Grupos y Anillos

Ángel del Río Mateos

September 29, 2022

Contenidos

Capítulo 1

Anillos

1.1 Operaciones binarias

Sea X un conjunto. Una *operación binaria* en X es una aplicación $* : X \times X \to X$. La imagen de (a, b) la denotamos $a * b$.

Decimos que $*$ es:

- *conmutativa* si $x * y = y * x$ para todo $x, y \in X$;
- *asociativa* si $x * (y * z) = (x * y) * z$ para todo $x, y, z \in X$.

Un elemento $x \in X$ se dice que es:

- *neutro por la izquierda* (*neutro por la derecha*) de X con respecto a $*$ si $x * y = y$ para todo $y \in X$ ($y * x = y$ para todo $y \in X$).
- *cancelable por la izquierda* (*cancelable por la derecha*) en X respecto de $*$ si para cada dos elementos distintos a y b de X se verifica $x * a \neq x * b$ ($a * x \neq b * x$).
- Supongamos que e es un elemento neutro de X con respecto a $*$. Sean x e y elementos de X. Decimos que x es *simétrico de y por la izquierda* y que y es *simétrico de x por la derecha* con respecto a $*$ si se verifica $x * y = e$.

Decimos que x es

- *neutro* de X con respecto a $*$ si es neutro por la izquierda y por la derecha de X con respecto a $*$.
- *cancelable* en X con respecto a $*$ si es cancelable en X con respecto a $*$ por los dos lados.
- *simétrico* de y con respecto a $*$ si es simétrico de y con respecto a $*$ por los dos lados. En tal caso decimos que x es *invertible* en X con respecto a $*$.

Un par $(X, *)$ formado por un conjunto y una operación $*$ decimos que es un

- *semigrupo* si $*$ es asociativa;

- *monoide* si es un semigrupo que tiene un elemento neutro con respecto a $*$;
- *grupo* si es un monoide y todo elemento de X es invertible con respecto a $*$.
- *grupo abeliano* si es un grupo y $*$ es conmutativa.

En el futuro simplificaremos la terminología y en lugar de decir "operación binaria" diremos simplemente "operación". Por otro lado nos ahorraremos los "con respecto a" cuando la operación esté clara por el contexto y los "de X" o "en X" cuando el conjunto X esté claro por el contexto o diremos que e es neutro, neutro por un lado, inverso, invertible o cancelable en $(X, *)$.

Veamos algunos ejemplos

Ejemplos 1.1 *Operaciones.*

(1) La suma es una operación en los conjuntos $\mathbb{N}$ de los números naturales, $\mathbb{Z}^{\geq 0}$ de los enteros no negativos, $\mathbb{Z}$ de los números enteros, $\mathbb{Q}$ de los números racionales, $\mathbb{R}$ de los números reales y $\mathbb{C}$ de los números complejos. En todos los casos se trata de una operación conmutativa y asociativa en la que todos los elementos son cancelable. Además 0 es neutro. Todo elemento a de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ es invertible respecto de la suma y su simétrico es su opuesto $-a$. Sin embargo en $\mathbb{N}$ sólo el 0 tiene simétrico respecto de la suma. Por tanto $(\mathbb{N}, +)$ es un semigrupo conmutativos, $(\mathbb{Z}^{\geq 0}, +)$ es un monoide conmutativo, y $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ y $(\mathbb{C}, +)$ son grupos abelianos.

(2) Otra operación conmutativa y asociativa en $\mathbb{N}$, $\mathbb{Z}^{\geq 0}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ es el producto. En este caso el 1 es el neutro y todo elemento $a \neq 0$ de $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ es invertible y su simétrico es su inverso a^{-1}. Sin embargo, en $\mathbb{Z}$ solamente 1 y -1 son invertibles respecto del producto mientras que 1 es el único elemento invertible de $\mathbb{N}$ y $\mathbb{Z}^{\geq 0}$. Por tanto, el producto define en todos estos conjuntos una estructura de monoide conmutativo y define una estructura de grupo abeliano en $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ y $\mathbb{C} \setminus \{0\}$. El único elemento de estos conjuntos que no es cancelativo con respecto al producto es el cero.

(3) Sea A un conjunto y sea $X = A^A$, el conjunto de las aplicaciones de A en A. La composición de aplicaciones define una operación asociativa en X para la que la identidad 1_X es neutro. Por tanto $(A^A, \circ)$ es un monoide. Sin embargo, esta operación no es conmutativa si A tiene al menos dos elementos (ver Problema 1.1.2).

(4) Sea A un conjunto y sea $X = \mathbb{R}^A$ el conjunto de las aplicaciones de A a $\mathbb{R}$. Definimos la suma en X poniendo

$$(f + g)(a) = f(a) + g(a) \quad (a \in A).$$

Esta es una operación conmutativa y asociativa, la aplicación 0 dada por $0(a) = 0$ para todo $a \in A$ es un neutro y para toda aplicación $f : A \to \mathbb{R}$, el simétrico de f con respecto a $+$ es la aplicación $-f$ dada por $(-f)(a) = -f(a)$. Por tanto $(\mathbb{R}^A, +)$ es un grupo abeliano.

Definimos ahora el producto $\cdot$ en X poniendo

$$(f \cdot g)(a) = f(a)g(a).$$

Esta operación también es conmutativa y asociativa y tiene por neutro la aplicación 1 dada por $1(a) = 1$ para todo $a \in A$. Para que un elemento f de X sea invertible es necesario y suficiente que $f(a) \neq 0$ para todo a. En tal caso el simétrico de f con respecto a $\cdot$ es la aplicación g dada por $g(a) = g(a)^{-1}$. Luego $(\mathbb{R}^A, \cdot)$ es un monoide conmutativo.

Veamos ahora algunas propiedades básicas de las definiciones dadas más arriba.

Proposición 1.2 *Sea $*$ una operación en un conjunto X.*

(1) Si $*$ es conmutativa entonces todo neutro por un lado, es neutro, todo elemento cancelativo por un lado es cancelativo y todo elemento que tenga simétrico por un lado es invertible.

(2) Si e es un neutro por la izquierda y f es un neutro por la derecha de X con respecto a $*$ entonces $e = f$. En particular, X tiene a lo sumo un neutro.

(3) Supongamos que $(X, *)$ es un monoide y sea $a \in X$.

(a) Si x es un simétrico por la izquierda de a e y es un simétrico por la derecha de a entonces $x = y$. Por tanto, en tal caso a es invertible y tiene a lo sumo un simétrico.

(b) Si a tiene un simétrico por un lado entonces es cancelable por ese mismo lado. En particular todo elemento invertible es cancelable.

Demostración. (1) es obvio.

(2) Como e es neutro por la izquierda y f es neutro por la derecha tenemos

$$f = e * f = e.$$

(3a) Ahora suponemos que $(X, *)$ es un monoide. Por (2), $(X, *)$ tiene un único neutro que vamos a denotar por e. Como x es inverso por la izquierda de a e y es inverso por la derecha de a, usando la propiedad asociativa, tenemos que

$$y = e * y = (x * a) * y = x * (a * y) = x * e = x.$$

(3b) Supongamos que a es un elemento de X que tiene un inverso por la izquierda b y que $ax = ay$ para $x, y \in X$. Usando la asociatividad una vez mas concluimos que

$$x = e * x = (b * a) * x = b * (a * x) = b * (a * y) = (b * a) * y = e * y = y.$$

∎

Por la Proposición 1.2, si $(X, *)$ es un monoide cada elemento invertible a sólo tiene un simétrico que habitualmente se denota a^{-1}.

Problemas

1.1.1 (1) Demostrar que si X es el conjunto vacío o tiene exactamente un elemento, entonces X sólo admite una operación. Sin embargo si X tiene dos elementos, entonces X tienen 16 operaciones. ¿Puedes enumerarlas todas y para cada una de ellas decir si son conmutativas, asociativas, cuáles son los elementos cancelables, si tienen neutro, y en tal caso identificar los elementos invertibles y los que tienen inverso por la izquierda o por la derecha?

(2) ¿Cuántas estructuras de semigrupo, monoide y grupo se pueden definir en un conjunto con dos elementos?

(3) ¿Cuántas operaciones tiene un conjunto con n elementos?

1.1.2 Sea A un conjunto y sea $X = A^A$, el conjunto de las aplicaciones de A en A.

(1) Demostrar que $(X, \circ)$ es conmutativo si y solo si A no tiene más de un elemento.

(2) ¿Cuáles son los elementos invertibles de X con respecto a $\circ$? ¿Cuáles son los que tienen simétrico por la izquierda y cuáles los que lo tienen por la derecha?

(3) Supongamos que $A = \mathbb{N}$ y sean $f, g : \mathbb{N} \to \mathbb{N}$ dadas por

$$f(x) = x + 1, \quad g(x) = \begin{cases} x - 1, & \text{si } x \neq 1; \\ 0, & \text{si } x = 1. \end{cases} \quad (x \in \mathbb{N}).$$

Demostrar que g es inverso por la izquierda de f pero que f no tiene inverso por la derecha.

(4) Demostrar que si A es finito entonces todo elemento de X que tiene un inverso por un lado es invertible.

1.1.3 Considérense los siguientes subconjuntos de números complejos: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{R}^+ = \{a \in \mathbb{R} : a > 0\}$, $\mathbb{R}^- = \{a \in \mathbb{R} : a < 0\}$, $\{1, -1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$, $\mathbb{Q}[i] \setminus \{0\}$, $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} : a, b \in \mathbb{Z}\}$ y $A = \{a + b\sqrt[3]{n} : a, b \in \mathbb{Z}\}$ donde n es un número natural.

(1) ¿Cuáles de ellos son cerrados respecto de la suma y cuáles respecto del producto?:

(2) ¿Cuáles de ellos son semigrupos, monoides o grupos respecto de la suma o del producto?

1.1.4 Para dos enteros positivos m y n y un conjunto A denotamos por $M_{m,n}(A)$ el conjunto de las matrices con m filas y n columnas y con entradas en A y también denotamos $M_n(A) = M_{n,n}(A)$.

(1) Demostrar que la suma habitual de matrices define una estructura de grupo abeliano en $M_{m,n}(\mathbb{C})$ y el producto de matrices define una estructura de monoide en $M_n(\mathbb{C})$.

(2) ¿Para qué valores de n, es $M_n(\mathbb{C})$ conmutativo?

(3) Decid cuáles de los siguientes conjuntos son cerrados para la suma y cuáles para el producto. Decid también cuántos forman un semigrupo, un monoide o un grupo con la suma o con el producto: $M_n(\mathbb{N})$, $M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$, $T_n(\mathbb{C})$ = matrices triangulares superiores o sea debajo de la diagonal tienen ceros, A = conjunto de las matrices n por n que tienen ceros en todas las entradas menos en la $(1,1)$, $D_n(\mathbb{C})$ = conjunto de las matrices diagonales, o sea todas las entradas fuera de la diagonal son cero, $E_n(\mathbb{C}) = \{aI_n : a \in \mathbb{C}\}$, donde I_n denota la matriz identidad n por n.

1.1.5 Demostrar que si a y b son elementos invertibles en un monoide entonces ab y a^{-1} también son invertible y $(a^{-1})^{-1} = a$. Deducir que el conjunto de los elementos invertibles de un monoide forma un grupo con la operación del monoide.

1.1.6 Sea $*$ una operación en un conjunto X y $\circ$ una operación en otro conjunto Y. Definimos en el producto cartesiano $X \times Y$ la operación

$$(a_1, b_1)\#(a_2, b_2) = (a_1 * a_2, b_1 \circ b_2).$$

Decidir qué tienen que cumplir las operaciones originales para que # sea asociativa, conmutativa, tenga neutro y en tal caso identificar los elementos invertibles con respecto a # y sus simétricos en función de las operaciones originales.

1.1.7 Demostrar que si $(X, *)$ es un monoide finito y $x \in X$ entonces las siguientes condiciones son equivalentes:

(1) a es cancelable por un lado.

(2) a es cancelable.

(3) a tiene simétrico por un lado.

(4) a tiene simétrico.

Dar un ejemplo de un elemento cancelable de un monoide conmutativo que no tenga simétrico.

1.1.8 Sea $*$ una operación en un conjunto X y supongamos que $*$ tiene un neutro y tres elementos a, b, c tales que $a \neq c$, b es simétrico por la izquierda de a y c es simétrico por la izquierda de b. Demostrar que $*$ no es asociativa. Conluir que si $(M, *)$ es un monoide en el que todo elemento por la izquierda tiene simétrico, entonces $(M, *)$ es un grupo.

1.2 Anillos

Definición 1.3 *Un* anillo *es una terna $(A, +, \cdot)$ formada por un conjunto no vacío A y dos operaciones $+$ y $\cdot$ en A; la primera llamada usualmente* suma *y la segunda* producto *o* multiplicación*, que verifican:*

(1) $(A, +)$ es un grupo abeliano.

(2) $(A, \cdot)$ *es un monoide.* [1]

(3) Distributiva del producto respecto de la suma $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *para todo* $a, b, c \in A$.

Si además $\cdot$ *es conmutativo en* A *entonces decimos que* $(A, +, \cdot)$ *es un* anillo conmutativo.

Cuando no haya riesgo de confusión con las operaciones diremos simplemente que A es un anillo. Si a y b son elementos de un anillo A, usualmente escribiremos ab en vez de $a \cdot b$. Además asumiremos que, en ausencia de paréntesis, los productos se realizan antes que las sumas (y que las restas). Así, por ejemplo, la propiedad distributiva se reescribe como $a(b+c) = ab+ac$. Se define la resta de a y b como $a - b = a + (-b)$. Los neutros de A con respecto a la suma y el producto se llaman respectivamente *cero* y *uno* de A y se denotan 0 y 1. El simétrico de un elemento a de A con respecto a la suma se llama *opuesto* y se denota $-a$. Decimos que a es *invertible* en A cuando lo sea respecto del producto y en tal caso al simétrico de a respecto del producto lo llamamos *inverso* de a en A y lo denotamos a^{-1}. Los elementos invertibles de A también se llaman *unidades* de A Denotaremos por A^* al conjunto de todas las unidades de A.

