[b] \subseteq M$ y por lo tanto la igualdad. $\square$

Proposición 5.2. Sean $A \subseteq B$ anillos conmutativos, y sea b un elemento de B . Las siguientes afirmaciones son equivalentes:

1. b es entero sobre A .
2. $A[b]$ es un A -módulo finitamente generado.
3. Existe un A -módulo finitamente generado $N \subseteq B$ que contiene a A y tal que $bN \subseteq N$.

Demostración El resultado previo muestra que (1) implica (2). Es trivial que (2) implica (3). Finalmente, supongamos que se cumple (3). Sean $v_1, \dots, v_n$ generadores de N como A -módulo. Se sigue que para cada $i = 1, \dots, n$ se tiene $bv_i = \sum_{j=1}^n a_{i,j} v_j$. En particular se tiene la identidad matricial $(bI - M)V = 0$ donde I es la matriz identidad, M es la matriz $(a_{i,j})_{i,j}$ y V es el vector columna

$$V = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}.$$

Multiplicando por la adjunta clásica $(bI - M)^*$ se tiene $\det(bI - M)V = 0$. En particular, $\det(bI - M)$ anula a cualquier combinación lineal de los v_i 's. En particular a todo elemento de N . Como $1 \in A \subseteq N$, se tiene que $\det(bI - M) = 0$ y $f(x) = \det(xI - M)$ es un polinomio mónico que anula a b . $\square$

Si $A \subseteq B$ diremos que B es entero sobre A si cada elemento de B es entero sobre A . Se sigue del resultado anterior que si B es finitamente generado como

A -módulo, entonces es entero sobre A . En particular, si b es entero sobre A entonces $A[b]$ es entero sobre A . Mas generalmente, se tiene el siguiente resultado.

Proposición 5.3. *Sea $B = A[b_1, \dots, b_m]$, las siguientes afirmaciones son equivalentes:*

1. B es entero sobre A .
2. Cada b_i es entero sobre A .
3. B es finitamente generado como A módulo.

Demostración Es claro que (1) implica (2), y (3) implica (1) por lo dicho arriba. Probaremos que (2) implica (3). Asumamos que cada b_i es entero sobre A . En particular, existe algún polinomio mónico f_i que satisface $f_i(b_i) = 0$. Se sigue que existe un entero positivo N tal que para todo $n > N$ y para cada $i = 1, \dots, m$, tenemos una identidad de la forma $b_i^n = \sum_{j=0}^N a_{i,j}(n)b_i^j$, con $a_{i,j}(n) \in A$. De hecho basta tomar $N \geq \deg(f_i)$, para cada $i \in \{1, \dots, m\}$. Multiplicando estas expresiones se tiene que cada producto de la forma $b_1^{n_1} \dots b_m^{n_m}$ es una combinación lineal, con coeficientes en A , de los productos $b_1^{k_1} \dots b_m^{k_m}$ con $0 \leq k_i \leq N$, por lo que B es finitamente generado como A -módulo. $\square$

Corolario 5.3.1. *Si b_1 y b_2 son enteros sobre A , también lo son $b_1 - b_2$, $b_1 + b_2$, y $b_1 b_2$.*

Demostración Todos ellos son elementos de $A[b_1, b_2]$. $\square$

Corolario 5.3.2. *El conjunto de los elementos de B que son enteros sobre A es un subanillo B^{ent} de B .*

El anillo B^{ent} recibe el nombre de clausura entera de A en B . Si $A = B^{\text{ent}}$ se dice que A es integralmente cerrado en B . Si A es un dominio de integridad se dice que es integralmente cerrado (o normal) si es integralmente cerrado en su cuerpo de cocientes.

Ejemplo 5.4. Sea $A = K[x^2, x^3] \subseteq K[x]$, donde x es trascendente sobre el cuerpo K . Como x es raíz de la ecuación $T^2 - (x^2) = 0$, es entero sobre A . Por otro lado $x = \frac{x^3}{x^2}$, de donde x está en el cuerpo de cocientes de A , por lo que A no es normal.

Ejemplo 5.5. Sea $A = \mathbb{Z}[\sqrt{-3}]$. Como $\omega = \frac{-1+\sqrt{-3}}{2}$ es raíz de la unidad, es entero sobre $\mathbb{Z}$, y por lo tanto sobre A . Además ω está en el cuerpo de cocientes de A , pero no en A , por lo que A no es normal.

Proposición 5.6. Sean $A \subseteq B \subseteq C$ anillos conmutativos. Sea c un elemento de C . Si B es entero sobre A y c es entero sobre B , entonces c es entero sobre A .

Demostración Como c es entero sobre B , satisface una ecuación $c^n = \sum_{k=0}^{n-1} b_k c^k$. Sea $B' = B[b_0, \dots, b_{n-1}]$. Se sigue que c es entero sobre B' . En particular cada elemento de $B'[c]$ es de la forma $\sum_{i=0}^{n-1} \beta_i c^i$ con $\beta_i \in B'$. Como B' es finitamente generado como A -módulo, también lo es

$$B'[c] = B' + cB' + c^2B' + \dots + c^{n-1}B'.$$

El resultado sigue. $\square$

Corolario 5.6.1. Sean $A \subseteq B$ anillos conmutativos. El subanillo B^{ent} de B es integralmente cerrado en B .

Corolario 5.6.2. Sea A un dominio de integridad y B su cuerpo de cocientes. El subanillo $B^{\text{ent}} \subseteq B$ es normal.

Proposición 5.7. Todo DFU es normal.

Demostración Sea D un DFU y sea $\frac{m}{n}$ un elemento de su cuerpo de cocientes que es entero sobre D . Podemos suponer que n y m son relativamente primos. Si n es una unidad, no hay nada que demostrar. De otro modo, sea p un primo que divide a n , y por lo tanto no a m . Si tenemos una ecuación del tipo

$$\left(\frac{m}{n}\right)^k = \sum_{i=0}^{k-1} s_i \left(\frac{m}{n}\right)^i,$$

donde cada coeficiente s_i esté en el anillo D , podemos multiplicar esta identidad por n^k y obtener $m^k = \sum_{i=0}^{k-1} s_i m^i n^{k-i}$. En la última identidad, el primo p divide a cada término de la derecha, pero no divide al lado izquierdo. La contradicción termina la demostración. $\square$

Ejemplo 5.8. $\mathbb{Z}$ y $K[x_1, \dots, x_n]$ son normales.

Ejemplo 5.9. Para toda extensión algebraica $L/\mathbb{Q}$ el anillo $\mathcal{O}_L$, formado por todos los enteros algebraicos contenidos en L , es un dominio normal, dado que su cuerpo de cocientes está contenido en L y $\mathcal{O}_L$ es su propia clausura entera allí. Veremos en la próxima sección que los anillos de enteros no son siempre DFUs. En el próximo capítulo se demuestra que el cuerpo de cocientes de $\mathcal{O}_L$ coincide con L .

Los anillos de la forma $\mathcal{O}_L$, donde $L/\mathbb{Q}$ es una extensión finita, jugarán un papel central en todo lo que sigue. Estos anillos se llaman anillos completos de enteros. Cualquier anillo B con $\mathbb{Z} \subseteq B \subseteq \mathcal{O}_L$ recibe el nombre de anillo de enteros.

5.2 Enteros en cuerpos cuadráticos

En esta sección, calcularemos el anillo de enteros en un caso básico, aquel donde $L/\mathbb{Q}$ es una extensión cuadrática.

Proposición 5.10. Sea $L = \mathbb{Q}[\sqrt{d}]/\mathbb{Q}$ una extensión cuadrática, donde d es un entero libre de cuadrados. Entonces

$$\mathcal{O}_L = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod{4}, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Demostración Es claro que $\sqrt{d}$ es entero, por lo que $\mathbb{Z}(\sqrt{d}) \subseteq \mathcal{O}_L$. Sea $\alpha = a + b\sqrt{d}$ con a y b racionales. Si α es un entero algebraico, también lo es su conjugado $a - b\sqrt{d}$. En particular $2a$ y $2b\sqrt{d}$ son enteros. Así que también lo es $(2b\sqrt{d})^2 = (2b)^2d$, por lo que, siendo d libre de cuadrados, $2b$ debe ser un entero. Se sigue que podemos escoger enteros n y m tales que $a - n$ y $b - m$ sean 0 o $\frac{1}{2}$. Se sigue que $\alpha - (n + m\sqrt{d}) \in \{0, \frac{1}{2}, \frac{\sqrt{d}}{2}, \frac{1+\sqrt{d}}{2}\}$, por lo que basta con verificar cuales de estos elementos son enteros:

- Claramente $\frac{1}{2}$ no es entero.
- Tampoco lo es $\frac{\sqrt{d}}{2}$ ya que su cuadrado es $\frac{d}{4}$.
- El elemento $\frac{1+\sqrt{d}}{2}$ tiene el polinomio irreducible $x^2 - x + \frac{1-d}{4}$, por lo que es un entero precisamente cuando $d \equiv 1 \pmod{4}$.

El resultado es ahora inmediato, si observamos que $\sqrt{d} = 2 \left(\frac{1+\sqrt{d}}{2} \right) - 1 \in \mathbb{Z} \left[\frac{1+\sqrt{d}}{2} \right]$. $\square$

Ejemplo 5.11. If $L = \mathbb{Q}[\sqrt{2}]$, then $\mathcal{O}_L = \mathbb{Z}[\sqrt{2}]$.

Ejemplo 5.12. If $L = \mathbb{Q}[\sqrt{3}]$, then $\mathcal{O}_L = \mathbb{Z}[\sqrt{3}]$.

Ejemplo 5.13. If $L = \mathbb{Q}[i]$ con $i = \sqrt{-1}$, then $\mathcal{O}_L = \mathbb{Z}[i]$. Este recibe, usualmente, el nombre de Anillo de Enteros de Gauss.

Ejemplo 5.14. If $L = \mathbb{Q}[\sqrt{5}]$, then $\mathcal{O}_L = \mathbb{Z} \left[\frac{1+\sqrt{5}}{2} \right]$. El generador $\frac{1+\sqrt{5}}{2}$ es raíz de la ecuación $x^2 - x - 1 = 0$ y juega un papel fundamental en el análisis de los números de Fibonacci.