Si b es invertible en A y A es conmutativo, escribiremos a veces a/b ó $\frac{a}{b}$ en lugar de ab^{-1}. Sin embargo no se debe usar esto si A no es conmutativo pues esa notación no distingue entre ab^{-1} y $b^{-1}a$.

Como $(A, +)$ es un grupo, todo elemento de A es invertible respecto de la suma y por tanto cancelable. Diremos que un elemento de A es *regular* en A si es cancelable con respecto al producto. En caso contrario decimos que el elemento es *singular* en A o *divisor de cero*.

Ejemplos 1.4 *Anillos.*

(1) Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos conmutativos con la suma y el producto usuales. Nótese que todo elemento no nulo de $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ es invertible. Sin embargo en $\mathbb{Z}$ sólo hay dos elementos invertibles aunque todos los elementos son regulares menos el 0.

(2) Sean A y B dos anillos. Entonces el producto cartesiano $A \times B$ tiene una estructura de anillo con las operaciones definidas componente a componente, o sea:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \quad \text{y} \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2).$$

Obsérvese que $A \times B$ es conmutativo si y solo si lo son A y B, y que esta construcción se puede generalizar a productos cartesianos de cualquier familia (finita o no) de anillos.

(3) Dados un anillo A y un conjunto X, el conjunto A^X de las aplicaciones de X en A es un anillo con las siguientes operaciones:

$$(f + g)(x) = f(x) + g(x) \qquad (f \cdot g)(x) = f(x) \cdot g(x).$$

¿Cuál es la relación entre este ejemplo y el anterior?

[1] Algunos autores distinguen entre anillo con y sin uno. En este segundo caso no se exige que el producto tenga un neutro. Sin embargo nosotros siempre supondremos que el producto tiene neutro, es decir nuestros anillos "tienen uno".

(4) Dado un anillo A, un *polinomio en una indeterminada* es una expresión del tipo

$$P = P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

donde n es un número entero no negativo y $a_i \in A$ para todo i y X es simplemente un símbolo que no representa ningún elemento de A al que nos referiremos como *indeterminada*[2]. Para cada i, a_i se llama *coeficiente* de *grado* i de P. Si un coeficiente no aparece en la expresión de un polinomio se considera que vale 0. Dos polinomios son iguales si y solo si lo son coeficiente a coeficiente. Además a_0 se llama *coeficiente independiente* de P y, si $a_n \neq 0$, entonces n es el *grado* de P y a_n es su *coeficiente principal*.

Denotaremos por $A[X]$ al conjunto de los polinomios en la indeterminada X con coeficientes en A.

Utilizando la estructura de anillo de A se puede dotar a $A[X]$ de una estructura de anillo definiendo la suma y el producto de la forma usual:

$$(a_0 + a_1X + a_2X^2 + \cdots) + (b_0 + b_1X + b_2X^2 + \cdots) = c_0 + c_1X + c_2X^2 + \cdots,$$

donde cada $c_n = a_n + b_n$, y

$$(a_0 + a_1X + a_2X^2 + \cdots) \cdot (b_0 + b_1X + b_2X^2 + \cdots) = d_0 + d_1X + d_2X^2 + \cdots,$$

donde cada $d_n = a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0 = \sum_{i=0}^{n} a_ib_{n-i}$.

(5) Dado un anillo A, denotamos por $A[[X]]$ el conjunto de las sucesiones $(a_0, a_1, a_2, \ldots)$ de elementos de A. En $A[[X]]$ consideramos la suma y el producto dados por

$$\begin{aligned} (a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots) \\ (a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) &= (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \ldots). \end{aligned}$$

Obsérvese la similitud con la definición de las operaciones en el anillo de polinomios; de hecho, el elemento $(a_0, a_1, a_2, \ldots)$ se suele denotar por $\sum_{i=0}^{\infty} a_iX^i$. Con estas operaciones, $A[[X]]$ es un anillo llamado el *anillo de series de potencias* con coeficientes en A.

(6) Si A es un anillo y n es un entero positivo entonces el conjunto $M_n(A)$ es un anillo con la suma y producto habituales de matrices.

De los axiomas de anillo se pueden deducir algunas propiedades elementales:

Lema 1.5 *Sea A un anillo y sean $a, b, c \in A$. Entonces se verifican las siguientes propiedades:*

(1) Todo elemento de A es cancelable respecto de la suma.

(2) Todo elemento invertible de A es regular en A.

[2]Más rigurosamente deberíamos definir un polinomio como una sucesión (a_n) de elementos de A de forma que $\{m \in \mathbb{Z}^{\geq 0} : a_m \neq 0\}$ es finito. Sin embargo, lo habitual es la notación $a_0 + a_1X + \cdots + a_nX^n$ para esta sucesión entendiendo que $a_m = 0$ para todo $m \geq n$.

(3) Si $b + a = a$, entonces $b = 0$. Si $ba = a$ para todo a, entonces $b = 1$. En particular, el cero y uno son únicos.

(4) El opuesto de a es único y si a es invertible, entonces a tiene un único inverso.

(5) $0a = 0 = a0$.

(6) $a(-b) = (-a)b = -(ab)$.

(7) $a(b - c) = ab - ac$.

(8) a y b son invertibles si y solo si ab y ba son invertible . En tal caso $(ab)^{-1} = b^{-1}a^{-1}$.

(9) Si $0 = 1$, *entonces* $A = \{0\}$.

Demostración. Demostraremos (5), (6), (8) y (9) y dejamos los otros apartados como ejercicio para el lector.

(5) $0a = (0 + 0)a = 0a + 0a$. Aplicando (3) deducimos que $0a = 0$. La otra igualdad se demuestra análogamente.

(6) $ab + a(-b) = a(b + (-b)) = a0 = 0$, por (5). Luego $a(-b) = -(ab)$. La otra igualdad se demuestra análogamente.

(8) Si a y b son invertibles entonces $(ab)(b^-1a^-1) = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1$ y análogamente $(b^{-1}a^{-1})(ab) = 1$. Por tanto ab es invertible y su inverso es b^-1a^-1. Por simetría ba es invertible y su inverso es $a^{-1}b^{-1}$.

Recíprocamente, supongamos que ab y ba son invertibles. Entonces $a(b(ab)^{-1}) = (ab)(ab)^{-1} = 1$ y $((ba)^{-1}b)a = (ba)^{-1}(ba) = 1$. Esto demuestra que a tiene un inverso por la derecha y otro por la derecha. Aplicando el apartado (3a) de la Proposición 1.2 deducimos que a es invertible. Por simetría b también es invertible.

(9) Si $0 = 1$ y $a \in A$ entonces $a = a1 = a0 = 0$, por (5). ∎

Dados un anillo A, un elemento $a \in A$ y un entero positivo n, la notación na (respectivamente a^n) representa el resultado de sumar (respectivamente multiplicar) a consigo mismo n veces, y si $n = 0$ convenimos que $0a = 0$ y $a^0 = 1$. Más rigurosamente, a partir de estas últimas igualdades se definen na y a^n de forma recurrente poniendo $(n + 1)a = a + na$ y $a^{n+1} = aa^n$ para $n \geq 0$. Por último, si $n \geq 1$ se define $(-n)a = -(na)$, y si además a es invertible se define $a^{-n} = (a^{-1})^n$.

El siguiente lema recopila algunas propiedades elementales de esta notación cuya demostración dejamos al lector.

Lema 1.6 *Dados un anillo A, elementos $a, b \in A$ y enteros $m, n \in \mathbb{Z}$, se verifican las siguientes propiedades:*

(1) $n(a + b) = na + nb$.

(2) $(n + m)a = na + ma$.

(3) Si $n, m \geq 0$ entonces $a^{n+m} = a^n a^m$. Si a es invertible entonces la igualdad también se verifica para n y m enteros arbitrarios.

(4) Si A es conmutativo y $n \geq 0$ entonces $(ab)^n = a^n b^n$. Si además a y b son invertibles entonces la igualdad también se verifica para todo entero n.

Problemas

1.2.1 Demostrar los apartados de los lemas 1.5 y 1.6 que no han sido demostrados.

1.2.2 Sea $m \in \mathbb{Z}$. Demostrar que si m no es un cuadrado en $\mathbb{Z}$, entonces tampoco es un cuadrado en $\mathbb{Q}$.

1.2.3 Dar un ejemplo de dos elementos invertibles a y b de un anillo en el que $(ab)^{-1} \neq a^{-1}b^{-1}$.

1.3 Subanillos

A partir de ahora supondremos que todos los anillos serán conmutativos, con lo que por defecto cada vez que digamos anillo estaremos suponiendo que se trata de un anillo conmutativo.

Sea $*$ una operación en un conjunto A y sea B un subconjunto de A. Decimos que B es *cerrado* con respecto a $*$ si para todo $a, b \in B$ se verifica que $a * b \in B$. En tal caso podemos considerar $*$ como una operación en B que se dice *inducida* por la operación en A.

Un *subsemigrupo* de un semigrupo es un subconjunto suyo que con la misma operación es un semigrupo. Un *subgrupo* de un grupo es un subconjunto suyo que con la misma operación es un grupo. Un *submonoide* de un monoide es un subconjunto suyo que con la misma operación es un monoide con el mismo neutro. Un *subanillo* de un anillo es un subconjunto suyo que con la misma suma y producto es un anillo con el mismo uno.

Está claro que para que un subconjunto X de un semigrupo $(S, *)$ es suficiente con que X sea cerrado con respecto a $*$. Sin embargo, para que un subconjunto X de un monoide $(M, *)$ sea submonoide además de que sea cerrado con respecto a $*$ también hace falta que X contenga el neutro de M.

La siguiente proposición nos dice cómo comprobar si un subconjunto es un subanillo.

Proposición 1.7 *Las condiciones siguientes son equivalentes para un subconjunto B de un anillo A:*

(1) B es un subanillo de A.

(2) B contiene al 1 y es cerrado para sumas, productos y opuestos.

(3) B contiene al 1 y es cerrado para restas y productos.

Demostración. (1) implica (2). Si B es un subanillo de A entonces B contiene al 1 y es cerrado para sumas y productos, por definición. Por otro lado, como B es un anillo, tiene un cero, que de momento denotamos 0_B y cada elemento $b \in B$ tiene un opuesto en B. En realidad $0_B + 0_B = 0_B = 0 + 0_B$, con lo que aplicando la propiedad cancelativa de la suma (Lema 1.5.(1)) deducimos que $0_B = 0$, o sea el cero de A está en B y por tanto es el cero de B (el único que puede tener por el Lema 1.5.(3).) Por la unicidad del opuesto (Lema 1.5.(4)), este opuesto ha de ser el de A, con lo que B es cerrado para opuestos.

(2) implica (3) es evidente.

(3) implica (1). Sea B un subconjunto de A que contiene al uno y es cerrado para restas y productos. Entonces $0 = 1 - 1 \in B$, con lo que si $b \in B$, entonces $-b = 0 - b \in B$; es decir, B es cerrado para opuestos. Si $a, b \in B$, entonces $-b \in B$ y, por tanto, $a + b = a - (-b) \in B$; es decir, B es cerrado para sumas. Ahora es evidente que B es un subanillo de A. ∎

Ejemplos 1.8 *Subanillos.*

(1) Todo anillo A es un subanillo de sí mismo, al que llamamos *impropio* por oposición al resto de subanillos, que se dicen *propios*.

(2) Cada uno de los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ es un subanillo de los posteriores (y de si mismo).

(3) Si A es un anillo, el subconjunto $\{0\}$ es cerrado para sumas, productos y opuestos. Si $A = \{0\}$ entonces $\{0\}$ sería subanillo de A, pero este es el único caso en el que esto pasa pues en todos los demás casos $1 \neq 0$ (¿por qué?).

(4) Si A es un anillo entonces el conjunto

$$\mathbb{Z}1 = \{n1 : n \in \mathbb{Z}\}$$

es un subanillo de A contenido en cualquier otro subanillo de A; es decir, $\mathbb{Z}1$ es el menor subanillo de A, y se conoce como el *subanillo primo* de A.

Es claro que $\mathbb{Z}$ y los $\mathbb{Z}_n$ son sus propios subanillos primos, y por lo tanto no tienen subanillos propios.

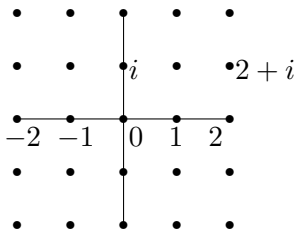
(5) Si A y B son anillos y $B \neq 0$ entonces $A \times 0 = \{(a, 0) \mid a \in A\}$ es cerrado para sumas y productos pero no es un subanillo de $A \times B$ (¿por qué?).

(6) Dado un número entero m, los conjuntos

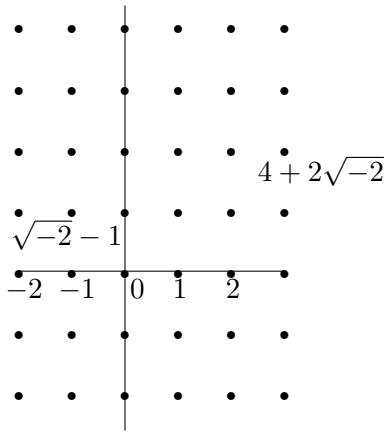
$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \qquad \text{y} \qquad \mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$$

son subanillos de $\mathbb{C}$. Si además m es positivo, entonces ambos son subanillos de $\mathbb{R}$. Si m es el cuadrado de un número entero entonces esos conjuntos coinciden con $\mathbb{Z}$ y con $\mathbb{Q}$, respectivamente, por lo que el ejemplo carece de interés. Cuando m no es el cuadrado de un entero (por ejemplo $m = 2$ ó $m = -1$) entonces tampoco es el cuadrado de un número racional (ver Problema 1.2.2), de manera que, en cualquiera de los dos anillos descritos, la igualdad $a + b\sqrt{m} = 0$ implica que $a = 0$ y $b = 0$, y por lo tanto la igualdad $a + b\sqrt{m} = c + d\sqrt{m}$ implica que $a = c$ y $b = d$.

Un caso particular es el anillo $\mathbb{Z}[i]$, donde $i = \sqrt{-1}$, llamado el *anillo de los enteros de Gauss*. Podemos visualizar $\mathbb{Z}[i]$ dentro del plano complejo como el conjunto de los vértices de un enlosado del plano complejo por losas cuadradas de lado 1, como muestra el siguiente esquema:



Más generalmente, si $m < 0$, entonces podemos visualizar $\mathbb{Z}[\sqrt{m}]$ como el conjunto de vértices de un enlosado del plano complejo por losas rectangulares con una base de longitud 1 y una altura de longitud $\sqrt{-m}$. Por ejemplo, una porción de $\mathbb{Z}[\sqrt{-2}]$ está representada por los siguientes puntos del plano complejo:



(7) Todo anillo A puede verse como un subanillo del anillo de polinomios $A[X]$ si identificamos los elementos de A con los *polinomios constantes* (del tipo $P = a_0$).

(8) Sea A un anillo y X un conjunto. Entonces la *diagonal*

$$B = \{f \in A^X : f(x) = f(y) \text{ para todo } x, y \in X\}$$

(es decir, el conjunto de las *aplicaciones constantes* de X en A) es un subanillo de A^X.

Problemas

1.3.1 ¿Cuáles de los siguientes subconjuntos A_i son subanillos de los anillos A indicados? ¿por qué?

(1) $A = \mathbb{C}$: $A_1 = \{a + bi : a = b\}$, $A_2 = \{ai : a \in \mathbb{R}\}$, $A_3 = \{a_1 + a_2\sqrt{2} + a_3 i + a_4\sqrt{2}i : a_1, a_2, a_3, a_4 \in \mathbb{Z}\}$, $A_4 = \{a + bi : b \geq 0\}$.

(2) $A = B \times B$, con B un anillo: $A_1 = B \times \{0\}$, $A_2 = B \times \{1\}$, $A_3 = B_1 \times B_2$, donde B_1 y B_2 son subanillos de B; $A_4 = \{(b, b) : b \in B\}$.

(3) $A = B[X]$, donde B es un anillo: $A_1 = B_1[X]$, donde B_1 es un subanillo de A; $A_2 =$ Polinomios de grado menor o igual que un número dado n.

(4) A, un anillo cualquiera: $A_1 = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n : n \geq 0, a_0, a_1, \ldots, a_n \in B\}$ donde B es un subanillo de A y $\alpha \in A$.

(5) $A = M_n(B)$, donde B es un anillo: $A_1 =$ Conjunto de las matrices diagonales, $A_2 =$ Conjunto de las matrices cuyas entradas no nulas están siempre en la primera fila.

1.3.2 Decimos que un entero d es *libre de cuadrados* si p^2 no divide a d para ningún número primo p (en particular 1 es libre de cuadrados). Demostrar que para todo $m \in \mathbb{Z}$ existe un $d \in \mathbb{Z}$ libre de cuadrados tal que $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{d}]$. ¿Ocurre lo mismo si cambiamos $\mathbb{Q}$ por $\mathbb{Z}$?

1.4 Homomorfismos de anillos

Definición 1.9 *Sean A y B dos anillos. Un* homomorfismo de anillos *entre A y B es una aplicación $f : A \to B$ que conserva las operaciones y la unidad; es decir, que satisface*

$$f(x + y) = f(x) + f(y), \qquad f(x \cdot y) = f(x) \cdot f(y)$$

para cada par de elementos $x, y \in A$ y

$$f(1) = 1.$$

Un endomorfismo *de A es un homomorfismo de un anillo de A en sí mismo. Un* isomorfismo de anillos *es un homomorfismo de anillos biyectivo. Dos anillos A y B se dice que son* isomorfos *si existe un isomorfismo entre ellos. Esto se denota poniendo $A \cong B$.*

En la definición anterior hemos usado el mismo símbolo para las operaciones y los neutros en los dos anillos que intervienen. Por ejemplo, para calcular $f(x+y)$ primero hay que sumar x con y en A y luego aplicarle f al resultado, mientras que en $f(x)+f(y)$ primero hay que calcular las imágenes de x e y por f y luego hay que sumar éstas en B. Usualmente el contexto hace evidente a qué operación o a qué neutro nos referimos en cada caso, así que mantendremos estos abusos de notación y dejaremos que el lector analice cada caso. Análogamente, las unidades de la ecuación $f(1) = 1$ están en dos anillos probablemente diferentes y por tanto son objetos distintos, que sin embargo denotamos igual.

Dos anillos isomorfos son esencialmente iguales pues el isomorfismo traspasará de uno a otro cualquier propiedad que dependa de la definición de anillo.

A continuación establecemos ciertas propiedades elementales de los homomorfismos de anillos. Demostramos algunas y dejamos el resto como ejercicio para el lector.

Proposición 1.10 *Sea $f : A \to B$ un homomorfismo de anillos. Entonces se verifican las siguientes propiedades para $a, b, a_1, \ldots, a_n \in A$:*

(1) (f conserva ceros) $f(0) = 0$.

(2) (f conserva opuestos) $f(-a) = -f(a)$.

(3) (f conserva restas) $f(a - b) = f(a) - f(b)$.

(4) (f conserva sumas finitas) $f(a_1 + \cdots + a_n) = f(a_1) + \cdots + f(a_n)$.

(5) (f conserva múltiplos enteros) *Si* $n \in \mathbb{Z}$ *entonces* $f(na) = nf(a)$.

(6) (f conserva inversos) *Si* a *es invertible, entonces* $f(a)$ *es invertible y* $f(a)^{-1} = f(a^{-1})$.

(7) (f conserva productos finitos) $f(a_1 \cdots a_n) = f(a_1) \cdots f(a_n)$.

(8) Si A_1 *es un subanillo de* A*, entonces* $f(A_1)$ *es un subanillo de* B.

(9) Si B_1 *es un subanillo de* B*, entonces* $f^{-1}(B_1)$ *es un subanillo de* A.

(10) Si f *es un isomorfismo de anillos entonces* f^{-1} *es un isomorfismo.*

Demostración. Para ver (1) basta con aplicar la propiedad de cancelación a la igualdad $0 + f(0) = f(0+0) = f(0) + f(0)$. (2) se tiene porque $f(a) + f(-a) = f(a + (-a)) = f(0) = 0$, y entonces (3) es claro. (4) se demuestra por inducción; el caso $n = 2$ no es más que la definición de homomorfismo y el caso general se reduce a éste notando que $a_1 + \cdots + a_n = (a_1 + \cdots + a_{n-1}) + a_n$. ∎

Observación 1.11 En la Proposición 1.10 hemos visto que la conservación de sumas implica la conservación del neutro para la suma, pero no hemos podido adaptar la demostración al caso de productos (¿por qué?); de hecho veremos ejemplos de aplicaciones entre anillos que conservan sumas y productos pero no identidades.

Ejemplos 1.12 *Homomorfismos de anillos.*

(1) Si A y B son anillos, la aplicación $f : A \to B$ dada por $f(a) = 0$ para cada $a \in A$ *no* es un homomorfismo de anillos salvo que $B = 0$. Si $B = 0$ entonces este homomorfismo se llama *homomorfismo cero* u *homomorfismo trivial*. Obsérvese que no hay ningún homomorfismo $0 \to B$, salvo que B sea 0.

(2) Sea A un un anillo con un subanillo B. Entonces la aplicación de inclusión $u : B \hookrightarrow A$, dada por $u(b) = b$, es un homomorfismo. En particular, la aplicación identidad $1_A : A \to A$ es un homomorfismo.

(3) Si A es un anillo, la aplicación $\mu : \mathbb{Z} \to A$ dada por $\mu(n) = n1$ (es decir, la aplicación consistente en multiplicar por 1) es un homomorfismo de anillos. De hecho, es el único homomorfismo de anillos $f : \mathbb{Z} \to A$ (¿por qué es el único?).

(4) Si A y B son anillos, la aplicación $p_A : A \times B \to A$ dada por $p_A(a, b) = a$ es un homomorfismo llamado *proyección en la primera coordenada*, y de modo análogo se tiene una proyección en la segunda coordenada.

Dado un producto arbitrario de anillos, debe estar claro cómo se generaliza este ejemplo para definir la proyección en cada coordenada.

(5) Dados $a, b \in \mathbb{R}$, el *conjugado* del número complejo $z = a + bi$ es $\bar{z} = a - bi$, y la aplicación *conjugación* $\mathbb{C} \to \mathbb{C}$ dada por $z \mapsto \bar{z}$ es un homomorfismo de anillos.

Análogamente, si d es un entero que no sea un cuadrado entonces el conjugado $a - b\sqrt{d}$ de $a + b\sqrt{d}$ (elementos de $\mathbb{Q}[\sqrt{d}]$ o de $\mathbb{Z}[\sqrt{d}]$) está bien definido y la conjugación $\mathbb{Q}[\sqrt{d}] \to \mathbb{Q}[\sqrt{d}]$ ó $\mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ es un homomorfismo de anillos.

(6) Sea A un anillo y sea $b \in A$. Entonces la aplicación

$$\begin{array}{ccc} A[X] & \stackrel{S_b}{\to} & A \\ P = a_0 + a_1X + \cdots + a_nX^n & \mapsto & P(b) = a_0 + a_1b + \cdots + a_nb^n \end{array}$$

es un homomorfismo de anillos llamado *homomorfismo de sustitución* en b. En particular, el homomorfismo de sustitución en 0 lleva cada polinomio a su coeficiente independiente.

Problemas

1.4.1 Demostrar los apartados de la Proposición 1.10 que se han dejado para el lector.

1.4.2 Demostrar que la composición de dos homomorfismos de anillos es un homomorfismo de anillos.

1.4.3 Demostrar que la relación "ser isomorfos" en la clase de los anillos es de equivalencia.

1.4.4 Sean $f_1 : A \to B_1$ y $f_2 : A \to B_2$ dos homomorfismos de anillos. Demostrar la aplicación $f_1 \times f_2 : A \to B_1 \times B_2$ dada por $(f_1 \times f_2)(a) = (f_1(a), f_2(a))$ es el único homomorfismo de anillos tal que $\pi_{B_i} \circ (f_1 \times f_2) = f_i$ para $i = 1, 2$. Demostrar que $(f_1, f_2) \mapsto f_1 \times f_2$ define una biyección $\mathrm{Hom}(A, B_1) \times \mathrm{Hom}(A, B_2) \to \mathrm{Hom}(A, B_1 \times B_2)$.

1.4.5 Sea $f : A \to B$ un homomorfismo de anillos y sea $b \in B$.

(1) Demostrar que la aplicación $f_b : A[X] \to B$ dada por $f_b(a_0 + a_1X + \cdots + a_nX^n) = f(a_0) + f(a_1)b + \ldots f(a_n)b^n$ es el único homomorfismo de anillos $A[X] \to B$ que extiende f asocia X con b.

(2) Demostrar que la siguiente aplicación es biyectiva:

$$\begin{array}{ccc} \mathrm{Hom}(A, B) \times B & \to & \mathrm{Hom}(A[X], B) \\ (f, b) & \mapsto & f_b \end{array}$$

1.5 Ideales y anillos cociente

Definición 1.13 *Un subconjunto I de A es un* ideal *si no es vacío y si, dados $x, y \in I$ y $a \in A$ se verifica que $x + y$ y ax están en I.*

En la definición podemos sustituir la condición $I \neq \emptyset$ por la condición $0 \in I$, ya que si $a \in I$ entonces $0 = a + (-1)a \in I$. Por otro lado está claro que si I es ideal de A entonces $\sum_{i=1}^{n} a_i x_i \in I$ para todo $a_1, \ldots, a_n \in A$ y $x_1, \ldots, x_n \in I$.

Ejemplos 1.14 *Ideales.*

(1) Si A es un anillo arbitrario entonces $\{0\}$ y A son ideales de A, el primero se llama *ideal cero* o *trivial* de A y lo denotaremos a partir de ahora por 0; el segundo se llama *ideal impropio* (en oposición a *ideales propios*, para los demás).

(2) Si A es un anillo, el conjunto

$$bA = (b) = \{ba : a \in A\}$$

es un ideal de A llamado *ideal principal generado por* b. Es fácil demostrar que todos los ideales de $\mathbb{Z}$ son de esta forma. Esto no es cierto en general, como pronto veremos. Obsérvese que bA es el menor ideal de A que contiene a b. Obsérvese también que $(1) = A$ y que $(0) = 0$[3].

(3) Más generalmente, si T es un subconjunto de un anillo, entonces el conjunto

$$(T) = \left\{ \sum_{i=1}^{n} a_i t_i : n \in \ a_i \in A, t_i \in X \right\}$$

es un ideal, llamado *ideal generado* por T.

(4) Si A y B son dos anillos entonces $A \times 0 = \{(a, 0) : a \in A\}$ es un ideal de $A \times B$.

(5) Sea $A[X]$ el anillo de los polinomios con coeficientes en un anillo. Es fácil ver que el conjunto formado por los polinomios sin coeficiente independiente, es decir

$$\{a_1 X + \ldots + a_n X^n \in A[X] : a_1, \ldots, a_n \in A\},$$

es un ideal de $A[X]$.

También es sencillo ver que si I es un ideal de A entonces el conjunto

$$J = \{a_0 + a_1 X + \ldots + a_n X^n \in A[X] : a_0 \in I\}$$

de los polinomios con coeficiente independiente en I es un ideal de $A[X]$. Otro ideal de $A[X]$ es $I[X] = \{a_0 + a_1 X + \cdots + a_n X^n : a_0, a_1, \ldots, a_n \in I\}$.