Ejemplo 5.15. If $L = \mathbb{Q}[\sqrt{-3}]$, then $\mathcal{O}_L = \mathbb{Z} \left[\frac{1+\sqrt{-3}}{2} \right]$ es llamado el anillo de enteros de Eisenstein. Nótese que este anillo puede escribirse también $\mathbb{Z}[\omega]$, donde $\omega = \frac{1-\sqrt{-3}}{2}$ es una raíz cúbica primitiva de la unidad.

Ejemplo 5.16. El anillo $A = \mathbb{Z}[\sqrt{-5}]$ no es un DFU, y es normal, dado que $A = \mathcal{O}_L$ donde $L = \mathbb{Q}[\sqrt{-5}]$. Concluimos que existen dominios normales que no son DFUs.

El siguiente resultado resulta bastante útil en el estudio de algunos de estos cuerpos cuadráticos, por lo menos en el caso de las raíces negativas, a las que nos referiremos como extensiones cuadráticas complejas.

Proposición 5.17. Sea Γ el paralelogramo, en $\mathbb{C}$, de vértices $\{0, 1, \eta, \eta + 1\}$, donde η es un entero generando una extensión cuadrática compleja. Asuma que se cumple la condición siguiente:

“Todo punto al interior de Γ está a una distancia menor a 1 del conjunto de vértices de Γ .”

Entonces $\mathbb{Z}[\eta]$ es un DE.

Demostración. Para probar que un anillo es euclideano es suficiente exhibir un algoritmo de Euclides que, en este caso, es el valor absoluto complejo $g(a + bi) = ||a + bi|| = a^2 + b^2$. La condición de que η es un entero y genera una extensión cuadrática, nos dice que todo elemento $s \in \mathbb{Z}(\eta)$ se escribe de manera única como $s = a + b\eta$ con a y b enteros.

Sean $n, m \in \mathbb{Z}(\eta)$. El conjunto (m) de los múltiplos sm de m está generado, como $\mathbb{Z}$ -módulo, por la observación anterior, por los elementos m y $m\eta$. Este conjunto puede visualizarse como los vértice de una retícula infinita como la que se muestra en la Figura 5.1. Cada uno de los paralelogramos determi-

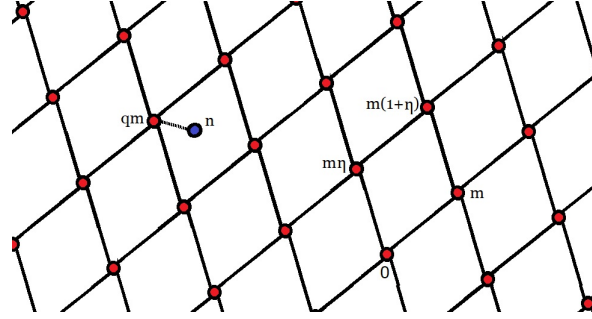


Figure 5.1: Un ideal principal como una retícula infinita.

nados por esta retícula es una imagen homotética del paralelogramo Γ . Girado en un ángulo α y con un factor de re-escalamiento r , donde $m = re^{i\alpha}$. Se sigue que n se encuentra al interior de uno de estos paralelogramos, por lo que existe un punto reticular qm que satisface la desigualdad $\|n - qm\| < \|m\|$. Definimos, por lo tanto $r = n - qm$ y se tiene $n = qm + r$ con $\|r\| < \|m\|$. $\square$

En las siguientes secciones nos concentraremos en los ejemplos más icónicos de anillos de enteros cuadráticos complejos. Ambos tienen numerosas aplicaciones a otras áreas de la matemática. Intentaremos ilustrar algunas en este capítulo. Dado que ambos son DEs, como se deduce de sencillos cálculos geométricos y de una aplicación directa de la proposición precedente.

5.3 Enteros de Gauss

El anillo $\mathbb{Z}[i]$, o anillo de enteros de Gauss, es el anillo de enteros algebraicos del cuerpo $\mathbb{Q}[i]$. Sus elementos son los complejos de la forma $a + bi$ con a y b enteros. Dado que la norma de este complejo está dado por $|a + bi|^2 = a^2 + b^2$, este anillo es particularmente útil para resolver ecuaciones diofánticas del tipo $x^2 + y^2 = a$ o $x^2 + y^2 = z^r$. Daremos algunos ejemplos en esta sección.

Proposición 5.18. $\mathbb{Z}[i]$ es un DE.

Demostración. Utilizaremos la proposición 5.17 con $\eta = i$. En este caso el paralelogramo Γ es un cuadrado de lado 1, cómo el que muestra la Figura 5.2. Basta ver que todo punto interior del cuadrado se encuentra a una distancia menor a uno de alguno de los vértices. De hecho, el punto interior que se encuentra más lejos de los vértices es el centro del cuadrado, y este está a distancia $\frac{\sqrt{2}}{2}$ de cada vértice. Hay varias maneras de probar esto.

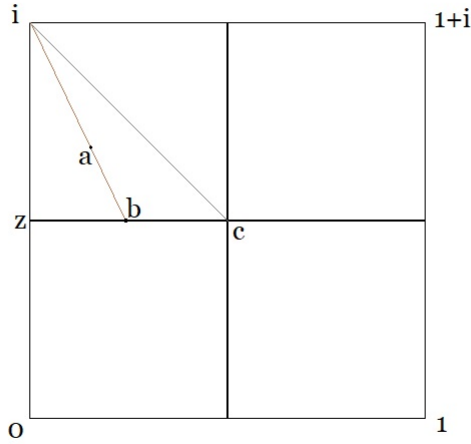


Figure 5.2: El cuadrado fundamental del anillo de Gauss

Una de ellas es dividir el cuadrado en 8 triángulos congruentes al triángulo $T_{i,z,c}$ de vértices i, z, c de la figura. Un punto interior cualquiera a de este último triángulo está mas cerca del vértice i que el punto b en el que la recta $L_{i,a} = \{it + (1-t)a | t \in \mathbb{R}\}$ corta a la recta $L_{z,c}$, definida análogamente. Del mismo modo, es claro que $|i - b|$ es mayor que $|i - c|$, dado que el triángulo $T_{i,b,c}$ es obtusángulo en b . El argumento para cualquiera de los otros ocho subtriángulos es similar. $\square$

Se sigue del resultado anterior que cada entero de Gauss es producto de

primos de manera única. En particular, los enteros en $\mathbb{Z}$, que en lo sucesivo serán denominados enteros racionales, son producto de primos de $\mathbb{Z}[i]$ de manera única. Como cada entero racional puede escribirse como producto de primos racionales de manera única, para hacer esta descomposición explícita, es suficiente con escribir cada primo racional como producto de enteros Gaussianos. Por ejemplo, si queremos escribir a 30 como un producto de primos en $\mathbb{Z}[i]$, basta con hacerlo para 2, 3 y 5. De hecho $2 = (-i)(1+i)^2$, $5 = (1+2i)(1-2i)$ mientras que 3 es primo. Para ver directamente que cada uno de los elementos mencionados es primo se pueden realizar los cálculos siguientes:

- El entero 3 es un primo ya que

$$\mathbb{Z}[i]/(3) \cong \mathbb{Z}[x]/(3, x^2 + 1) \cong \mathbb{F}_3[x]/(x^2 + 1),$$

y el polinomio $x^2 + 1$ no tiene raíces en $\mathbb{F}_3$.

- $1 + i$ es primo, ya que

$$\begin{aligned} \mathbb{Z}[i]/(1+i) &= \mathbb{Z}[i]/(2, 1+i) \cong \mathbb{Z}[x]/(2, 1+x, x^2+1) \\ &\cong \mathbb{F}_2[x]/(1+x, x^2+1) = \mathbb{F}_2[x]/(1+x) \cong \mathbb{F}_2. \end{aligned}$$

- $1 + 2i$ es primo, ya que

$$\begin{aligned} \mathbb{Z}[i]/(1+2i) &= \mathbb{Z}[i]/(5, 1+2i) \cong \mathbb{Z}[x]/(5, 1+2x, x^2+1) \\ &\cong \mathbb{F}_5[x]/(1+2x, x^2+1) = \mathbb{F}_5[x]/(1+2x) \cong \mathbb{F}_5. \end{aligned}$$

- $1 - 2i$ es primo, ya que

$$\begin{aligned} \mathbb{Z}[i]/(1-2i) &= \mathbb{Z}[i]/(5, 1-2i) \cong \mathbb{Z}[x]/(5, 1-2x, x^2+1) \\ &\cong \mathbb{F}_5[x]/(1-2x, x^2+1) = \mathbb{F}_5[x]/(1-2x) \cong \mathbb{F}_5. \end{aligned}$$

Sin embargo, el hecho de que $\mathbb{Z}$ es un DE nos entrega una alternativa más simple. Si $c = ab$ donde a , b , y c son enteros gaussianos, entonces sus valores absolutos satisfacen la relación $|c| = |a| \cdot |b|$. Además, los cuadrados de los valores absolutos de los enteros de Gauss son siempre enteros. Se sigue que, si c es un entero de Gauss para el cual $|c|^2$ es un primo, entonces c es irreducible. Como $\mathbb{Z}[i]$ es un DE, cada elemento irreducible allí es un primo. Concluimos

así que $1+i$, $1+2i$ y $1-2i$ son primos, pues $|1+i|^2 = 2$ y $|1+2i|^2 = |1-2i|^2 = 5$. Por otro lado, si algún primo p no es suma de cuadrados, no puede escribirse $p = ab$, con $a, b \in \mathbb{Z}[i]$ y ninguno de ellos unidad. Esto es porque $|p|^2 = p^2$, de modo que, al no haber enteros de Gauss de valor absoluto $\sqrt{p}$, algunos de estos enteros, a o b , debe tener largo uno, por lo que debe estar en el conjunto $\{1, -1, i, -i\} = \mathbb{Z}[i]^*$. Se sigue que p es irreducible, y por lo tanto primo en $\mathbb{Z}[i]$. Esto se aplica, por ejemplo a $p = 3$. Concluimos que la factorización en primos de 30 es

$$30 = (-i) \cdot 3 \cdot (1+i)^2 \cdot (1+2i) \cdot (1-2i).$$

Proposición 5.19. *Un primo racional es un primo en $\mathbb{Z}[i]$ si y sólo si es de la forma $4k-1$. Todo primo en $\mathbb{Z}[i]$ es divisor de algún primo racional.*

Demostración. La primera afirmación se demuestra mediante un cálculo directo del cociente. De hecho se tiene