Proposición 1.15 *Todos los ideales de* $\mathbb{Z}$ *son principales.*

Demostración. Sea I un ideal de $\mathbb{Z}$. Si $I = 0$ entonces $I = (0)$ con lo que I es principal. Supongamos que $I \neq 0$ y sea $n \in I \setminus 0$. Entonces $-n \in I$, con lo que I tiene un elemento positivo, o sea $I \cap \mathbb{N} \neq \emptyset$. Como $\mathbb{N}$ está bien ordenado, I tiene un mínimo que denotamos como a. Como $a \in I$ se tiene que $(a) \subseteq I$. Para ver que se da la igualdad tomamos $b \in I$ y sean q y r el cociente y el resto de la división entera de b entre a. Entonces $b = qa + r$ y $0 \leq r < a$. Pero $r = b - qa \in I$, por que I es un ideal de $\mathbb{Z}$ que contiene a a y b y $q \in \mathbb{Z}$. Como r es estrictamente menor que a y a es mínimo en $I \cap \mathbb{N}$, necesariamente $r \notin \mathbb{N}$, es decir r no es positivo. Luego $r = 0$, con lo que $b = qa \in (a)$. ∎

[3]Obsérvese que en este ejemplo y en el siguiente estamos usando que suponeos que todos los anillos son conmutativos.

Definición 1.16 *Sea I un ideal de un anillo A. Decimos que dos elementos $a, b \in A$ son* congruentes módulo I*, y escribimos $a \equiv b \bmod I$, si su diferencia está en I; o sea:*

$$a \equiv b \bmod I \Leftrightarrow b - a \in I.$$

Lema 1.17 *Si A es un anillo, I es un ideal de A y $a, b, c, d \in A$, entonces:*

(1) $a \equiv a \bmod I$

(2) Si $a \equiv b \bmod I$*, entonces* $b \equiv a \bmod I$.

(3) Si $a \equiv b \bmod I$ *y* $b \equiv c \bmod I$*, entonces* $a \equiv c \bmod I$.

(4) $a \equiv b \bmod (0)$ *si y solo si* $a = b$.

Del Lema 1.17 se deduce que la relación "ser congruente módulo I" es una relación de equivalencia en A y, por tanto, las clases de equivalencia por esta relación definen una partición de A. La clase de equivalencia que contiene a un elemento $a \in A$ es

$$a + I = \{a + x : x \in I\}$$

(en particular $0 + I = I$), de modo que

$$a + I = b + I \Leftrightarrow a \equiv b \bmod I$$

(en particular $a + I = 0 + I \Leftrightarrow a \in I$). El conjunto de las clases de equivalencia se denota

$$A/I = \frac{A}{I} = \{a + I : a \in A\}.$$

Proposición 1.18 *Sea A un anillo con un ideal I. Las operaciones suma y producto en A/I dadas por*

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I) \cdot (b + I) = (ab) + I$$

están bien definidas y dotan a A/I de una estructura de anillo con neutro $0+I$ y unidad $1+I$. Este anillo se llama anillo cociente *de A módulo I.*

La proyección *(o* proyección canónica*) $\pi : A \to A/I$, dada por $\pi(a) = a + I$, es un homomorfismo de anillos.*

Demostración. Supongamos que $a + I = a' + I$ y $b + I = b' + I$ con $a, a', b, b' \in A$. Entonces $a - a', b - b' \in I$ y por tanto $(a + b) - (a' + b') = (a - a') + (b - b') \in I$ y $ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' \in I$, pues I es un ideal de A. Esto demuestra que las operaciones están bien definidas. El resto de la proposición se deja como ejercicio. ∎

Al hacer el cociente de un anillo A por un ideal I, elementos que eran distintos en A "pasan a ser iguales" en el cociente (estrictamente hablando, son sus clases de equivalencia las que se hacen iguales); en particular, los elementos de I "se hacen cero". En muchas de las ocasiones en las que se construyen estructuras cociente eso es precisamente lo que se busca, identificar entre sí o anular ciertos elementos.

Ejemplos 1.19 *Anillos cociente.*

(1) Sea n un entero positivo. El anillo cociente del anillo $\mathbb{Z}$ por el ideal (n) se denota $\mathbb{Z}_n$ y la notación $a \equiv b \bmod (n)$ se suele simplificar como $a \equiv b \bmod n$. Si $a \in \mathbb{Z}$ y r es el resto de dividir a entre n entonces $a \equiv r \bmod n$. Esto muestra que $\mathbb{Z}_n$ tiene exactamente n elementos, más concretamente las clases de $0, 1, \ldots, n-1$. Además si $a, b \in \mathbb{Z}$ y r y s son los restos de dividir $a+b$ y ab entre n, respectivamente, entonces

$$(a+(n))+(b+(n)) = r+(n) \quad \text{y} \quad (a+(n))(b+(n)) = s+(n).$$

(2) $A/0$ es el propio anillo A, mientras que $A/A = 0$.

(3) Consideremos el ideal I del anillo de polinomios $A[X]$ formado por los polinomios con coeficiente independiente 0 (ver los Ejemplos 1.14). Como todo polinomio es congruente módulo I con su coeficiente independiente (visto como polinomio), no es difícil convencerse de que la composición de la inclusión $A \to A[X]$ con la proyección $\pi : A[X] \to A[X]/(X)$ es un isomorfismo por tanto $A \cong A[X]/(X)$.

(4) Sean A y B anillos e $I = A \times 0$. Como $(a, b) \equiv (0, b) \bmod I$ la aplicación $b \to (0, b) + I$ es un isomorfismo $B \to (A \times B)/I$. esencialmente iguales (isomorfos).

Lema 1.20 *Sea A un anillo. Un elemento b de A es invertible si y sólo si $(b) = A$. Por tanto, las siguientes condiciones son equivalentes para un ideal I de A.*

(1) I es impropio; es decir, $I = A$.

(2) $1 \in I$.

(3) I contiene una unidad de A; es decir, $I \cap A^* \neq \emptyset$.

Hemos visto que, si $f : A \to B$ es un homomorfismo de anillos, entonces $f(A)$ es un subanillo de B, y es evidente que f es suprayectivo precisamente cuando $f(A) = B$. Más generalmente, podemos decir que cuanto mayor es $f(A)$ más cerca está f de ser suprayectivo. En el otro extremo, $f^{-1}(0)$ es un ideal de A que nos va a servir para determinar si f es o no inyectivo.

Definición 1.21 *Sea $f : A \to B$ un homomorfismo de anillos; llamamos* imagen *y* núcleo *de f, respectivamente, a los conjuntos*

$$\text{Im } f = f(A) = \{f(a) : a \in A\} \qquad y \qquad \text{Ker } f = f^{-1}(0) = \{a \in A : f(a) = 0\}$$

(la notación para el núcleo procede de la voz germánica Kernel*). En general* Im f *es un subanillo de B y* Ker f *es un ideal de A.*

Proposición 1.22 *Un homomorfismo de anillos $f : A \to B$ es inyectivo si y solo si* Ker $f = 0$.

Demostración. Si f es inyectivo, entonces $f^{-1}(a)$ tiene a lo sumo un elemento, para todo $a \in A$. En particular Ker $f = f^{-1}(0)$ tiene exactamente un elemento, a saber 0.

Recíprocamente, supongamos que Ker $f = 0$ y sean $a, b \in A$ tales que $a \neq b$. Entonces $f(a) - f(b) = f(a - b) \neq 0$; es decir, $f(a) \neq f(b)$, y por tanto f es inyectiva. ∎

El siguiente resultado describe los ideales de un anillo cociente. Consideramos la proyección canónica $\pi : A \to A/I$. La imagen por π de un subconjunto J de A es

$$\pi(J) = \{a + I : a \in J\}.$$

Si J contiene a I, denotaremos este conjunto por J/I.

Teorema 1.23 (Teorema de la Correspondencia) *Si I es un ideal de un anillo A, las asignaciones $J \mapsto J/I$ y $X \mapsto \pi^{-1}(X)$ definen aplicaciones biyecciones (una inversa de la otra) que conservan la inclusión entre el conjunto de los ideales de A que contienen a I y el conjunto de todos los ideales de A/I.*

Demostración. Hay que comprobar los siguientes puntos, cosa que el lector podrá hacer como ejercicio:

- Si J es un ideal de A que contiene a I entonces J/I es un ideal de A/I y $\pi^{-1}(J/I) = J$.
- Si X es un ideal de A/I entonces $\pi^{-1}(X)$ es un ideal de A que contiene a I y $\pi^{-1}(X)/I = X$.
- Si $J \subseteq K$ son ideales de A que contienen a I entonces $J/I \subseteq K/I$.
- Si $X \subseteq Y$ son ideales de A/I entonces $\pi^{-1}(X) \subseteq \pi^{-1}(Y)$.

∎

Problemas

1.5.1 Demostrar el Lema 1.17 y las Proposiciones 1.18 y 1.20.

1.5.2 Demostrar además que si n y m son dos número enteros entonces $(n) \subseteq (m)$ si y solo si $m \mid n$.

1.5.3 Si n es un entero positivo, demostrar que los ideales de $\mathbb{Z}_n$ son precisamente los de la forma $m\mathbb{Z}_n$, donde m es un divisor positivo de n, y además $m\mathbb{Z}_n$ está contenido en $m'\mathbb{Z}_n$ si y solo si m' divide a m.

1.5.4 Sea $f : A \to B$ un homomorfismo de anillos. Demostrar que si I es un ideal de B, entonces $f^{-1}(I)$ es un ideal de A. Demostrar que si I es un ideal de A y f es suprayectiva, entonces $f(I)$ es un ideal de B. Dar un ejemplo de un homomorfismo de anillos $f : A \to B$ en el que la imagen por f de un ideal de A no sea ideal de B.

1.5.5 Sean A y B dos anillos. Describir los ideales de $A \times B$ en función de los ideales de A y de B. Determinar todos los ideales de $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$.

1.5.6 Demostrar que si p y q son dos primos distintos entonces no hay ningún homomorfismos de $\mathbb{Z}_p$ a $\mathbb{Z}_q$ ni de $\mathbb{Z}_q$ a $\mathbb{Z}_p$. ¿Cuántos homomorfismos hay de Z_4 a $\mathbb{Z}_2$? ¿Y de $\mathbb{Z}_2$ a $\mathbb{Z}_4$?

1.5.7 Demostrar que si $f : A \to B$ es un homomorfismo suprayectivo de anillos y todos los ideales del anillo A son principales entonces todos los ideales de B son principales.

1.5.8 Sea $f : A \to B$ un homomorfismo suprayectivo de anillos. Demostrar que existe una correspondencia biunívoca, que conserva la inclusión, entre el conjunto de los ideales de B y los ideales de A que contienen a Ker f.

1.5.9 Sea X un conjunto y $*$ una operación en X. Una *congruencia* en X con respecto a $*$ es una relación de equivalencia $\sim$ en X que verifique la siguiente condición para todo $a, a', b, b' \in X$:

$$a \sim a' \quad \text{y} \quad b \sim b' \quad \Rightarrow \quad a * b \sim a' * b'.$$

En tal caso definimos la siguiente operación $*$ en el conjunto cociente $X/\sim$, donde $\overline{a}$ denota la clase de equivalencia en $X/\sim$ que contiene a a:

$$\overline{a} * \overline{b} = \overline{a * b}.$$

Demostrar las siguientes propiedades para $\sim$ una congruencia en X con respecto a $*$:

(1) Si $(X, *)$ es un semigrupo entonces $(X/\sim, *)$ es un semigrupo y si además $(X, *)$ es un monoide o un grupo entonces $(X/\sim, *)$ también lo es.

(2) Si A es un anillo y $\sim$ es una relación de equivalencia en A entonces $\sim$ es una congruencia respecto de la suma y el producto de A si y solo si el conjunto $I = \{a \in A : a \sim 0\}$ es un ideal de A y $\sim$ es la relación de equivalencia "ser congruentes módulo I".

1.6 Operaciones con ideales

Sea A un anillo. Recordemos que si X es un subconjunto de A entonces llamamos *ideal* de A *generado* por X al menor ideal de A que contiene a A y que

$$(X) = \left\{ \sum_{i=1}^{n} a_i x_i : n \geq 0, a_i \in A, x_i \in X \right\}.$$

Es fácil ver que la intersección de una familia de ideales de A es un ideal de A. Eso implica que (X) es también la intersección de todos los ideales de A.

Si I y J son dos ideales de A entonces la suma y producto de A son los conjuntos

$$\begin{aligned} I + J &= \{x + y : x \in I, y \in J\} \\ IJ &= \{x_1 y_1 + \ldots + x_n y_n : x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J\}. \end{aligned}$$

Más generalmente, si $I_1, \ldots, I_n$ son ideales, entonces la suma de estos ideales es

$$I_1 + \cdots + I_n = \{x_1 + \cdots + x_n : x_1 \in I_1, \ldots, x_n \in I_n\}$$

y el producto $I_1 \cdots I_n$ es el ideal formado por las sumas de productos de la forma $x_1 \cdots x_n$ donde $x_1 \in I_1, \ldots, x_n \in I_n$.

Aún más generalmente, si $\{I_x : x \in X\}$ es una familia de ideales de A entonces

$$\sum_{x \in X} I_x = \left\{ \sum_{x \in X} a_x : a_x \text{ para todo } x \in X \text{ y } a_x = 0 \text{ para casi todo } x \in X \right\}$$

y $\prod_{x \in X} I_x$ es el ideal formado por las sumas de productos de la forma $\prod_{x \in X} a_x$ donde $a_x \in I_x$ para todo $x \in X$ y $a_x = 1$ para casi todo $x \in X$.

Proposición 1.24 *Si $\{I_x : x \in X\}$ es una familia de ideales de un anillo A entonces:*

(1) $\sum_{x \in X} I_x$ es el menor ideal de A que contiene a todos los I_x, o sea el ideal generado por $\cup_{x \in X} I_x$.