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[x]/(p, x^2 + 1) \cong \mathbb{F}_p[x]/(x^2 + 1),$$

y el polinomio $x^2 + 1$ tiene raíces en $\mathbb{F}_p$ si y sólo si -1 es un cuadrado módulo p . Si p es impar, esto es equivalente a que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$, como se vió en el capítulo 3. El primo $p = 2$ ya se factorizó arriba. Para la segunda afirmación, basta ver que todo primo π del anillo de Gauss divide al entero $|\pi|^2 = \pi\bar{\pi}$. Como este entero se escribe como un producto de primos racionales, el entero de Gauss π debe dividir a alguno de estos por definición de primo. $\square$

Corolario 5.19.1. *Todo primo racional de la forma $4k+1$ es suma de dos cuadrados de números enteros. Además esta expresión es única salvo el orden y el signo.*

Demostración. Se sigue del resultado anterior que todo primo p de la forma $p = 4k+1$ debe factorizarse en $\mathbb{Z}[i]$ en forma no trivial. Además, como $|p|^2 = p^2$, p sólo puede factorizarse como el producto $p = \pi_1\pi_2$ de dos primos de valor absoluto $\sqrt{p}$. Las propiedades de la notación polar compleja muestran que π_1 y π_2 deben ser complejos conjugados. Digamos $\pi_1 = \pi$ y $\pi_2 = \bar{\pi}$. Si escribimos $\pi = x + yi$, se tiene $p = x^2 + y^2$. Además, por la unicidad de la

descomposición en primos, las únicas alternativas son intercambiar π con su conjugado, por un elemento de la forma $u\pi$, donde $u \in \{1, -1, i, -i\}$ es una unidad, o una combinación de ambos. Esta elección dá todas las posibles permutaciones de x e y y de sus inversos, como lo demuestra una tediosa comprobación que se deja al lector. $\square$

Corolario 5.19.2. *Todo primo del anillo de Gauss es, un primo racional de la forma $4k - 1$, un primo de la forma $\pi = x + yi$, donde $x^2 + y^2$ es un primo racional de la forma $4k + 1$ o el primo $1 + i$.* $\square$

El siguiente resultado, el que es inmediato por las propiedades de la conjugación compleja, será útil en todo lo que sigue:

Lema 5.20. *Si z , u y w son enteros de Gauss que satisfacen $z = uw$, entonces $\bar{z} = \bar{u}\bar{w}$. En particular, si w divide a z , entonces $\bar{w}$ divide a $\bar{z}$.* $\square$

Lema 5.21. *Si $\pi = x + yi$, donde $x^2 + y^2$ es un primo racional de la forma $4k + 1$, entonces π y $\bar{\pi}$ son primos no asociados.*

Demostración. Las únicas unidades de $\mathbb{Z}[i]$ son los elementos del conjunto $\{1, -1, i, -i\}$. Se sigue que los únicos asociados de $\pi = x + yi$ son los elementos de

$$\{\pi, -\pi, i\pi, -i\pi\} = \{x + yi, -x - yi, y - xi, -y + xi\}.$$

Ninguno de estos coincide con $\bar{\pi}$, salvo que $xy = 0$ o que $x = \pm y$. La primera no es posible si $x^2 + y^2$ es primo. La segunda sólo es posible si $x = \pm 1$ y $x^2 + y^2 = 2$. $\square$

A partir de aquí, usaremos la notación $v_p(n)$ para la mayor potencia de un primo p que divide a un entero n . Es decir $t = v_p(n)$ significa que p^t divide a n y que p^{t+1} no divide a n .

Proposición 5.22. *El máximo común divisor entre los enteros de Gauss $\rho = a + bi$ y $\bar{\rho}$ es el máximo común divisor d de a y b , salvo cuando $v_2(a) = v_2(b)$, en cuyo caso es $d(1 + i)$.*

Demostración. Es claro que d divide a ρ y a $\bar{\rho}$. Reemplazando ρ por $\frac{\rho}{d}$, podemos suponer que $d = 1$, es decir que a y b son relativamente primos. En particular no pueden ser ambos pares. Supongamos que π es un primo que divide a ambos, π no puede ser un primo racional si $d = 1$, por lo que debe ser un primo de la forma $\pi = x + yi$, con $x^2 + y^2$ primo de la forma $4k + 1$, o bien $\pi = 1 + i$. En el primer caso, $\bar{\pi} = x - yi$ divide también a ρ y $\bar{\rho}$. Como π y $\bar{\pi}$ no son asociados, se sigue que el primo racional $|\pi|^2 = \pi\bar{\pi}$ divide a ρ , y por lo tanto también a a y b , contradiciendo la hipótesis de que $d = 1$. El entero de Gauss $(1 + i)^2 = 2i$ tampoco puede dividir a ρ y $\bar{\rho}$ si $d = 1$. Se concluye que el único posible divisor común es $1 + i$. Si $1 + i$ divide a ρ , también divide a $\bar{\rho}$, dado que $\overline{1 + i} = 1 - i = (-i)(1 + i)$. Basta, por lo tanto, determinar cuando $1 + i$ divide a ρ . Esto ocurre si

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

es un entero. Esto es equivalente a que a y b sean impares, dado que no son ambos pares. $\square$

El problema de los triángulos pitagóricos. Este problema consiste en encontrar todos los triángulos rectángulos que tienen coordenadas enteras, como el de la Figura 5.3. El teorema de pitágoras nos dice que el área del triángulo C de la figura es igual a la suma de las áreas de los triángulos A y B . Se sigue que los lados del triángulo deben ser soluciones enteras de la ecuación $a^2 + b^2 = c^2$. Diremos que un triángulo pitagórico es primitivo, si los enteros a , b y c no tienen divisores comunes. Como multiplicar los lados de cualquier triángulo pitagórico por un entero, o dividirlos por un divisor común, produce un nuevo triángulo pitagórico, es suficiente con encontrar los triángulos primitivos.

A fin de resolver este problema, utilizaremos la aritmética del anillo de Gauss. Re-escribimos la ecuación en la forma $(a + bi)(a - bi) = c^2$. En otras palabras, tenemos que la norma del entero de Gauss $z = a + bi$ es un cuadrado. Si escribimos la factorización prima $z = u\pi_1^{\alpha_1}\pi_2^{\alpha_2}\cdots\pi_N^{\alpha_N}$, vemos que ninguno de los π_i puede ser un primo racional, por la condición de que a y b sean relativamente primos. Del mismo modo, comparando la descomposición anterior con $\bar{z} = \bar{u}\bar{\pi}_1^{\alpha_1}\bar{\pi}_2^{\alpha_2}\cdots\bar{\pi}_N^{\alpha_N}$, Debemos concluir que los divisores primos de z no pueden incluir dos primos conjugados, y que el primo $1 + i$

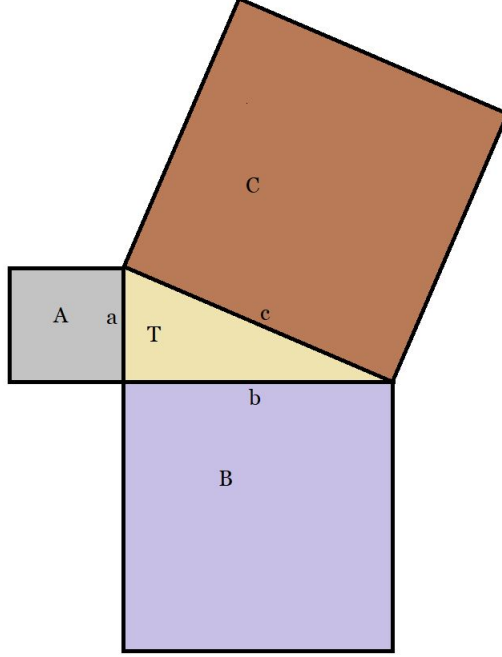


Figure 5.3: Un triángulo pitagórico.

no puede aparecer con una potencia que exceda 1. Multiplicando ambas factorizaciones se obtiene

$$c^2 = z\bar{z} = (\pi_1\bar{\pi}_1)^{\alpha_2}(\pi_1\bar{\pi}_2)^{\alpha_2} \cdots (\pi_N\bar{\pi}_N)^{\alpha_N},$$

donde hemos usado que $u\bar{u} = 1$ si u es una unidad. Cada uno de los productos $\pi_N\bar{\pi}_N$ es un primo racional. Se sigue que los exponentes α_i deben ser todos pares y que $1 + i$ no aparece en la descomposición. En particular, $z = uw^2$ donde u es unidad y w es un entero de Gauss. Cambiando el orden o los signos de x e y , podemos suponer que $u = 1$. En conclusión, se tiene

$$a + ib = z = w^2 = (c + di)^2 = (c^2 - d^2) + 2cdi.$$

Esto demuestra el siguiente resultado:

Proposición 5.23. *Los catetos de un triángulo pitagórico tienen lados de la forma $2cd$ y $c^2 - d^2$, donde c y d son enteros.* $\square$

Sumas de cuadrados. Supongamos que un entero n se escribe como suma de cuadrados, en la forma $x^2 + y^2 = n$. Razonando como antes, definimos $z = x + iy$, el cual es un entero de Gauss de norma n . Como antes, escribimos la factorización prima $z = u\pi_1^{\alpha_1}\pi_2^{\alpha_2}\cdots\pi_N^{\alpha_N}$, de la que se concluye que

$$n = |z|^2 = |\pi_1|^{\alpha_1}|\pi_2|^{\alpha_2}\cdots|\pi_N|^{\alpha_N}.$$

Cada factor $|\pi_i|$ es un primo o el cuadrado de un primo. Lo último sólo en el caso de que se trate de un primo de la forma $4k - 1$. Se sigue que para cada primo p , de la forma $4k - 1$, que divide a n , debemos tener que $v_p(n)$ es par. Por otro lado, cuando esta condición se cumple, podemos escoger primos del anillo de Gauss con el valor absoluto apropiado, en cada caso. Podemos, por lo tanto, concluir el siguiente resultado:

Proposición 5.24. *Un entero n puede escribirse como suma de dos cuadrados si y sólo si $v_p(n)$ es par para cada primo de la forma $4k - 1$ que divide a n .* $\square$

En general, la solución no es única, dado que es posible intercambiar $\pi = a + bi$ por su conjugado $a - bi$ para algunos de los primos de la forma $4k + 1$. La forma en que esto influye en las soluciones se ilustra en algunos de los ejemplos siguientes:

Ejemplo 5.25. La ecuación $x^2 + y^2 = 35 = 5 \times 7$ no tiene solución, ya que 7 es de la forma $4k - 1$, y el exponente correspondiente es impar.