(2) Si $I_1, \ldots, I_n$ son ideales de A entonces $I_1 \cdots I_n$ es el menor ideal de A generado por los productos $x_1 \cdots x_n$ con $x_1 \in I_1, \ldots, x_n \in I_n$.

Ejemplos 1.25 *Operaciones con ideales.*

(1) Sean n y m son dos números enteros coprimos y consideremos los ideales (n) y (m) de $\mathbb{Z}$. Claramente $(n)(m) = (nm)$. Entonces, $(n) \cap (m)$ está formado por los números enteros que son múltiplos de n y de m. Esos son precisamente los múltiplos del mínimo común múltiplo de n y m. Por otro lado, $(n) + (m)$ es el menor ideal (d) de $\mathbb{Z}$ que contiene a (n) y (m). De la Proposición 1.15 se deduce que $(d) = (n) + (m)$ si y solo si d divide a n y m y es múltiplo de todos los divisores comunes de n y m. O sea d es el máximo común divisor de n y m. En resumen:

$$(n)(m) = (nm), \quad (n) + (m) = (\text{mcm}(n, m)), \quad (n) + (m) = (\text{mcd}(n, m)).$$

(2) Consideremos ahora el anillo $\mathbb{Z}[X]$ de los polinomios con coeficientes enteros. Entonces $(2) + (X)$ está formado por los polinomios cuyo término principal es par. Vamos a ver que este ideal no es principal. Supongamos por reducción al absurdo que $(2) + (X) = (a)$ para algún $a \in \mathbb{Z}[X]$. Entonces $2 = ab$ para algún polinomio b, lo que implica que $a \in \mathbb{Z}$. Además, como $A \in (2, X)$, necesariamente A es par, lo que implica que $X \notin (a) = (2) + (X)$, una contradicción.

Problemas

1.6.1 Escribir una demostración de la Proposición 1.24.

1.6.2 Si I, J y K son ideales de un anillo A, demostrar que:

(1) $IJ \subseteq I \cap J$.

(2) $I(J \cap K) \subseteq IJ \cap IK$.

(3) $I(JK) = (IJ)K$.

(4) $I(J + K) = IJ + IK$.

(5) $IA = I$.

(6) Si $\mathcal{I}$ denota el conjunto de los ideales de A entonces $(\mathcal{I}, \cap)$ y $(\mathcal{I}, +)$ y $(\mathcal{I}, \cdot)$ son monoides. ¿Qué le falta a $(\mathcal{I}, +, \cdot)$ para ser un anillo?

1.7 Los Teoremas de Isomorfía y Chino de los Restos

Teorema 1.26 (Primer Teorema de Isomorfía) *Sea $f : A \to B$ un homomorfismo de anillos. Entonces existe un único isomorfismo de anillos $\bar{f} : A/\mathrm{Ker}\ f \to \mathrm{Im}\ f$ que hace conmutativo el diagrama*

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ A/\mathrm{Ker}\ f & \overset{\bar{f}}{\dashrightarrow} & \mathrm{Im}\ f \end{array}$$

es decir, $i \circ \bar{f} \circ p = f$, donde i es la inclusión y p es la proyección. En particular

$$\frac{A}{\mathrm{Ker}\ f} \simeq \mathrm{Im}\ f.$$

Demostración. Sean $K = \mathrm{Ker}\ f$ e $I = \mathrm{Im}\ f$. La aplicación $\bar{f} : A/K \to I$ dada por $\bar{f}(x + K) = f(x)$ está bien definida (no depende de representantes) pues si $x + K = y + K$ entonces $x - y \in K$ y por lo tanto $f(x) - f(y) = f(x - y) = 0$; es decir, $f(x) = f(y)$. Además es elemental ver que es un homomorfismo de anillos y que es suprayectiva. Para ver que es inyectiva usamos la Proposición 1.22: si $x + K$ está en el núcleo de $\bar{f}$ entonces $0 = \bar{f}(x + K) = f(x)$, de modo que $x \in K$ y así $x + K = 0 + K$. Es decir $\mathrm{Ker}\ \bar{f} = 0$ y por lo tanto $\bar{f}$ es inyectiva. En conclusión, $\bar{f}$ es un isomorfismo, y hace conmutativo el diagrama porque, para cada $x \in K$, se tiene

$$i(\bar{f}(p(x))) = \bar{f}(x + K) = f(x).$$

En cuanto a la unicidad, supongamos que otro homomorfismo $\widehat{f} : A/K \to I$ verifica $i \circ \widehat{f} \circ p = f$; entonces para cada $x \in K$ se tiene $\widehat{f}(x + K) = i(\widehat{f}(p(x))) = f(x) = \bar{f}(x + K)$, y por lo tanto $\widehat{f} = \bar{f}$. ∎

Teorema 1.27 (Segundo Teorema de Isomorfía) *Sea A un anillo y sean I y J dos ideales tales que $I \subseteq J$. Entonces J/I es un ideal de A/I y existe un isomorfismo de anillos*

$$\frac{A/I}{J/I} \simeq \frac{A}{J}.$$

Demostración. Por el Teorema de la Correspondencia 1.23, J/I es un ideal de A/I. Sea $f : A/I \to A/J$ la aplicación definida por $f(a+I) = a+J$. Es elemental ver que f está bien definida, que es un homomorfismo suprayectivo de anillos y que Ker $f = J/I$. Entonces el isomorfismo buscado se obtiene aplicando el Primer Teorema de Isomorfía a f. ∎

Teorema 1.28 (Tercer Teorema de Isomorfía) *Sea A un anillo con un subanillo B y un ideal I. Entonces:*

(1) $B \cap I$ es un ideal de B.

(2) $B + I$ es un subanillo de A que contiene a I como ideal.

(3) Se tiene un isomorfismo de anillos $\dfrac{B}{B \cap I} \simeq \dfrac{B+I}{I}$.

Demostración. Los dos primeros apartados se dejan como ejercicio. En cuanto al último, sea $f : B \to A/I$ la composición de la inclusión $j : B \to A$ con la proyección $p : A \to A/I$. Es claro que Ker $f = B \cap I$ y que Im $f = (B+I)/I$, por lo que el resultado se sigue del Primer Teorema de Isomorfía. ∎

Ejemplos 1.29 *Aplicaciones del Primer Teorema de Isomorfía.*

(1) Si A y B son anillos, el homomorfismo $A \times B \to A$ de proyección en la primera componente es suprayectivo y tiene núcleo $I = 0 \times B$, por lo que $\frac{A \times B}{0 \times B} \simeq A$. En realidad ya habíamos visto esto en el Ejemplo 1.19.(4).

(2) Si A es un anillo, el homomorfismo $f : A[X] \to A$ de sustitución en 0 (dado por $a_0 + a_1X + \cdots \mapsto a_0$) es suprayectivo y tiene por núcleo el ideal (X) generado por X (consistente en los polinomios con coeficiente independiente nulo), de modo que $A[X]/(X) \simeq A$, como ya habíamos observado en el Ejemplo 1.19.(3).

(3) Sean A un anillo e I un ideal de A. Para cada $a \in A$, sea $\overline{a} = a + I$. La aplicación $f : A[X] \to (A/I)[X]$ dada por $f(a_0 + a_1X + \cdots + a_nX^n) = \overline{a}_0 + \overline{a}_1X + \cdots + \overline{a}_nX^n$ es un homomorfismo suprayectivo de anillos cuyo núcleo es $I[X] = \{a_0 + a_1X + \cdots + a_nX^n : a_i \in I\}$. Del Primer Teorema de Isomorfía se deduce que $(A/I)[X] \simeq A[X]/I[X]$.

Definición 1.30 *Sea A un anillo, y recordemos que si $n \in \mathbb{Z}^+$ escribimos $n1 = 1 + \cdots + 1$ (n veces). Si existe $n \in \mathbb{Z}^+$ tal que $n1 = 0$, definimos la* característica *de A como el menor $n \in \mathbb{Z}^+$ que verifica tal igualdad. Si no existe un tal n, decimos que la característica de A es* 0.

Proposición 1.31 *Sea A un anillo A y sea $f : \mathbb{Z} \to A$ el único homomorfismo de anillos (dado por $f(n) = n1$). Para un número natural n las condiciones siguientes son equivalentes:*

(1) n es la característica de A.

(2) $n\mathbb{Z}$ es el núcleo de f.

(3) El subanillo primo de A es isomorfo a $\mathbb{Z}_n$ (recuérdese que $\mathbb{Z}_0 = \mathbb{Z}$ y $\mathbb{Z}_1 = 0$).

(4) A contiene un subanillo isomorfo a $\mathbb{Z}_n$.

Demostración. La equivalencia entre (1) y (2) se deja como ejercicio para el lector, y es obvio que (3) implica (4).

(2) implica (3). Se obtiene aplicando el Primer Teorema de Isomorfía y observando que Im f es el subanillo primo de A.

(4) implica (2). Si B es un subanillo de A y $g : \mathbb{Z}_n \to B$ es un isomorfismo, considerando la proyección $\pi : \mathbb{Z} \to \mathbb{Z}_n$ y la inclusión $u : B \hookrightarrow A$ se obtiene un homomorfismo de anillos $u \circ g \circ \pi : \mathbb{Z} \to A$ que debe coincidir con f por su unicidad (Ejemplo 1.12.(3)). Como $u \circ g$ es inyectiva, es elemental ver que Ker $f = n\mathbb{Z}$. ∎

Teorema 1.32 (Teorema Chino de los Restos) *Sea A un anillo y sean $I_1, \ldots, I_n$ ideales de A tales que $I_i + I_j = A$ para todo $i \neq j$. Entonces $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$. Además*

$$\frac{A}{I_1 \cap \cdots \cap I_n} \simeq \frac{A}{I_1} \times \cdots \times \frac{A}{I_n}.$$

Demostración. Razonamos por inducción sobre n, empezando con el caso $n = 2$. La hipótesis $I_1 + I_2 = A$ nos dice que existen $x_1 \in I_1$ y $x_2 \in I_2$ tales que $x_1 + x_2 = 1$, y entonces para cada $a \in I_1 \cap I_2$ se tiene $a = ax_1 + ax_2 \in I_1 I_2$, de modo que $I_1 \cap I_2 \subseteq I_1 I_2$, y la otra inclusión es clara. Claramente la aplicación $f : A \to A/I_1 \times A/I_2$ dada por $f(a) = (a + I_1, a + I_2)$ es un homomorfismo de anillos con núcleo $I_1 \cap I_2$, y es suprayectiva pues, dado un elemento arbitrario $(a_1 + I_1, a_2 + I_2)$ de $A/I_1 \times A/I_2$, el elemento $a = a_1 x_2 + a_2 x_1$ verifica $f(a) = (a_1 + I_1, a_2 + I_2)$. Ahora el resultado se obtiene aplicando el Primer Teorema de Isomorfía.

En el caso general ($n > 2$) basta ver que las hipótesis implican que $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$, pues entonces la hipótesis de inducción nos da

$$I_1 \cap \cdots \cap I_{n-1} \cap I_n = (I_1 \cap \cdots \cap I_{n-1}) I_n = I_1 \cdots I_{n-1} I_n$$

y

$$\frac{A}{I_1 \cap \cdots \cap I_n} = \frac{A}{(\cap_{i=1}^{n-1} I_i) \cap I_n} \simeq \frac{A}{\cap_{i=1}^{n-1} I_i} \times \frac{A}{I_n} \simeq \frac{A}{I_1} \times \cdots \times \frac{A}{I_{n-1}} \times \frac{A}{I_n}.$$

Para ver que $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$ notemos que, para cada $i \leq n - 1$, existen $a_i \in I_i$ y $b_i \in I_n$ tales que $1 = a_i + b_i$, y multiplicando todas esas expresiones se obtiene

$$1 = \Pi_{i=1}^{n-1}(a_i + b_i) = a_1 \cdots a_{n-1} + b,$$

donde b engloba a todos los sumandos que se obtendrían desarrollando los productos (excepto $a_1 \cdots a_{n-1}$) y está en I_n porque en cada sumando hay al menos un factor del ideal I_n. Como además $a_1 \cdots a_{n-1} \in I_1 \cap \cdots \cap I_{n-1}$, deducimos que $1 \in (I_1 \cap \cdots \cap I_{n-1}) + I_n$ y así $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$, como queríamos ver. ∎

Problemas

1.7.1 Sea $a \in \mathbb{R}$. ¿Qué se deduce al aplicar el Primer Teorema de Isomorfía al homomorfismo $\mathbb{R}[X] \to \mathbb{R}$, dado por $P(X) \mapsto P(a)$? ¿Y qué se deduce al aplicarlo al homomorfismo $\mathbb{R}[X] \to \mathbb{C}$, dado por $P(X) \mapsto P(i)$?

1.7.2 Demostrar el recíproco del Teorema Chino de los Restos para anillos; es decir, probar que si $I_1, \ldots, I_n$ son ideales de un anillo A tales que la aplicación $f : A \to \prod_{i=1}^{n} A/I_i$, dada por $f(a) = (a + I_1, \ldots, a + I_n)$ es suprayectiva, entonces $I_i + I_j = (1)$, para todo $i \neq j$.

1.7.3 Sean $f : A \to B$ un homomorfismo de anillos, J un ideal de B e $I = f^{-1}(I)$. Demostrar

(1) Existe un único homomorfismo $\bar{f} : A/I \to B/J$ que hace conmutativo el siguiente diagrama, donde π_I y π_J son los homomorfismos canónicos

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ {\scriptstyle \pi_I}\downarrow & & \downarrow{\scriptstyle \pi_J} \\ A/I & \overset{\bar{f}}{\dashrightarrow} & B/J \end{array}$$

(2) $\overline{f}$ es inyectivo.

(3) A/I y $(f(A) + J)/J$ son anillos isomorfos.

1.7.4 Sea A un anillo de característica n y sea m un número entero. ¿Cuántos homomorfismos de anillos $\mathbb{Z}_m \to A$ existen? ¿Cuántos homomorfismos de anillos $\mathbb{Z}_n \to \mathbb{Z}_m$ existen?