Ejemplo 5.26. Para resolver la ecuación $x^2 + y^2 = 245 = 5 \times 7^2$ factorizamos como $(x + yi)(x - yi) = 5 \times 7^2$. Como 7 es de la forma $4k - 1$, debe ser un primo en $\mathbb{Z}[i]$. Se sigue que algún factor al lado izquierdo debe ser divisible por 7, y por lo tanto ambos, ya que son conjugados. Se sigue que $x + yi = 7(a + bi)$ donde $a^2 + b^2 = 5$. Una posible solución es $a = 2$, $b = 1$, lo que da $x + yi = 14 + 7i$. Obtenemos la solución $14^2 + 7^2 = 245$. En este caso la solución es única salvo orden o signo, ya que sólo hay un primo de la forma $4k + 1$.

Ejemplo 5.27. Para resolver la ecuación $x^2 + y^2 = 377 = 13 \times 29$, se debe encontrar un entero de Gauss de norma 13 y uno de norma 29 y multiplicarlos. Partimos de las soluciones $2^2 + 3^2 = 13$ y $5^2 + 2^2 = 29$, por lo que podemos tomar $x + yi = (2 + 3i)(5 + 2i) = 4 + 19i$, lo que da la solución $4^2 + 19^2 = 377$. Sin embargo, podemos tomar también $x + yi = (2 + 3i)(5 - 2i) = 16 + 11i$, lo que da la solución alternativa $16^2 + 11^2 = 377$.

Ejemplo 5.28. Para resolver la ecuación $x^2 + y^2 = 289 = 17^2$, se debe encontrar un entero de Gauss de norma 17 y elevarlo al cuadrado, o bien multiplicar dos primos distintos de esa norma. En el primer caso escribimos $x + yi = (4 + i)^2 = 15 + 8i$, lo que da la solución $15^2 + 8^2 = 289$. En el segundo caso tenemos $x + yi = (4 + i)(4 - i) = 17$. Esto da la solución $17^2 + 0^2 = 289$.

El ajedrez infinito. Una interpretación natural del anillo de enteros de Gauss es la del conjunto de casillas de un ajedrez infinito como el de la Figura 5.4. En este tablero interpretaremos cada casilla como un entero de Gauss,

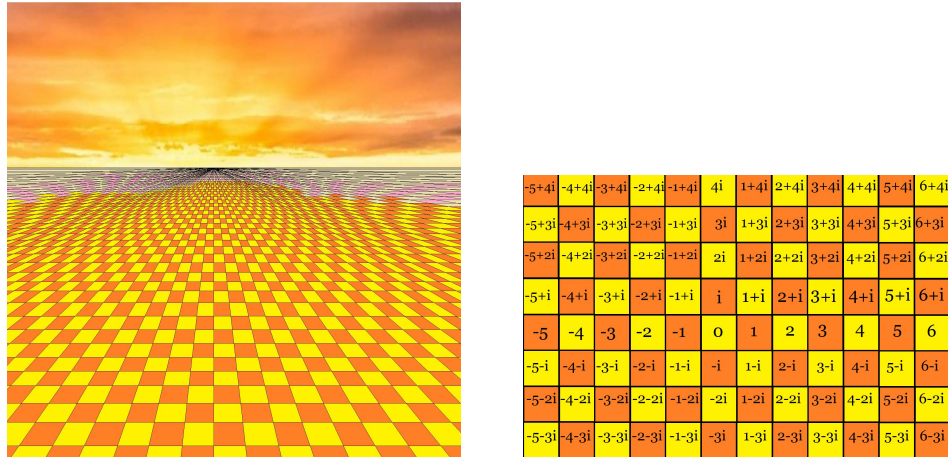


Figure 5.4: Un tablero de ajedrez infinito y su interpretación como el anillo de enteros de Gauss.

como se muestra a la derecha de la figura. Una pieza de ajedrez es un objeto que ocupa un casillero por vez y que puede desplazarse de un casillero a otro mediante un cierto conjunto de reglas que son invariantes bajo rotaciones. En otras palabras, si una pieza de ajedrez puede ir de una casilla x a una casilla y , entonces puede también ir de x a la casilla z que se obtiene de y mediante una rotación de 90, 180 o 270 grados centrado en x . El ejemplo más representativo de esta definición es el caballo. Nótese que los movimientos ilustrados en la figura 5.5 se obtienen unos de otros mediante una rotación del tipo ya mencionado. En otras palabras, si el caballo se encuentra en una posición dada x , entonces puede alcanzar las posiciones $x + a$, $x + ia$, $x - a$ y $x - ia$, donde, en este caso $a = 2 + i$. Se sigue por iteración que esta pieza puede

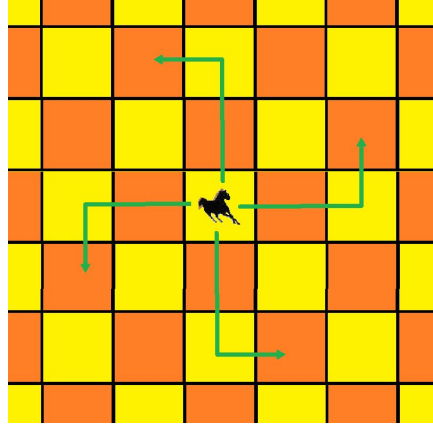


Figure 5.5: Movimientos del caballo zurdo.

alcanzar cualquier posición del tipo $x + za$, donde z es un entero de Gauss. Nótese que los movimientos aquí considerados incluyen sólo giros del caballo a la izquierda. Llamaremos caballo zurdo a la pieza de ajedrez que sólo puede realizar estos movimientos. El caballo del juego tradicional de ajedrez puede también realizar giros a la derecha, lo que equivale a desplazarse en múltiplos de $2 - i$. Dado que $2 + i$ y $2 - i$ son relativamente primos, se tiene la identidad entre ideales $(2 + i) + (2 - i) = (1)$, lo que nos dice que el caballo tradicional puede recorrer el tablero completo. En general, llamaremos (a, b) -caballo a una pieza de ajedrez que puede moverse utilizando múltiplos de un entero dado $a + bi$.

Ejemplo 5.29. El alfil es un $(1, 1)$ -caballo, es decir, puede recorrer todos los múltiplos de $1 + i$, los que corresponden exactamente a las casillas de un mismo color en el tablero infinito.

Ejemplo 5.30. El camello es, por definición, un $(3, 1)$ -caballo y un $(3, -1)$ -caballo, es decir, se mueve mediante múltiplos de $3 + i$ y $3 - i$. Dado que el máximo común divisor de estos dos enteros de Gauss es $1 + i$, concluimos que el camello puede recorrer todas las casillas de un color.

Ejemplo 5.31. Consideremos ahora una pieza que puede realizar dos tipos de movimiento. puede moverse tres casillas en una dirección, para luego girar a la izquierda y avanzar una casilla. Alternativamente puede desplazarse

cinco casillas en una dirección, para luego girar a la derecha y moverse dos casillas. Dada su naturaleza híbrida, llamaremos a esta pieza el hipogrifo (ver Figura 5.6). En este caso, un cálculo de máximo común vivior nos entrega

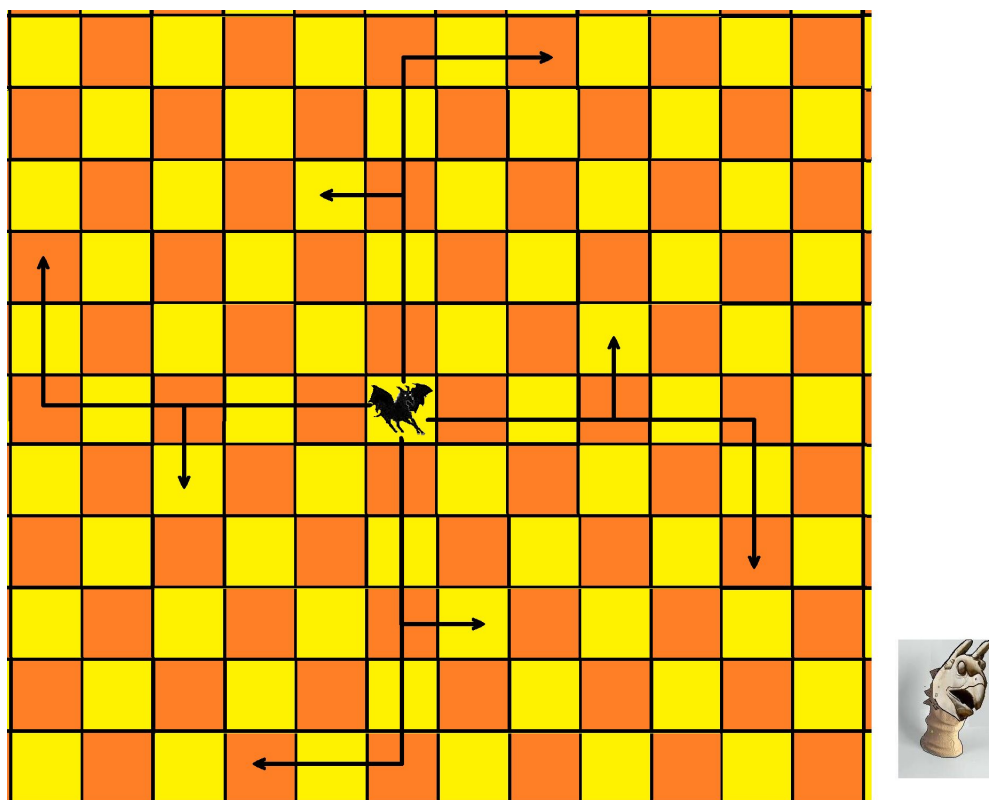


Figure 5.6: El hipogrifo.

$(3 + i) + (5 - 2i) = (2 - i)$. Concluimos que el hipogrifo recorre las mismas caillas que un caballo diestro.

Nótese que, de acuerdo a nestra definición general, los peones del ajedrez no se consideran piezas, ya que se mueven sólo en una dirección preferente. Ignoraremos aquí movimientos especiales como el que los peones hacen al comer, normalmente o al paso, o el salto inicial. En estas notas, un peón puede moverse en una única dirección, la que, por simplicidad, asumiremos que les permite pasar de una casilla dada x a la casilla $x + 1$. Un híbrido

peón pieza es un objeto que puede realizar movimientos de peón aparte de los inherentes a una pieza, digmos un (a, b) -caballo. A tal objeto le llamaremos un (a, b) -mestizo. Un problema natural pregunta bajo que condiciones puede un mestizo recorrer todo el tablero. Daremos dos soluciones de este problema. Una geométrico-combinatorial, que usa directamente los movimientos del mestizo, y otra algebraica, via teoría de ideales.

Proposición 5.32. *Un (a, b) -mestizo puede recorrer todo el tablero si y sólo si a y b son relativamente primos.*

Demostración. Asumiremos que a y b son positivos, por lo que moverse a unidades a la derecha y b hacia arriba nos deja en el primer cuadrante. Los casos restantes son similares, dado que todo entero de Gauss tiene una rotación que lo ubica en el primer cuadrante. Utilizando rotaciones en 90 y 180 grados en sentido levógiro de ese movimiento, es decir, multiplicandolo por i o -1 , es posible llevar el mestizo atras tan lejos como se quiera. En la Figura 5.7 asumimos que $a = 3$ y $b = 2$. Si se utiliza ta veces la primera

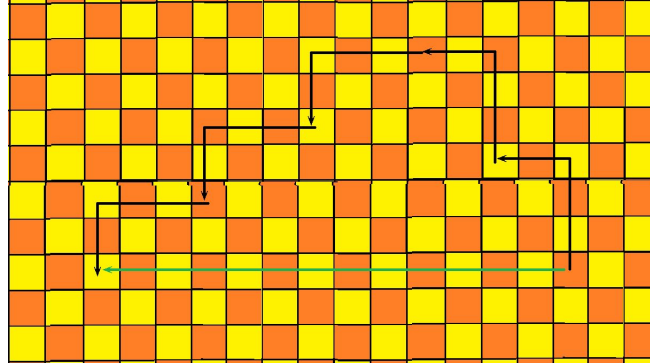


Figure 5.7: Un retroceso.

rotación y tb veces la segunda, el mestizo queda ubicado exáctamente atras de la casilla de partido, luego de lo cual se puede volver tanto como se quiera mediante movimientos de peón. Esto nos dice que el mestizo puede desplazarse arbitrariamente en una fila, por lo que basta probar que puede colocarse en cualquier fila. Ahora observamos que las cuatro rotaciones suman b , a , $-b$ y $-a$ al número de la fila, por lo que, para colocarse en la fila número n ,

es suficiente con escribir n como combinación lineal de a y b , lo que puede hacerse para un n arbitrario si y sólo si a y b son relativamente primos. $\square$

Para dar una demostración puramente algebraica necesitamos una afirmación equivalente. Observemos que un (a, b) -caballo puede, partiendo del origen, colocarse en cualquier casilla que corresponda a un múltiplo de $z = a + bi$. Es suficiente, por lo tanto, comprobar que los avances de peón nos permiten recorrer todas las clases de congruencia módulo z . Como un avance de peón consiste en sumar uno, esto equivale a que cada clase de congruencia sea la clase de un entero racional. En otras palabras, se tiene el resultado siguiente:

Proposición 5.33. *Un (a, b) -mestizo puede recorrer todo el tablero si y sólo si $\mathbb{Z}[i]/(a + bi) \cong \mathbb{Z}/n\mathbb{Z}$ para algún entero racional n .*

Se sigue que la afirmación sobre mestizos es equivalente al siguiente resultado:

Proposición 5.34. *Si $z = a + bi$ es un entero de Gauss, entonces existe un entero n tal que $\mathbb{Z}[i]/(z) \cong \mathbb{Z}/n\mathbb{Z}$ si y sólo si a y b son relativamente primos.*

Demostración. Sea $n = a^2 + b^2 = (a + bi)(a - bi)$ y sea $R = \mathbb{Z}/n\mathbb{Z}$. Un cálculo directo nos da lo siguiente:

$$\mathbb{Z}[i]/(z) = \mathbb{Z}[i]/(z, n) \cong \mathbb{Z}[x]/(a + bx, n, x^2 + 1) \cong R[x]/(a + bx, x^2 + 1).$$

Asumamos primero que a y b son relativamente primos, de modo que b sea relativamente primo con n . Sea k el inverso de b en R . En este caso se tiene lo siguiente:

$$R[x]/(a + bx, x^2 + 1) \cong R/\left((-ak)^2 + 1\right) \cong R.$$

En el primer paso se evalúa en $-ak$, que es la raíz de $a + bx$, y en el último se usa que $(-ak)^2 + 1 = k^2(a^2 + b^2) = 0$. En el caso general utilizamos el hecho de que cada elemento de $R[x]/(x^2 + 1)$ se escribe de manera única en la forma $c + dx$, dado que $x^2 + 1$ es mónico. Si d es el MCD de a y b , es fácil ver que todo múltiplo de $a + bx$ tiene un coeficiente en x divisible por d . Se concluye que, si $d > 1$, la clase de $x - r$ en el cociente $R[x]/(a + bx, x^2 + 1)$ no se anula para ningún entero r . Esto concluye la prueba. $\square$

La demostración vía ideales nos entrega fácilmente la siguiente versión del resultado original:

Proposición 5.35. *Si a y b son relativamente primo, $nn(a, b)$ -mestizo puede llegar a cualquier casilla del tablero utilizando menos de $a^2 + b^2$ movimientos de peón. Además, esta cota es optimal.* $\square$

5.4 Enteros de Eisenstein

Nuestro segundo ejemplo es el anillo $\mathbb{Z}[\omega]$, donde $\omega = \frac{-1+\sqrt{-3}}{2} = e^{2\pi i/3}$ es una raíz cúbica primitiva de la unidad. Este se conoce como el anillo de enteros de Eisenstein. Este anillo cumple un papel significativo en el estudio de ecuaciones diofánticas del tipo $x^3 + y^3 = a$. Nótese que el elemento ω es una raíz del polinomio

$$\frac{x^3 - 1}{x - 1} = x^2 + x + 1,$$

el que es un polinomio cuadrático, por lo que es anillo de Eisenstein es un anillo de enteros cuadráticos. Por otro lado, ω^2 es la otra raíz cúbica primitiva de la unidad, por lo que es el conjugado complejo de ω . Se sigue que

$$\overline{a_0 + a_1\omega} = a_0 + a_1\omega^2 = a_0 + a_1(-1 - \omega) = (a_0 - a_1) - a_1\omega,$$

y que

$$|a_0 + a_1\omega|^2 = (a_0 + a_1\omega)(a_0 + a_1\omega^2) = a_0^2 - a_0a_1 + a_1^2,$$

donde se usa el hecho de que $\omega^3 = 1$ y $\omega + \omega^2 = -1$.

Comenzaremos, como antes, comprobando que este anillo es un dominio euclideano. Este resultado tiene también una demostración geométrica.

Proposición 5.36. *El anillo $\mathbb{Z}[\omega]$ es un DE.*

Demostración. Como antes, utilizamos la proposición 5.17, esta vez con $\eta = \omega$. En este caso el paralelogramo Γ se subdivide fácilmente en dos triángulos equiláteros como se muestra a la izquierda de la Figura 5.8. Basta ver que todo punto interior a uno de estos triángulos se encuentra a una distancia menor a uno de algún vértice. De hecho, en este caso esto es cierto para cualquiera de los vértices. Esto se vé fácilmente del hecho de que el círculo de radio uno centrado en uno de los vértices contiene totalmente al triángulo, como se vé a la derecha de la misma figura. $\square$

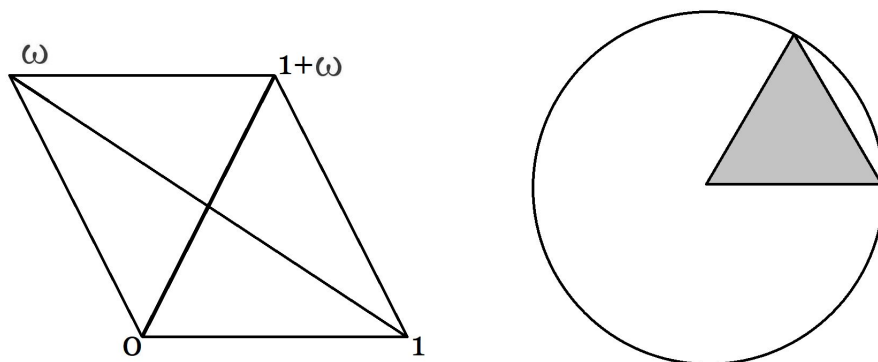


Figure 5.8: El paralelogramo fundamental del anillo de Eisenstein.

Lo anterior es suficiente para demostrar que $\mathbb{Z}[\omega]$ es un DE. Para efectos de estudiar la eficiencia del algoritmo en este anillo, el Lema 5.38, probado más abajo, puede ser útil.

Lema 5.37. *Para todo punto D , interior a un triángulo ABC como el de la Figura 5.9, la suma de los largos de los segmentos AD y DB es inferior a la suma de los lados AC y BC .*

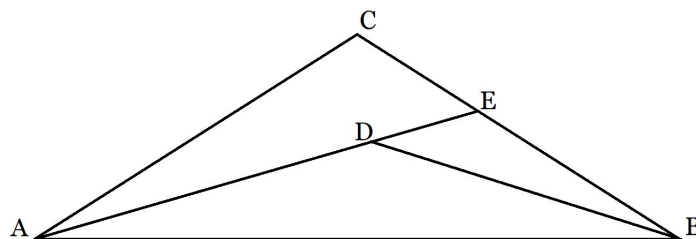


Figure 5.9: Caminos en un triángulo.