Capítulo 2

Divisibilidad en Dominios

En este capítulo suponemos que todos los anillos que aparecen son conmutativos y en ellos $1 \neq 0$.

2.1 Cuerpos y dominios; ideales maximales y primos

Definición 2.1 *Un elemento a de un anillo A se dice* regular *si la relación $ab = ac$ con $b, c \in A$ implica que $b = c$; es decir, si a es cancelable respecto del producto. Claramente, el 0 nunca es regular*[1].

Un cuerpo *es un anillo en el que todos los elementos no nulos son invertibles, y un* dominio *(o* dominio de integridad*) es un anillo en el que todos los elementos no nulos son regulares.*

Un subanillo de un anillo A que sea un cuerpo se llama un subcuerpo *de A, y un homomorfismo de anillos entre dos cuerpos se llama* homomorfismo de cuerpos*.*

Como todo elemento invertible es regular (Lema 1.5), tenemos:

Proposición 2.2 *Todo cuerpo es un dominio.*

Otras propiedades que se demuestran fácilmente quedan recogidas en la siguientes proposición:

Proposición 2.3 *Sea A un anillo.*

(1) Las condiciones siguientes son equivalentes:

- *(a) A es un cuerpo.*
- *(b) Los únicos ideales de A son 0 y A.*
- *(c) Todo homomorfismo de anillos $A \to B$ con $B \neq 0$ es inyectivo.*

(2) Un elemento $a \in A$ es regular si y solo si la relación $ab = 0$ con $b \in A$ implica $b = 0$ (por este motivo, los elementos no regulares se suelen llamar divisores de cero*).*

(3) A es un dominio si y solo si, para cualesquiera $a, b \in A$ no nulos, se tiene $ab \neq 0$.

[1] Obsérvese la importancia de la hipótesis $1 \neq 0$ en este caso.

(4) Todo subanillo de un dominio es un dominio.

(5) La característica de un dominio es cero o un número primo.

Demostración. (1) Supongamos que A es cuerpo e sea I un ideal no nulo de A entonces I tiene un elemento $a \neq 0$. Como A es cuerpo a es invertible, con lo que del Lema 1.20 deducimos que $I = A$. Supongamos ahora que A no es cuerpo y sea a un elemento no invertible de A diferente de 0. Entonces $0 \neq (a) \neq A$. Esto demuestra que (a) y (b) son equivalentes.

Si $f : A \to B$ es un homomorfismo de anillos y $B \neq 0$ entonces $f(1_A) = 1_B \neq 0$, con lo que $\ker f \neq A$. Por tanto si los únicos ideales de A son 0 y A entonces $\ker f = 0$, con lo que f es inyectivo por Proposición 1.22. Sin embargo si I es un ideal de A que no es ni 0 ni A entonces el homomorfismo canónico $A \to A/I$ no es inyectivo y $A/I \neq 0$. Esto demuestra que (b) y (c) son equivalentes.

(2) Supongamos que a es regular y que $ab = 0$. Entonces $ab = a0$ y por tanto $b = 0$. Sin embargo si a no es regular existen elementos distintos b y c de A con $ab = ac$. Entonces $a(b - c) = ab - ac = 0$.

(3) es consecuencia inmediata de (2).

(4) es obvio. ∎

Ejemplos 2.4 *Dominios y cuerpos.*

(1) Los anillos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos y $\mathbb{Z}$ es un dominio que no es un cuerpo (aunque es subanillo de un cuerpo).

(2) Para $n \geq 2$, el anillo $\mathbb{Z}_n$ es un dominio si y solo si es un cuerpo, si y sólo si n es primo (¿por qué?).

(3) Si m es un entero que no es el cuadrado de un número entero entonces $\mathbb{Z}[\sqrt{m}]$ es un dominio (subanillo de $\mathbb{C}$) que no es un cuerpo (el 2 no tiene inverso). Sin embargo, $\mathbb{Q}[\sqrt{m}]$ sí que es un cuerpo; de hecho, si $a+b\sqrt{m} \neq 0$, entonces $q = (a+b\sqrt{m})(a-b\sqrt{m}) = a^2-b^2m$ es un número racional no nulo (¿por qué?) y $aq^{-1} - bq^{-1}\sqrt{m}$ es el inverso de $a + b\sqrt{m}$.

(4) Un producto de anillos diferentes de 0 nunca es un dominio, pues $(1, 0)(0, 1) = (0, 0)$.

(5) Los anillos de polinomios no son cuerpos, pues la indeterminada genera un ideal propio y no nulo. Por otra parte, $A[X]$ es un dominio si y solo si lo es A. Una implicación es clara, pues A es un subanillo de $A[X]$. Para ver la otra obsérvese que si P es un polinomio de grado n y Q es un polinomio de grado m entonces tenemos $P = a_0 + a_1X + \cdots + a_nX^n$ y $Q = b_0 + b_1X + \cdots + b_mX^m$ con $a_n \neq 0$ y $b_m \neq 0$. Si A e dominio entonces el coeficiente de X^{n+m} en PQ es a_nb_m que si A es dominio no es 0.

Definición 2.5 *Sean A un anillo e I un ideal propio de A.*
Se dice que I es maximal *si no está contenido en ningún ideal propio (excepto en sí mismo).*
Se dice que I es primo *si, para todo $a, b \in A$, la relación $ab \in I$ implica $a \in I$ ó $b \in I$.*

Proposición 2.6 *Sean A un anillo e I un ideal propio de A. Entonces:*

(1) I es maximal si y solo si A/I es un cuerpo.

(2) I es primo si y solo si A/I es un dominio.

(3) Si I es maximal entonces es primo.

(4) A es un cuerpo si y solo si el ideal 0 es maximal.

(5) A es un dominio si y solo si el ideal 0 es primo.

Demostración. El apartado (1) es consecuencia inmediata de la Proposición 2.3.(1) y del Teorema de la Correspondencia (Teorema 1.23). Para demostrar (2), supongamos que I es primo y sean $a+I, b+I$ dos elementos no nulos de A/I; entonces $a, b \notin I$ y por lo tanto $ab \notin I$, luego $(a+I)(b+I) = ab + I \neq 0$ y en consecuencia A/I es un dominio. El recíproco se demuestra usando la misma idea, y el resto de apartados se deducen de estos dos y de la Proposición 2.2. ∎

Ejemplo 2.7 De la Proposición 1.15 sabemos que todos los ideales de $\mathbb{Z}$ son principales. Además si n y m son enteros entonces $(n) \subseteq (m)$ si y solo si m divide a n. Por tanto, (n) es un ideal maximal de $\mathbb{Z}$ si y solo si $n \notin \{0, 1, -1\}$ y los únicos divisores de n son ± 1 y $\pm n$, o sea si n es un número primo. En tal caso (n) es ideal primo de $\mathbb{Z}$ por la Proposición 2.6.(3). Obsérvese que (0) es un ideal primo de $\mathbb{Z}$ que no es maximal pues $\mathbb{Z}$ es un dominio que no es un cuerpo. Sin embargo si $n \neq 0$ y n no es primo entonces (n) no es un ideal primo de $\mathbb{Z}$, pues o bien $n = \pm 1$ en cuyo caso $(n) = \mathbb{Z}$ o bien $n = ab$ con a y b dos divisores propios de $\mathbb{Z}$, con lo que $ab \in (n)$ pero ni a ni b están en (n).

En resumen, los ideales maximales de $\mathbb{Z}$ son los de la forma (n) con n un número primo y los ideales primos $\mathbb{Z}$ son los de la forma (n) con $n = 0$ o un número primo.

Proposición 2.8 *Todo ideal propio de un anillo está contenido en un ideal maximal.*

Demostración. Sea I un ideal propio de A y sea Ω el conjunto de los ideales propios de A que contienen a I. Obsérvese que la unión de una cadena $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ de elementos de Ω es un ideal, que además es propio, pues si no lo fuera, contendría a 1 y por tanto algún I_n contendría a 1 en contra de que todos los I_n son ideales propios. Aplicando el Lema de Zorn deducimos que Ω tiene un elemento maximal que obviamente es un ideal maximal de A. ∎

Problemas

2.1.1 Sean a y b dos elementos de un anillo. Demostrar que ab es un divisor de cero si y solo si a ó b es un divisor de cero.

2.1.2 Sea A un anillo finito. Demostrar que todo elemento de A es o divisor de cero o unidad. Deducir que todo dominio finito es un cuerpo.

2.1.3 Sea $f : A \to B$ un homomorfismo de anillos. Demostrar que:

(1) Si p es un ideal primo de B, entonces $f^{-1}(p)$ es un ideal primo de A.

(2) En general, no se verifica el resultado análogo para ideales maximales. (Indicación: Considerar la inclusión de $\mathbb{Z}$ en $\mathbb{Q}$.)

2.1.4 Sea I un ideal propio del anillo A. Demostrar que las biyecciones del Teorema de la Correspondencia llevan ideales maximales (respectivamente primos) de A que contienen a I a ideales maximales (respectivamente primos) de A/I, y viceversa.

2.1.5 Demostrar que si D es un dominio entonces su característica es o 0 o un número primo.

2.1.6 Determinar los ideales de $\mathbb{Z}_n$. ¿Cuáles de ellos son primos y cuáles maximales.

2.1.7 Se considera el anillo $A[[X]]$ de series de potencias con coeficientes en un anillo A. Se pide:

(1) Demostrar que $\sum_{i=1}^{\infty} a_i X^i$ es una unidad de $A[[X]]$ precisamente si a_0 es una unidad de A.

(2) Si A es un cuerpo, demostrar que todo ideal de $A[[X]]$ es de la forma (X^n) para algún $n \in \mathbb{N}$.

(3) Demostrar que $A[[X]]$ es un dominio precisamente si A es un dominio.

(4) Identificar los ideales maximales de $A[[X]]$ en función de los ideales maximales de A.

2.1.8 Demostrar que si P es un ideal primo de un anillo A entonces tanto $P[X]$ como

$$P + (X) = \{a_0 + a_1 X + \cdots + a_n X^n : a_0 \in P, a_1, \ldots, a_n \in A\}$$

son ideales primos de $A[X]$. ¿Puede ser $P[X]$ ideal maximal de $A[X]$? ¿Y $P + (X)$?

2.1.9 Demostrar que las siguientes condiciones son equivalentes para un anillo A.

(1) A tiene un único ideal maximal.

(2) A tiene un ideal propio I que contiene todos los elementos no invertibles de A.

(3) El conjunto de los elementos no invertibles de A es un ideal.

(4) Para todo $a, b \in A$, si $a + b$ es invertible, entonces a ó b es invertible.

Un anillo que satisface las condiciones anteriores se dice que es *local*.

2.1.10 Demostrar que los siguientes anillos son locales:

(1) $\mathbb{Z}_{p^n}$, donde p es primo y $n \geq 0$.

(2) A/m^n, donde A es cualquier anillo, m es un ideal maximal y $n \in \mathbb{N}$.

(3) $K[[X]]$, donde K es un cuerpo.

2.1.11 Sea A un anillo cuya característica es un número primo p. Demostrar que la aplicación $x \mapsto x^{p^n}$ es un endomorfismo de A para todo $n \in \mathbb{Z}^{\geq 0}$.

2.1.12 Demostrar que, si K es un cuerpo finito con un subcuerpo F, entonces el cardinal de K es una potencia del cardinal de F. (Indicación: Considerar K como espacio vectorial sobre F). Deducir que:

(1) El cardinal de cualquier cuerpo finito es una potencia de un número primo. (Indicación: Considerar el subanillo primo de K.)

(2) Si K es un cuerpo finito con un subcuerpo F, entonces existen un número primo p y enteros positivos n y m tales que $n \mid m$, $|F| = p^n$ y $|K| = p^m$.

2.1.13 Demostrar que si K es un cuerpo finito entonces 1 y -1 son los únicos elementos de K cuyo cuadrado es 1. Usar esto para demostrar que el producto de todos los elementos no nulos de K es -1 y deducir el Teorema de Wilson: Si p es un número primo entonces $(p-1)! \equiv -1 \bmod p$. Demostrar también el recíproco del Teorema de Wilson: Si n es un entero positivo que cumple $(n-1)! \equiv -1 \bmod n$ entonces n es primo.

2.1.14 Sean I un ideal de un anillo y $p_1, \ldots, p_n$ ideales primos del mismo anillo. Demostrar que si $I \subseteq \cup_{i=1}^{k} p_i$ entonces $I \subseteq p_i$ para algún i.

2.2 Divisibilidad

Recuérdese que estamos suponiendo que todos los anillos son conmutativos y satisfacen $1 \neq 0$.

Sea A un anillo y sean $a, b \in A$. Si existe $c \in A$ tal que $b = ac$ entonces se dice que a *divide* a b en A, o que a es *un divisor* de b en A, o que b es *un múltiplo* de a en A. Para indicar que a divide a b en A escribiremos $a \mid b$ en A. Si el anillo A está claro por el contexto escribiremos simplemente $a \mid b$.

Obsérvese que la noción de divisibilidad depende del anillo. Por ejemplo, si a es un entero diferente de 0, entonces a divide a todos los números enteros en $\mathbb{Q}$, pero no necesariamente en $\mathbb{Z}$.

Lema 2.9 *Si A es un anillo y $a, b, c \in A$ entonces se verifican las siguientes propiedades:*

(1) (Reflexiva) $a \mid a$.

(2) (Transitiva) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

(3) $a \mid 0$ y $1 \mid a$.

(4) $0 \mid a$ si y solo si $a = 0$.

(5) $a \mid 1$ si y solo si a es una unidad; en este caso $a \mid x$ para todo $x \in A$ (es decir, las unidades dividen a cualquier elemento).

(6) Si $a \mid b$ y $a \mid c$ entonces $a \mid rb + sc$ para cualesquiera $r, s \in A$ (y en particular $a \mid b + c$, $a \mid b - c$ y $a \mid rb$ para cualquier $r \in A$). Más generalmente, si a divide a ciertos elementos, entonces divide a cualquier combinación lineal suya con coeficientes en A.