Demostración. La suma de los segmentos AD y DB , en la figura, es menos a la suma de los segmentos AE y EB , como se prueba fácilmente a partir de la instancia $DE + EB > DB$ de la desigualdad triangular. Del

mismo modo, $AC + CE > AE$ demuestra que $AC + CB > AE + EB$. $\square$

Lema 5.38. *Todo punto interior de un triángulo equilátero de lado 1 está a una distancia no mayor a $\frac{\sqrt{3}}{3}$ de alguno de los vértices, con igualdad si y sólo si el punto es el baricentro del triángulo.*

Demostración. Se subdivide el triángulo en tres subtriángulos como muestra la Figura 5.10, donde u es el baricentro. Todo punto interior debe estar contenido en alguno de ellos. Si está en el inferior, como el punto z de la figura, se tiene $|z| + |1 - z| < |u| + |1 - u| = \frac{2\sqrt{3}}{3}$, por lo que $|u| < \frac{\sqrt{3}}{3}$, o bien $|1 - u| < \frac{\sqrt{3}}{3}$. Los casos restantes son análogos. $\square$

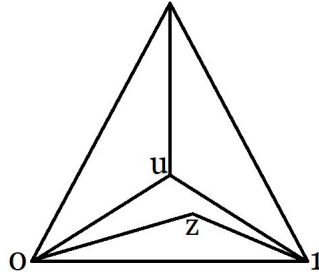


Figure 5.10: Distancia a los vértices.

El lema anterior muestra que la división con resto en el anillo de Eisenstein puede realizarse de modo que un elemento z puede escribirse siempre en la forma $z = qw + r$, de modo que el resto r satisfaga $|r| \leq \frac{\sqrt{3}}{3}|w|$. En particular, concluimos que el algoritmo de euclides, si se aplica eficientemente, permite encontrar el máximo común divisor más rápidamente aquí que en el anillo de Gauss.

Proposición 5.39. *Todo primo del anillo de Eisenstein divide a un primo racional. Los primos del anillo de Eisenstein son los primos racionales de la forma $3k - 1$, los primos de la forma $a + b\omega$, donde $a^2 - ab + b^2$ es un primo de la forma $3k + 1$, y el primo $\omega - 1$, el cual divide a 3.*

Demostración. La primera afirmación se prueba observando que todo primo π del anillo de Eisenstein divide a $|\pi|^2 = \pi\bar{\pi}$, y por lo tanto a alguno de sus factores primos, al igual que para el anillo de Gauss. Nótese que en este caso el conjugado de $\pi = a + b\omega$ es $a + b\omega^2$. El primo racional 3 se factoriza como $3 = (\omega - 1)(\omega^2 - 1) = (\omega + 1)(\omega - 1)^2 = -\omega^2(\omega - 1)^2$. Para ver que $\omega - 1$ es un primo realizamos el cálculo

$$\mathbb{Z}[\omega]/(\omega - 1) = \mathbb{Z}[x]/(x - 1, x^2 + x + 1) \cong \mathbb{Z}/\left((1)^2 + (1) + 1\right) \cong \mathbb{F}_3.$$

Del mismo modo investigamos bajo que condiciones un primo racional $p \neq 3$ es primo en el anillo de Eisenstein:

$$\mathbb{Z}[\omega]/(p) = \mathbb{Z}[x]/(p, x^2 + x + 1) \cong \mathbb{F}_p/(x^2 + x + 1).$$

Este último cociente es isomorfo a un producto $\mathbb{F}_p \times \mathbb{F}_p$, si el polinomio $x^2 + x + 1$ tiene dos raíces distintas en $\mathbb{F}_p$. Cuando el polinomio no tiene raíces, el cociente de arriba es una extensión cuadrática de $\mathbb{F}_p$. El polinomio tiene raíces si el discriminante -3 es un cuadrado. Esto sucede si y sólo si $\left(\frac{-3}{p}\right) = 1$. Un cálculo encillo nos da

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Se sigue que los primos de la forma $3k - 1$ siguen siendo primos en $\mathbb{Z}[\omega]$. Esto incluye el caso $p = 2$. Los primos de la forma $p = 3k + 1$ se factorizan en $\mathbb{Z}[\omega]$, y sólo pueden hacerlo en dos primos $\pi = a + b\omega$ de largo $\sqrt{p}$. Estos primos satisfacen $p = |\pi|^2 = a^2 - ab + b^2$. $\square$

Es posible probar que, para cada primo racional p y cada entero positivo n , existe un único cuerpo finito con p^n elementos. Este cuerpo se denota $\mathbb{F}_{p^n}$. Para detalles sobre la teoría de cuerpos finitos, el lector puede consultar los apuntes de estructuras algebraicas.

Proposición 5.40. *Un entero n tiene una expresión del tipo $n = a^2 - ab + b^2$ si y sólo si $v_p(n)$ es par para cada primo de la forma $3k - 1$ que divida a n .*

Demostración. Se pregunta si existe un elemento $z = a + b\omega \in \mathbb{Z}[\omega]$ cuyo valor absoluto sea $\sqrt{n}$. Si se escribe la factorización en primos

$$z = u\pi_1^{\alpha_1}\pi_2^{\alpha_2}\cdots\pi_N^{\alpha_N},$$

y se observa que $|u| = 1$, se obtiene

$$n = |z|^2 = |\pi_1|^{2\alpha_1} |\pi_2|^{2\alpha_2} \cdots |\pi_N|^{2\alpha_N},$$

donde cada factor $|\pi_1|^2$ es 3, un primo de la forma $3k + 1$ o el cuadrado de un primo de la forma $3k - 1$. La necesidad sigue de aquí, y la suficiencia del hecho de que siempre se pueden escoger un primo apropiados para cada uno de los factores, en cada caso. $\square$

Ejemplo 5.41. La ecuación $x^2 - xy + y^2 = 35 = 5 \times 7$ no tiene solución, ya que 5 es de la forma $3k - 1$, y el exponente correspondiente es impar.

Ejemplo 5.42. La ecuación $x^2 - xy + y^2 = 231 = 7 \times 37$ puede resolverse encontrando primero soluciones para $x^2 - xy + y^2 = 231 = 7$ y $x^2 - xy + y^2 = 231 = 37$. La primera tiene la solución $x + y\omega = 2 - \omega$ y la segunda $x + y\omega = 4 - 3\omega$. Se sigue que una solución de la solución original es

$$x + y\omega = (2 - \omega)(4 - 3\omega) = 8 - 10\omega + 3\omega^2 = 5 - 13\omega.$$

Ejemplo 5.43. La ecuación $x^2 - xy + y^2 = 175 = 5^2 \times 7$ sólo tiene soluciones del tipo $x + y\omega = 5(r + s\omega)$, con $r^2 - sr + s^2 = 7$. Una solución nos da $r = 2$ y $s = -1$, lo que nos da $w = r + s\omega = 2 - \omega$. Las restantes soluciones son de la forma uw o $u\bar{w}$, donde u es una unidad. Como las unidades tienen largo 1, es fácil ver que estas son los elementos del conjunto $\{\pm 1, \pm\omega, \pm\omega^2\}$. Esto nos dice que hay 12 soluciones esencialmente equivalentes. Estas son las siguientes:

$$\pm(r + s\omega), \pm\omega(r + s\omega) = \pm(-s + (r - s)\omega), \pm\omega^2(r + s\omega) = \pm((s - r) - r\omega)$$

y sus seis conjugados.

En el ejemplo precedente se necesita saber si los elementos de la forma uw o $u\bar{w}$, donde u es una unidad, son todos diferentes. De hecho, no es difícil ver que los elementos de la forma uw son los vértices de un hexágono regular centrado en el origen. Para que estos coincidan con los elementos de la forma $u\bar{w}$, es necesario y suficiente que el eje real sea un eje de simetría del hexágono. Esto ocurre exactamente cuando el argumento del complejo w es de la forma $\frac{k\pi}{12}$. Una mirada a la Figura 5.11 nos muestra que esto sólo

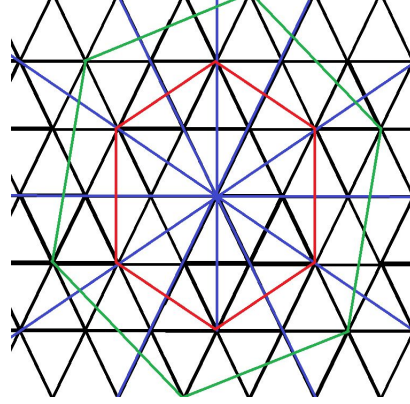


Figure 5.11: Un hexágono simétrico en rojo y uno asimétrico en verde.

puede ocurrir cuando w es un múltiplo entero racional de una unidad, o un múltiplo entero racional de $\omega - 1$ por una unidad.

La técnica nos permite también estudiar el problema más natural de la suma de dos cubos:

Ejemplo 5.44. La ecuación $x^3 + y^3 = 221 = 13 \cdot 17$ se factoriza como $(x+y)(x^2 - xy + y^2) = 221$. Lo que nos lleva a $(x+y)|x+y\omega|^2 = 221$. Nótese que $|x+y\omega|^2$ no puede ser 17 ni 221, así que podemos intentar $|x+y\omega|^2 = 13$ o $|x+y\omega|^2 = 1$. Escribiendo cada una de las seis unidades en la forma $x+y\omega$, obtenemos soluciones para x e y que no suman 221. Nos queda $|x+y\omega|^2 = 13$, lo que tiene las soluciones $x+y\omega = uw$ y $x+y\omega = u\bar{w}$, donde $w = 4 + 3\omega$. Esto nos da las soluciones $\{4, 3\}$, $\{3, -1\}$, $\{-1, -4\}$ para el par $\{x, y\}$, junto con sus negativos, lo que da 12 pares ordenados. Ninguna de estas soluciones satisface $x+y = 17$, por lo que 221 no puede ser la suma de dos cubos.

Ejemplo 5.45. Aplicando el mismo procedimiento a la ecuación $x^3 + y^3 = 91 = 13 \cdot 7$, obtenemos que $|x+y\omega|^2$ puede tomar cualquiera de los cuatro valores 1, 7, 13 o 91. Como antes, descartamos fácilmente $|x+y\omega|^2 = 1$. Si $|x+y\omega|^2 = 7$ debemos tener $x+y\omega = uw$ o $x+y\omega = u\bar{w}$, con $w = 2 - \omega$. Esto nos da las soluciones $\{2, -1\}$, $\{3, 2\}$, $\{1, 3\}$ para el par $\{x, y\}$, junto con sus negativos. Nuevamente, ninguna de estas soluciones satisface $x+y = 13$. Al probar, $|x+y\omega|^2 = 13$, se tienen como antes las soluciones $\{4, 3\}$, $\{3, -1\}$, $\{-1, -4\}$ para el par $\{x, y\}$, junto con sus negativos. El

primer par satisface $x + y = 7$, en tanto los otros se descartan. Esto nos da la solución $3^3 + 4^3 = 91$. Finalmente $|x + y\omega|^2 = 91$ tiene las soluciones de la forma $x + y\omega = u\bar{w}$, con $w = 2 - \omega$, donde $w = (2 - \omega)(4 + 3\omega) = 11 + 5\omega$, o bien $w = (2 - \omega^2)(4 + 3\omega) = 9 + 10\omega$. La primera opción nos da las soluciones $\{11, 5\}$, $\{6, 11\}$, $\{-5, 6\}$ para el par $\{x, y\}$. La segunda nos da $\{9, 10\}$, $\{-1, -10\}$ y $\{-1, 9\}$. De todas estas, sólo $\{x, y\} = \{-5, 6\}$ satisface la condición $x + y = 1$, lo que nos da la solución $(-5)^3 + 6^3 = 91$.

Un contraejemplo minimal. Consideremos el anillo $R = \mathbb{Z}[\sqrt{-3}] = \mathbb{Z}[2\omega + 1]$. Este es un subanillo del anillo de Eisenstein que contiene sólo los puntos reticulares que se encuentran una fila por medio en la retícula de la Figura 5.12. Los puntos de R están marcados en rojo en esa figura. El

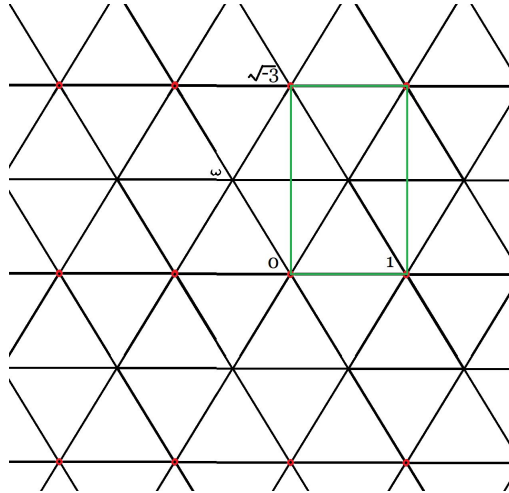


Figure 5.12: Un anillo no principal.

paralelogramo de vértices 0 , 1 , $\sqrt{-3}$ y $1 + \sqrt{-3}$ se muestra en verde. Nótese que todo punto interior a este rectángulo está a una distancia inferior a uno de uno de los puntos rojos, exceptuando sólo al centro del rectángulo, que se encuentra a distancia 1 de cualquiera de las esquinas. El anillo R , sin embargo, no es un DIP. Esto se deduce del hecho de que todo DIP es normal, mientras que la clausura entera de R en su cuerpo de cocientes es el anillo de Eisenstein.

Es interesante buscar un ejemplo donde no se tenga factorización única en irreducibles. Por ejemplo se tiene

$$(\sqrt{-3} + 1)(\sqrt{-3} - 1) = 4 = 2^2,$$

pero ninguno de los factores de la izquierda es divisible por 2 en el anillo R . Sin embargo, 2 es irreducible, dado que este anillo no tiene elementos de largo menor a $\sqrt{3}$, excepto 1, 0 y -1 , como se aprecia fácilmente en el dibujo.

Un lema que nos será útil más adelante es el siguiente:

Lema 5.46. *Un entero de Eisenstein pertenece al anillo R de arriba si y sólo si es congruente a 0 o 1 módulo 2. Las únicas unidades que satisfacen esta condición son 1 y -1 .*

Demostración. Como todo entero racional es congruente a 1 o 0 módulo 2, es suficiente probar que $R = \mathbb{Z} + 2\mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}(2\omega)$. Esto es inmediato de la Figura 5.12. La última afirmación es inmediata de la misma figura. $\square$

Nótese que $\mathbb{Z}[\omega]/(2) \cong \mathbb{F}_4$. Se sigue que el conjunto $(\mathbb{Z}[\omega]/(2))^*$ es un grupo cíclico con tres elementos.

El caso $n = 3$ de la ecuación de Fermat. Nuestro próximo consiste en aplicar la aritmética del anillo de Eisenstein, y del anillo R , al estudio de la ecuación de Fermat. Para ello necesitamos los siguientes lemas previos:

Lema 5.47. *Si u y v son relativamente primos con $u + v$ impar, entonces el elemento $u - v\sqrt{-3}$ no es divisible por ningún primo racional en $\mathbb{Z}[\omega]$.*

Demostración. Para ver que $\frac{z}{p} = \frac{u}{p} + \frac{v}{p}\sqrt{-3}$ no es entero, basta ver que los enteros de Eisenstein tienen la forma $a + b\omega = \frac{2a+b}{2} + \frac{b}{2}\sqrt{-3}$, con a y b enteros, por lo que ningún primo impar puede aparecer en el denominador, y el primo 2 sólo si aparece en ambos, mientras que nosotros asumimos que $u + v$ es impar, por lo que u y v no pueden ser ambos impares. $\square$

Lema 5.48. *Si s es impar y satisface la ecuación $s^3 = u^2 + 3v^2$, donde $u + v$ es impar y $(u) + (v) = (1)$, entonces existen enteros e y f que satisfacen la relación siguiente:*

$$u - v\sqrt{-3} = (e - f\sqrt{-3})^3.$$

Además, s no es divisible por 2 ni 3.

Demostración. Definimos $z = u + v\sqrt{-3}$, y consideramos la factorización prima $z = w\pi_1^{\alpha_1} \cdots \pi_N^{\alpha_n}$. Conjugando, se tiene $\bar{z} = \bar{w}\bar{\pi}_1^{\alpha_1} \cdots \bar{\pi}_N^{\alpha_n}$, y por lo tanto $|z|^2 = |\pi_1|^{2\alpha_1} \cdots |\pi_N|^{2\alpha_n}$. El hecho de que u y v sean relativamente primos, con $u + v$ impar, muestra que z no es divisible por ningún primo racional, por el lema precedente. Esto nos dice que en la descomposición de z no puede aparecer ningún primo de la forma $3k - 1$, ningún par de primos no asociados de la misma norma, y el primo $\omega - 1$ no puede aparecer elevado a una potencia superior a uno. En particular, esto muestra que $|z|^2 = |\pi_1|^{2\alpha_1} \cdots |\pi_N|^{2\alpha_n}$ es la descomposición prima de $|z|^2 = s^3$, por lo que los exponentes deben ser todos divisibles por 3. Se sigue que z es un cubo, salvo unidades. Además, 2 no divide a s , por ser de la forma $3k - 1$, ni tampoco 3, dado que $(\omega - 1)^3$ no puede dividir a $|z|^2$. Por otro lado, z es congruente a 1 módulo dos (por ser un elemento de R no divisible por 2), mientras que todo cubo perfecto de un elemento no divisible por 2 tiene esa misma propiedad, dado que $(\mathbb{Z}[\omega]/(2))^*$ es un grupo cíclico con tres elementos. Concluimos que la unidad es 1 o -1 , y en cualquier caso z es un cubo, por lo que podemos escribir $z = w^3$. Multiplicando por una unidad, de ser necesario, podemos suponer que w es congruente a 1 módulo 2, por lo que es también de la forma $w = e + f\sqrt{-3}$. El resultado sigue. $\square$

Demostraremos que la ecuación $a^3 + b^3 + d^3 = 0$ no tiene soluciones enteras no triviales. Como $(-1)^3 = -1$, esto es equivalente a $a^3 + b^3 = c^3$, con $c = -d$. La primera forma es simétrica, por lo que, asumiendo que las soluciones sean relativamente primas, puede asumirse que a y b son impares. Como c^3 es par, y por lo tanto divisible por 8, tenemos

$$a + b = a^3 + b^3 + a(1 - a^2) + b(1 - b^2) \cong a^3 + b^3 = c^3 \cong 0 \pmod{8}.$$

Utilizaremos también los elementos $u = \frac{a+b}{2}$ y $v = \frac{a-b}{2}$. Nótese que $a = u + v$ y $b = u - v$. En términos de estos elementos se tiene $a + b = 2u$ y

$$\begin{aligned} z &= (u + v) + (u - v)\omega = u(1 + \omega) + v(1 - \omega) \\ &= (1 + \omega) \left(u + v \frac{1 - \omega}{1 + \omega} \right) = (1 + \omega) (u - v\sqrt{-3}), \end{aligned}$$

con u par y v impar. Además son relativamente primos, o a y b no lo serían. Este remplazo es conveniente, dado que calcular valores absolutos es más sencillo en el anillo $R = \mathbb{Z}[\sqrt{-3}]$. Nótese que $1 + \omega = -\omega^2$ es una unidad. En particular, se tiene $|z|^2 = u^2 + 3v^2$.

Afirmamos que el máximo común divisor de z con $a+b$ es 1 o $\omega-1$. Esto sigue de observar que cualquier divisor común divide también a los siguientes:

$$(a+b\omega) - (a+b) = (\omega-1)b, \quad \omega(a+b) - (a+b\omega) = (\omega-1)a.$$

Un cálculo similar se aplica a los pares $(z, \bar{z})$ y $(\bar{z}, a+b)$. Esto nos reduce a dos casos:

- Asumamos primero que $\omega-1$ no divide a z . En particular, tampoco divide a $\bar{z}$, por lo que z , $\bar{z}$ y $a+b$ deben ser relativamente primos a pares. Se concluye que tanto $a+b=2u$ como $|z|^2 = u^2-3v^2$ son cubos. Digamos $r^3 = 2u$ y $s^3 = |z|^2$. En particular, el lema precedente muestra que $u - v\sqrt{-3}$ es un cubo de un elemento de la forma $w = e - f\sqrt{-3}$. Un cálculo directo nos da las relaciones

$$s = e^2 + 3f^3, \quad u = e(e^2 - 9f^2), \quad v = 3f(e^2 - f^2).$$

Como v es impar, se deduce que f es impar y e par. También son relativamente primos, ya que, si algún primo racional divide a w , lo mismo ocurre con z , contradiciendo el Lema 5.47.