(7) Si c no es divisor de cero y $ac \mid bc$, entonces $a \mid b$.

Demostración. Todas las propiedades son obvias o muy sencillas de demostrar. Demostramos solo la última. Si $ac \mid bc$ entonces $bc = acd$ para algún $d \in A$. Como c no es divisor de cero, o sea es regular, se tiene que $b = ad$ con lo que $a \mid b$. ∎

Definición 2.10 *Dos elementos a y b de un anillo A se dice que son* asociados *en A si se dividen mutuamente en A; es decir, si $a \mid b$ y $b \mid a$ en A. Cuando esté claro por el contexto en qué anillo estamos trabajando, diremos simplemente que a y b son asociados.*

Por ejemplo, una unidad es lo mismo que un elemento asociado a 1.

Es elemental ver que "ser asociados" es una relación de equivalencia en A, y que dos elementos son asociados si y solo si tienen los mismos divisores, si y solo si tienen los mismos múltiplos. Por lo tanto, al estudiar cuestiones de divisibilidad, un elemento tendrá las mismas propiedades que sus asociados.

La siguiente caracterización de la relación "ser asociado" en un dominio será importante (y por motivos como éste pronto empezaremos a suponer sistemáticamente que los anillos que aparecen son dominios):

Lema 2.11 *Si D es un dominio entonces $a, b \in D$ son asociados en D si y solo si existe una unidad u de D tal que $b = au$.*

Demostración. Si $b = au$ con u unidad entonces $a = bu^{-1}$ con lo que $a \mid b$ y $b \mid a$, es decir a y b son asociados. Recíprocamente, supongamos que a y b son asociados. Entonces $b = bu$ y $a = bv$ para ciertos $u, v \in D$. Claramente si a ó b es 0 entonces el otro también es 0, con lo que en este caso $a = b1$. Por otro lado, si a y b son ambos distintos de 0 también lo son u y v con lo que $uv \neq 0$ por ser D un dominio. Como además $auv = bv = a = a1$ y a es cancelable por ser distinto de 0 y D un dominio, deducimos que $uv = 1$ con lo que u es una unidad de D. ∎

En el Problema 3.5.5 se verá un ejemplo de un anillo con dos elementos asociados a y b para los cuales no existe ninguna unidad u en el anillo tal que $b = au$.

Sabemos que cualquier elemento a de un anillo A es divisible por sus asociados y por las unidades de A, y que si a divide a uno de los elementos b ó c entonces divide a su producto bc. A continuación estudiamos los elementos que verifican "los recíprocos" de estas propiedades. A menudo consideraremos elementos a de un anillo A que no son cero ni unidades, lo que sintetizaremos en la forma $0 \neq a \in A \setminus A^*$.

Definición 2.12 *Diremos que un elemento a del anillo A es* irreducible *si $0 \neq a \in A \setminus A^*$ y la relación $a = bc$ en A implica que $b \in A^*$ ó $c \in A^*$ (y por lo tanto que uno de los dos es asociado de a).*

Diremos que a es primo *si $0 \neq a \in A \setminus A^*$ y la relación $a \mid bc$ en A implica que $a \mid b$ ó $a \mid c$.*

Ambas nociones dependen del anillo ambiente, y si éste no está claro por el contexto hablaremos de irreducibles y primos "en A".

Proposición 2.13 *En un dominio A todo elemento primo es irreducible.*

Demostración. Sea p un elemento primo de A y supongamos que $p = ab$, con $a, b \in A$. Entonces p divide a a ó a b. Supongamos que p divide a a y p son asociados. Entonces, Lema 2.11, se tiene que $ab = p = au$ para algún $u \in D^*$. Como D es dominio $b = u$, con lo que b es unidad. Esto demuestra que p es irreducible. ∎

El recíproco no se verifica en general, como muestra el siguiente ejemplo.

Ejemplo 2.14 *Irreducible no implica primo.*
En el anillo $\mathbb{Z}[\sqrt{-5}]$ hay elementos irreducibles que no son primos. Comencemos observando que el cuadrado del módulo de un elemento $a+b\sqrt{-5}$ de $\mathbb{Z}[\sqrt{-5}]$, con $a, b \in \mathbb{Z}$ es $|a+b\sqrt{-5}|^2 = a^2 + 5b^2$. Como además $|xy| = |x|\ |y|$ si $x|y$ en $\mathbb{Z}[\sqrt{-5}]$, entonces $|x|^2$ divide a $|y|^2$ en $\mathbb{Z}$. En particular, si $x = a + b\sqrt{-5}$ y $|x|^2 = 1$ entonces $x = \pm 1$. De aquí deducimos que

$$\mathbb{Z}[\sqrt{-5}]^* = \{x \in \mathbb{Z}[\sqrt{-5}] : |x|^2 = 1\} = \{1, -1\}.$$

Por otro lado los cuadrados en $\mathbb{Z}_5$ son $0 + (5)$ y $\pm 1 + (5)$, y que por lo tanto la congruencia $a^2 \equiv \pm 2 \bmod 5$ no tiene solución. Esto implica que en $\mathbb{Z}[\sqrt{-5}]$ no hay elementos cuyo módulo al cuadrado valga 2, 3 ó 12 (¿por qué?).

Sea ahora $x \in \mathbb{Z}[\sqrt{-5}]$ con $|x|^2 = 4$. Si $y \mid x$ entonces $|y|^2$ divide a $|x|^2 = 4$, en $\mathbb{Z}$ y, por lo tanto, $|y|^2$ vale 1, 2 ó 4: En el primer caso $y \in \mathbb{Z}[\sqrt{-5}]^*$, el segundo es imposible y en el tercero y es asociado de x (¿por qué?), y en consecuencia x es irreducible. De igual modo se ve que los elementos con módulo 6 ó 9 son irreducibles, y en particular lo son todos los factores de la igualdad

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Pero ninguno de ellos es primo: por ejemplo de la igualdad se deduce que $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, y es claro que $2 \nmid (1 + \sqrt{-5})$ y $2 \nmid (1 - \sqrt{-5})$.

Todas las nociones de divisibilidad que hemos presentado pueden enunciarse en términos de los ideales principales generados por los elementos involucrados.

Proposición 2.15 *Si D es un dominio y $a, b \in D$ entonces se verifican las siguientes propiedades:*

(1) $a = 0$ si y solo si $(a) = 0$.

(2) $a \in D^*$ si y solo si $(a) = D$.

(3) $a \mid b$ si y solo si $(b) \subseteq (a)$ (o si $b \in (a)$).

(4) a y b son asociados si y solo si $(a) = (b)$.

(5) a es primo si y solo si (a) es un ideal primo no nulo de D.

(6) a es irreducible si y solo si (a) es maximal entre los ideales principales propios no nulos de D; es decir, $a \neq 0$ y $(a) \subseteq (b) \subset D$ implica $(a) = (b)$.

Definición 2.16 *Sea A un anillo y sean S un subconjunto de A y $a \in A$.*

(1) a es un máximo común divisor *de S en A si a es divisor de cada elemento de S, y múltiplo de cada elemento de A que sea divisor de todos los elementos de S.*

(2) a es un de S en A si a múltiplo de cada elemento de S, y divisor de cada elemento de A que sea múltiplo de todos los elementos de S.

Obsérvese que no hablamos "del" máximo común divisor ni "del" mínimo común múltiplo sino que en ambos casos usamos el artículo indeterminado "un". En la siguiente proposición se precisa por qué tenemos que usar el artículo indeterminado y hasta qué punto "el" máximo común divisor y "el" mínimo común múltiplo son únicos. Sin embargo en ocasiones abusaremos del lenguaje diciendo "el" máximo común divisor o "el" mínimo común múltiplo entendiendo que son conceptos que son "únicos salvo asociados". También abusaremos del lenguaje escribiendo $d = \mathrm{mcd}(S)$ ó $m = \mathrm{mcm}(S)$ significando que d es un máximo común divisor de S en A y que m es un mínimo común múltiplo de S en A, respectivamente.

Proposición 2.17 *Sea A un anillo y sean S un subconjunto de A y $a, b \in A$. Entonces*

(1) a es un máximo común divisor de S en A si y solo si (a) es el menor ideal principal de A que contiene a S. En particular si $(S) = (a)$ entonces a es el máximo común divisor de S.

(2) a es un mínimo común múltiplo de S en A si y solo si (a) es el mayor ideal principal contenido en $\cap_{\mathrm{sin}\, S}(s)$. En particular, si $(a) = \cap_{s \in S}(s)$ entonces a es mínimo común múltiplo de S.

(3) Si a es un máximo común divisor de S entonces b también es máximo común divisor de S si y solo si a y b son asociados en A.

(4) Si a es un mínimo común múltiplo de S entonces b también es máximo común divisor de S si y solo si a y b son asociados en A.

(5) Si a es un divisor común de los elementos de S y $a \in (S)$ entonces $a = \mathrm{mcd}(S)$.

Obsérvese que la condición $a \in (S)$ significa que existen elementos $s_1, \ldots, s_n \in S$ y $a_1, \ldots, a_n \in A$ tales que

$$a = a_1 s_1 + \cdots + a_n s_n. \tag{2.1}$$

En el caso en que $a = \mathrm{mcd}(S)$ se se dice que esta expresión es una identidad de Bezout *para S.*

(6) Se verifica $1 = \mathrm{mcd}(S)$ si y solo si los únicos divisores comunes de los elementos de S son las unidades de A.

(7) Si $(S) = 1$ (o sea, 1 es combinación lineal de elementos de S) entonces $1 = \mathrm{mcd}(S)$.

Demostración. (1) Usando la definición de máximo común divisor y la Proposición 2.15.(3) tenemos que $a = \mathrm{mcd}(S)$ si y sólo si $(s) \subseteq (a)$ para todo $s \in S$ y para todo $b \in A$ se tiene que si $S \subseteq (b)$ entonces $(a) \subseteq (b)$. Esto demuestra que $a = \mathrm{mcd}(S)$ si y sólo si (a) es el menor ideal principal que contiene a S.

(2) se demuestra de forma similar y (3) y (4) son consecuencias evidentes de las definiciones.

(5) Supongamos que a satisface la condición dada y sea b un elemento de A que divide a todos los elementos de S. Entonces divide a $a_1s_1 + \cdots + a_ks_k = a$. Esto demuestra que $a = \mathrm{mcd}(S)$.

(7) es consecuencia inmediata de (5). ∎

Ejemplo 2.18 *Los recíprocos de las propiedades* (5) *y* (7) *no se verifican. Por ejemplo, los únicos divisores comunes de* 2 *y* X *en* $\mathbb{Z}[X]$ *son* 1 *y* -1*, es decir las unidades de* $\mathbb{Z}[X]$*. Por tanto,* $1 = \mathrm{mcd}(2, X)$*. Sin embargo,* $1 \notin (S)$*.*

Si $1 = \mathrm{mcd}(S)$ decimos que los elementos de S son *coprimos* en A. Si para cada par de elementos distintos $a, b \in S$ se verifica $\mathrm{mcd}(a, b) = 1$, decimos que los elementos de S son *coprimos dos a dos*.

Problemas

2.2.1 Escribir demostraciones de los apartados del Lema 2.9 que no se han demostrado y de las Proposición 2.15 y 2.17.

2.2.2 Demostrar que si dos elementos de un anillo son asociados, entonces uno es irreducible (respectivamente primo) si y solo si lo es el otro.

2.2.3 Sea a un elemento diferente de cero de un anillo A. Demostrar que si todos los divisores de a son unidades o asociados a a entonces a es irreducible. Demostrar también que el recíproco se verifica si A es dominio pero no en general.

2.2.4 Demostrar las siguientes afirmaciones para elementos a y b de un anillo:

(1) $a \mid b$ si y solo si $a = \mathrm{mcd}(a, b)$, si y solo si $b = \mathrm{mcm}(a, b)$. En particular, $1 = \mathrm{mcd}(a, 1)$, $\mathrm{mcd}(a, 0) = a = \mathrm{mcm}(a, 1)$ y $0 = \mathrm{mcm}(a, 0)$.

(2) Si a es irreducible entonces $\mathrm{mcd}(a, b) = 1$ si y solo si $a \nmid b$.

2.2.5 Demostrar las siguientes propiedades para d y m dos elementos de un dominio D y S un subconjunto de D.

(1) $d = \mathrm{mcd}(S)$ si y solo si (d) es mínimo entre los ideales principales que contienen a S (o al ideal generado por S).

En particular, si (S) es un ideal principal entonces cualquier generador suyo es un máximo común divisor de S, y además existe una identidad de Bezout para S.

(2) $m = \text{mcm}(S)$ si y solo si $(m) = \cap_{s\in S}(s)$.

En consecuencia, $\text{mcm}(S)$ existe si y solo si el ideal $\cap_{s\in S}(s)$ es principal, y entonces cualquier generador de $\cap_{s\in S}(s)$ es un mínimo común múltiplo de S.

2.2.6 En este ejercicio todas las propiedades de divisibilidad se refieren al anillo $\mathbb{Z}[\sqrt{-5}]$. Demostrar

(1) 2 y $1+\sqrt{-5}$ son coprimos y sin embargo no hay una identidad de Bezout para $\{2, 1+\sqrt{-5}\}$.

(2) 2 y $1+\sqrt{-5}$ no tienen mínimo común múltiplo.

(3) No existe $\text{mcd}(6, 2(1+\sqrt{-5}))$.

2.2.7 Sea S un subconjunto finito de un anillo A y supongamos que para cada dos elementos elementos distintos s y t de S se verifica que $(s,t) = A$. Demostrar que $\text{mcm}(S) = \prod_{s\in S} s$. Dar un ejemplo de dos elementos a y b de un dominio que verifiquen que $\text{mcd}(a,b) = 1$ no existe el mínimo común múltiplo de a y b.