Nótese que $r^3 = 2u = 2e(e-3f)(e+3f)$. Afirmamos que los factores $2e$, $e-3f$ y $e+3f$ son relativamente primos a pares. Como $(e-3f) + (e+3f) = e$, basta ver que ningún primo divide simultáneamente a los tres. Los enteros $e-3f$ y $e+3f$ son impares y e no puede ser divisible por 3, o también lo sería s , contradiciendo el Lema precedente. Para cualquier $p > 3$, Si p divide a $2e$ y $e-3f$, también divide a $2e - 2(e-3f) = 6f$, lo que contradice la hipótesis de que e y f son relativamente primos. Concluimos que cada uno de ellos es un cubo perfecto. Poniendo

$$-2e = k^3, \quad e - 3f = j^3, \quad e + 3f = m^3,$$

se obtiene la solución no trivial $j^3 + m^3 + k^3 = 0$.

- Asumamos ahora que $\omega-1$ divide a z . En este caso, $|z|^2$ es divisible por 3. Sin embargo, $(\omega-1)^2 = -3\omega$ no divide a z por el Lema 5.47, por lo que $|z|^2$ no es divisible por 3. Como $a^3 + b^3 = 2u|z|^2$ es un cubo perfecto, $2u$ debe ser divisible por 9. En particular, podemos escribir $u = 3g$. Escribimos

$$u - v\sqrt{-3} = -\left((-3)g + v\sqrt{-3}\right) = -\sqrt{-3}(v - g\sqrt{-3})$$

$$= \omega(\omega - 1) (v - g\sqrt{-3}).$$

Se sigue que $c^3 = 18g|y|^2$, con $y = v - g\sqrt{-3}$. Ahora $|y|^2 = \frac{|z|^2}{3}$ no es divisible por 3, por lo que es relativamente primo con $18g = 3(2u)$. Se sigue que tanto $18g$ como $|y|^2$ son cubos perfectos. Digamos $r^3 = 18g$ y $s^3 = |y|^2$. Además g y v son relativamente primos, y $g + v = u + v - 2g$ es impar. Se concluye que y es un cuadrado en R por el lema previo. Escribimos $y = w^3$ con $w = e - f\sqrt{-3}$. Un cálculo directo nos da las relaciones

$$s = e^2 + 3f^3, \quad v = e(e^2 - 9f^2), \quad g = 3f(e^2 - f^2).$$

Como v es impar, se deduce que e es impar y f par. También son relativamente primos, ya que, si algún primo racional divide a w , lo mismo ocurre con z , contradiciendo el Lema 5.47.

Nótese que $r^3 = 18g = 54f(e - f)(e + f)$, por lo que $(\frac{r}{3})^2 = 2f(e - f)(e + f)$. Se deduce como antes que $2f$, $e - f$ y $e + f$ son coprimos a pares, salvo que no se necesita un argumento para el primo 3. Ahora se escribe

$$-2f = k^3, \quad f - e = j^3, \quad f + e = m^3.$$

En cualquier caso se obtiene una solución de la ecuación de Fermat con números que resultan ser más pequeños, dado que jkm es un factor de c , en cada caso. Esto produce una contradicción si se parte, por ejemplo, con una solución con $|a| + |b| + |c|$ minimal. $\square$

Hexajedrez. En analogía al ajedrez infinito descrito en la sección anterior, es posible definir un juego de ajedrez hexagonal, o hexajedrez, como el que se ilustra en la Figura 5.13. En este tablero, el equivalente a las piezas reciben el nombre de abejas. En este caso, los desplazamientos horizontales o verticales se rempazan por desplazamientos en cualquiera de las seis direcciones que permiten pasar de una casilla x a otra casilla y con la que x comparte un borde. Estos desplazamientos se obtienen unos de otros mediante una rotación en un múltiplo de 60 grados, lo que corresponde a una multiplicación por una de las seis unidades del anillo de Eisenstein. Una (a, b) -abeja puede desplazarse a casillas en una de tales direcciones, para luego girar 120 grados en sentido antihorario y avanzar b casillas en la nueva dirección. El

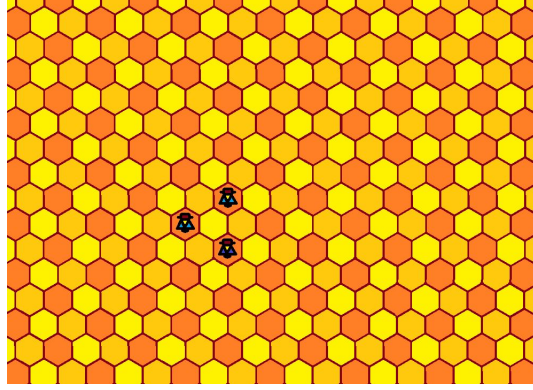


Figure 5.13: El Hexajedrez.

estudio de los tipos de abejas híbridas que pueden recorrer este tablero en su totalidad se realiza con el apoyo de la aritmética del anillo de Eisenstein, en completa analogía con el ajedrez infinito descrito antes. Nótese, en particular, que este tablero se colorea usando tres colores, que corresponden a las 3 clases residuales módulo $\omega - 1 = \omega\sqrt{-3}$. Una abeja se mueve entre casillas del mismo color si y sólo si todos sus movimientos permitidos son divisibles por $\omega - 1$.

También pueden en este caso definirse mestizos, que combinan los movimientos de una (a, b) -abeja con movimientos individuales (de hormiga?) en una dirección única. Tal como ocurre en el ajedrez, es posible demostrar que tales mestizos pueden recorrer todo el tablero. Estas generalizaciones se desarrollan en los ejercicios.

5.5 Ejercicios

1. Factorice completamente $6 + 8i$ y $12 + 5i$ en $\mathbb{Z}[i]$.
2. Factorice completamente $12\omega + 3$ y $8\omega + 3$ en $\mathbb{Z}[\omega]$.
3. Probar que $\mathbb{Z}[\sqrt{-2}]$ es un DIP.
4. Sea $u = \frac{1+\sqrt{-7}}{2}$. Probar que $\mathbb{Z}[u]$ es un DIP.

5. Probar que $\mathbb{Z}[\sqrt{-7}]$ no es un DIP, encontrando un primo racional que sea irreducible pero no primo en ese anillo. Repita lo mismo para $\mathbb{Z}[\sqrt{-13}]$.
6. De un ejemplo de un ideal no principal en $\mathbb{Z}[\sqrt{-5}]$.
7. De un ejemplo de un ideal no principal en $\mathbb{Z}[\sqrt{-3}]$. Sugerencia: Observe que si $B \subseteq A$ son anillos, todo ideal de A contenido en B es un ideal de B .
8. Encuentre todos los pares de enteros (a, b) tales que $a - bi$ es un múltiplo (en el anillo de enteros de Gauss) de $a + bi$.
9. Encuentre todos los pares de enteros (a, b) tales que $a + b\omega^2$ es un múltiplo (en el anillo de enteros de Eisenstein) de $a + b\omega$.
10. Encuentre todas las maneras de escribir 1729 como suma de dos cubos de números enteros.
11. Sea D un DFU, sea L un cuerpo que contiene a D , y sea $\alpha \in L$ un elemento que es entero sobre D (es decir que satisface algún polinomio mónico con coeficientes en D). Probar que el polinomio irreducible de α sobre el cuerpo $K = \text{Quot}(D)$ tiene coeficientes en D .
12. Sea D un dominio de integridad, y sea K su cuerpo de cocientes. Probar que una matriz $A \in \mathbb{M}_n(K)$ es entera sobre D (es decir que satisface un polinomio con coeficientes en D) si y sólo si sus valores propios (en $\overline{K}$) son enteros sobre D .
13. Sea K un cuerpo y sean D y D' dos dominios de integridad contenidos en K . Suponga que los cuerpos de cocientes de D y D' coinciden. Probar que si $\alpha \in K$ es entero simultáneamente sobre D y D' , entonces es entero sobre $D \cap D'$.
14. Sea D un dominio de integridad, sea L un cuerpo que contiene a D , y sea $\alpha \in K$ un elemento algebraico sobre $K = \text{Quot}(D)$. Probar que si existe $n \in D$ tal que $n\alpha$ es entero sobre D .
15. Probar que si D es un DIP, también lo es $D[1/d]$ para todo $d \in D$.

16. Probar que si

$$R = \mathbb{Z} \left[x, \frac{1}{x+1} \right]$$

entonces $R/(x^2+x+1)$ es un dominio de ideales principales (Sugerencia: usar que $\mathbb{Z}[x]/(x^2+x+1)$ es isomorfo al anillo de enteros de Eisenstein).

17. Describa el anillo $A/(x^2+1)$ donde $A = \mathbb{Z}[x, x^{-1}]$.
18. Sea $f(x) = x^n + \cdots + a_1x + a_0$ un polinomio mónico irreducible con coeficientes enteros. Sea α una raíz de f y suponga que $\mathbb{Z}[\alpha]$ es un dominio de ideales principales. Probar que existen infinitos primos en $\mathbb{Z}[\alpha]$.
19. Considere la $\mathbb{R}$ -álgebra $A = \mathbb{R} \times \mathbb{R}$ con operaciones por coordenada. Sea d un entero positivo libre de cuadrados. Muestre que el anillo $\mathbb{Z}[\sqrt{d}]$ es isomorfo al subanillo D de A generado por $1_D = (1, 1)$ y $\delta = (\sqrt{d}, \sqrt{-d})$.
20. En las notaciones de la pregunta anterior, asuma que el rectángulo de vértices $0_D, 1_D, \delta, \delta + 1_D$ puede ser totalmente cubierto por regiones abiertas de la forma $z + U$ con $z \in D$ y $U = \{(x, y) \in \mathbb{R} \times \mathbb{R} | xy < 1\}$. Demuestre que $g(x + y\sqrt{d}) = |x^2 - dy^2|$ es un algoritmo de Euclides para el anillo D . Concluya que D es un DIP.
21. Extienda los dos ejercicios precedentes a anillos de la forma $\mathbb{Z} \left[\frac{1+\sqrt{d}}{2} \right]$, con $d = 4k + 1$.
22. Usar los ejercicios anteriores para probar que $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z} \left[\frac{1+\sqrt{5}}{2} \right]$ y $\mathbb{Z}[\sqrt{7}]$ son dominios Euclidianos.
23. Sea L/K una extensión finita de cuerpos, y sea Ω un dominio de integridad cuyo cuerpo de cocientes es L . Sea $D = K \cap \Omega$. Es necesariamente cierto que Ω es entero sobre D ? Demuestre dicha afirmación o de un contraejemplo.