2.2.8 Demostrar que si a y b son elementos coprimos de un anillo A que verifican $(a,b) = A$ entonces $(a^n, b^m) = A$ para todo $n, m \in \mathbb{N}$. Dar un ejemplo de dos elementos a y b de un dominio que verifiquen que $\text{mcd}(a,b) = 1$ y $\text{mcd}(a^2, b) \neq 1$.

2.3 Dominios de factorización única

En esta sección vamos a introducir un tipo de dominios que verifican la propiedad más significativa de los números enteros: El Teorema Fundamental de la Aritmética.

Definición 2.19 *Sea D un dominio. Una* factorización en producto de irreducibles *de un elemento a de D es una expresión del tipo*

$$a = up_1 \cdots p_n$$

donde $n \in \mathbb{Z}^{\geq 0}$, u es una unidad de D y $p_1, \ldots, p_n$ son irreducibles de D. [2] *Diremos que D es un* dominio de factorización *o* DF *si todo elemento no nulo de D admite una factorización en producto de irreducibles.*

Dos factorizaciones de $a \in D$ en producto de irreducibles se dice que son equivalentes si solo se diferencian en el orden y en asociados. Dicho con más rigor, las factorizaciones

$$a = up_1 \cdots p_n = vq_1 \cdots q_m$$

(con $u, v \in D^*$ y el resto de factores irreducibles) son equivalentes *si $n = m$ y existe una* permutación σ *de $\mathbb{N}_n$ (una biyección de $\mathbb{N}_n = \{1, 2, \ldots, n\}$ en sí mismo) tal que p_i y $q_{\sigma(i)}$ son asociados para cada $i = 1, \ldots, n$.*

[2] Obsérvese que se admite la posibilidad de que sea $n = 0$, en cuyo caso la factorización se reduce a $a = u$ ya que, por convenio, el producto vacío es 1

Diremos que D es un dominio de factorización única *ó* DFU *(UFD, en inglés) si es un dominio de factorización en el que, para cada $0 \neq a \in D$, todas las factorizaciones de a son equivalentes.*

Ejemplos 2.20 *(Dominios de factorización y de factorización única)*

(1) El Teorema Fundamental de la Aritmética simplemente nos dice que el anillo de los números enteros es un DFU.

(2) Sea m un entero positivo. Vamos a ver que $\mathbb{Z}[\sqrt{m}]$ es un dominio de factorización. Si m es un cuadrado en $\mathbb{Z}$ entonces $\mathbb{Z}[\sqrt{m}] = \mathbb{Z}$ que es un dominio de factorización. Por tanto, a partir de ahora suponemos que m no es un cuadrado en $\mathbb{Z}$ y siempre que utilicemos una expresión $a + b\sqrt{m}$ suponemos implícitamente que a y b son enteros. Vamos a utilizar la conjugación en $\mathbb{Z}[\sqrt{m}]$ que es la siguiente aplicación[3]

$$\begin{array}{rcl} \mathbb{Z}[\sqrt{m}] & \to & \mathbb{Z}[\sqrt{m}] \\ a + b\sqrt{m} & \mapsto & \overline{a + b\sqrt{m}} = a - b\sqrt{m} \end{array}$$

Es fácil comprobar que esta aplicación es un homomorfismo de anillos con lo que la siguiente aplicación

$$\begin{array}{rcl} N : \mathbb{Z}[\sqrt{m}] & \to & \mathbb{Z} \\ a + b\sqrt{m} & \mapsto & a^2 - b^2 m = (a + b\sqrt{m})(a - b\sqrt{m}) \end{array}$$

satisface $f(xy) = f(x)f(y)$ para todo $x, y \in \mathbb{Z}[\sqrt{m}]$. Sea $x \in \mathbb{Z}[\sqrt{m}]$. Si x es invertible en $\mathbb{Z}[\sqrt{y}]$ entonces $1 = N(1) = N(xx^{-1}) = N(x)N(x^{-1})$ con lo que $N(x)$ es invertible en $\mathbb{Z}$, es decir $N(x) = \pm 1$. Recíprocamente, si $N(x) = \pm 1$, entonces $x\overline{x} = \pm 1$, con lo que x es invertible en $\mathbb{Z}[\sqrt{m}]$. Esto demuestra que

$$\mathbb{Z}[\sqrt{m}]^* = \{x \in \mathbb{Z}[\sqrt{m}] : |N(x)| = 1\}.$$

Vamos a demostrar que si $x \neq 0$ entonces tiene una factorización $\mathbb{Z}[\sqrt{m}]$ por inducción en $|N(x)|$. Obsérvese que si $|N(x)| \neq 0$ pues si $a^2 - b^2 m$ entonces m es un cuadrado en $\mathbb{Z}$ en contra de la hipótesis. Por tanto, el menor valor posible para $|N(x)|$ es 1 y en el caso en que $|N(x)| = 1$ entonces x es una unidad con lo que efectivamente tiene una factorización. Asumamos pues la hipótesis de inducción y supongamos que $|N(x)| > 1$. Entonces x no es unidad. Si x es irreducible por supuesto que tiene una factorización con lo que podemos suponer que x no es irreducible. Por tanto $x = ab$ con a y b no unidades. Por tanto $|N(a)|$ y $|N(b)|$ son divisores propios de $|N(x)|$ y por hipótesis de inducción a y b son productos de irreducibles. Luego x también es producto de irreducibles.

En el siguiente lema vemos que en un DFU los elementos irreducibles coinciden con los primos. Combinando los Ejemplos 2.14 y 2.20.(2) nos proporcionan un DF que no es DFU: $\mathbb{Z}[\sqrt{-5}]$.

[3]Si m es negativo, esta aplicación es la conjugación compleja, pero m es positivo entonces es una aplicación diferente.

Lema 2.21 *Si D es un DFU, entonces todo elemento irreducible de D es primo.*

Demostración. Sea $p \in D$ irreducible, y sean $a, b \in D$ tales que $p \mid ab$. Se trata de ver que $p \mid a$ ó $p \mid b$. Esto está claro si $a = 0$ o $b = 0$ con lo que suponemos que ambos son diferentes de 0. Por hipótesis $pt = ab$ para algún $t \in D$. Si $t = up_1 \cdots p_n$, $a = vq_1 \cdots q_m$ y $b = wr_1 \cdots r_k$ son factorizaciones en irreducibles (con $u, v, w \in D^*$), entonces se tiene

$$upp_1 \cdots p_n = (vw)q_1 \cdots q_m r_1 \cdots r_k,$$

y por la unicidad de la factorización p es asociado de algún q_i (y entonces $p \mid a$) o de algún r_i (y entonces $p \mid b$). ∎

Proposición 2.22 *Para un dominio D, las condiciones siguientes son equivalentes:*

(1) D es un dominio de factorización única.

(2) Todo elemento no nulo de D es producto de primos.

(3) D es un dominio de factorización en el que todo elemento irreducible es primo.

Demostración. (1) implica (2). Por la definición de DFU y por el Lema 2.21.

(2) implica (3) Supongamos que todo elemento de D es producto de primos. Claramente D es un DF. Supongamos que p es irreducible y sea $p = q_1 \dots q_k$ con $q_1, \dots, q_k$ primos. Entonces p divide a algún q_i y por simetría podemos suponer que p divide a q_1. Como también q_1 divide a p se tiene que p y q_1 son asociados. Como q_1 es primo, se tiene que p es primo.

(3) implica (1). Por hipótesis, todo elemento no nulo de D se factoriza como un producto de primos, y podemos demostrar la unicidad de tales factorizaciones adaptando la demostración del Teorema Fundamental de la Aritmética. En efecto, sean $up_1 \cdots p_n = vq_1 \cdots q_m$, con p_i y q_i irreducibles para todo i, y $u, v \in D^*$. Suponemos que $n \leq m$ y razonamos por inducción sobre n. Si $n = 0$ entonces $m = 0$, ya que los divisores de unidades son unidades, y no hay nada que demostrar. Supongamos que $n > 0$ y, la hipótesis de inducción. Por hipótesis, p_n es primo, luego divide a algún q_i y de hecho son asociados (¿por qué?); además, reordenando si es necesario, podemos suponer que $i = m$. Es decir, existe una unidad w tal que $q_m = wp_n$. Entonces

$$up_1 \cdots p_{n-1} = (vw)q_1 \cdots q_{m-1}.$$

Por hipótesis de inducción se tiene $n - 1 = m - 1$ (luego $n = m$) y existe una biyección $\tau : \{1, \dots, n-1\} \to \{1, \dots, n-1\}$ tal que p_i y $q_{\tau(i)}$ son asociados para cada $i = 1, \dots, n-1$. Ahora es evidente que τ se extiende a una permutación σ de $\mathbb{N}_n$ tal que p_i y $q_{\sigma(i)}$ son asociados para cada $i = 1, \dots, n$, y por lo tanto las factorizaciones iniciales son equivalentes. ∎

Problemas

2.3.1 Sean D un DFU y P un conjunto de representantes de los irreducibles de D por la relación de equivalencia "ser asociados", es decir P está formado por irreducibles de D y cada elemento irreducible p de D es asociado de un único elemento de P.

(1) Demostrar que cada elemento a de D se puede escribir de forma única como $a = u\prod_{p\in P} p^{\alpha_p}$, donde u es una unidad de D, cada $\alpha_p \geq 0$ y $\alpha_p = 0$ para casi todo $p \in P$. Llamaremos a esto "la" factorización de a en irreducibles de P.

(2) Demostrar que si
$$a = u\prod_{p\in P} p^{\alpha_p} \qquad \text{y} \qquad b = v\prod_{p\in P} p^{\beta_p}$$
son las factorizaciones de a y b en irreducibles de P entonces $a \mid b$ si y solo si $\alpha_p \leq \beta_p$, para todo $p \in P$.

(3) El número de divisores de un elemento no nulo a de D es finito, salvo asociados. Es decir, existe un conjunto finito F tal que todos los divisores de a son asociados de un elemento de F.

(4) Obtener una fórmula para calcular el número de divisores de a, salvo asociados, en términos de una factorización de a.

(5) Demostrar que todo subconjunto de D tiene máximo común divisor y mínimo común múltiplo y dar una fórmula para ambos. ¡Cuidado con los subconjuntos infinitos!

(6) Dar ejemplos de conjuntos P como los del ejercicio para $\mathbb{Z}$ y $K[X]$ donde K es un cuerpo.

2.3.2 Sea D un dominio y supongamos que existe una aplicación $\mu : D \to \mathbb{Z}^{\geq 0}$ que verifica las tres propiedades siguientes:

- $\mu(ab) = \mu(a)\mu(b)$ para cualesquiera $a, b \in D$.
- $\mu(a) = 0$ si y sólo si $a = 0$.
- $\mu(a) = 1$ si y sólo si a es invertible.

Demostrar que D es un dominio de factorización (no necesariamente única). Demostrar también que si $\mu(a)$ es primo y diferente de $\mu(1)$ entonces a es irreducible en D.

2.3.3 ¿Qué conclusión sobre el anillo $\mathbb{Z}[\sqrt{-3}]$ se extrae de la igualdad $(1+\sqrt{-3})(1-\sqrt{-3}) = 4$?

2.3.4 Comprueba la siguiente igualdad $(5+\sqrt{2})(2-\sqrt{2}) = (11-7\sqrt{2})(2+\sqrt{2})$. ¿Son los cuatro factores irreducibles? ¿Podrías deducir que $\mathbb{Z}[\sqrt{2}]$ no es DFU? ¿Qué sale si calculas $\frac{2+\sqrt{2}}{2-\sqrt{2}}$?

2.3.5 Sea $m \neq 1$ un entero libre de cuadrados y sea $R = \mathbb{Z}[\sqrt{m}]$; se pide:

(1) Usando la igualdad $(m+\sqrt{m})(m-\sqrt{m}) = m(m-1)$, demostrar que 2 no es primo en R.

(2) Si $m \leq -3$, demostrar que 2 es irreducible en R y deducir que R no es un DFU.

(3) Si m es un múltiplo de 5, demostrar que 2 es irreducible en R y deducir que R no es DFU.

(4) Encontrar dos factorizaciones de 4 esencialmente distintas en $\mathbb{Z}[\sqrt{-3}]$.

(5) Encontrar dos factorizaciones de 6 esencialmente distintas en $\mathbb{Z}\sqrt{-6}]$.

(6) Encontrar dos factorizaciones de 4 esencialmente distintas en $\mathbb{Z}[\sqrt{5}]$.

(7) Encontrar dos factorizaciones de 6 esencialmente distintas en $\mathbb{Z}\sqrt{10}]$.

2.4 Dominios de ideales principales

En vista de los resultados de la Sección 2.2, las nociones sobre divisibilidad se manejarán fácilmente en dominios en los que todos los ideales sean principales.

Definición 2.23 *Un* dominio de ideales principales*, o* DIP *(PID, en la literatura en inglés), es un dominio en el que todos los ideales son principales.*

Proposición 2.24 *Si D es un DIP y $0 \neq a \in D \setminus D^*$, las siguientes condiciones son equivalentes:*

(1) a es irreducible.

(2) (a) es un ideal maximal.

(3) $A/(a)$ es un cuerpo.

(4) a es primo.

(5) (a) es un ideal primo.

(6) $A/(a)$ es un dominio.

Demostración. La equivalencia entre (1), (2) y (3) es consecuencia de la Proposición 2.15 y de la Proposición 2.6, y lo mismo puede decirse de la equivalencia entre (4), (5) y (6). También de la Proposición 2.6 se deduce que (2) implica (5). Finalmente, (4) implica (1) por la Proposición 2.13. ∎

Teorema 2.25 *Todo dominio de ideales principales D es un dominio de factorización única.*

Demostración. Por las Proposiciones 2.22 y 2.24, basta con demostrar que D es un dominio de factorización. Por reducción al absurdo suponemos que D no lo es, y vamos a construir, por recurrencia, una sucesión $a_1, a_2, \ldots$ de elementos de D que no admiten factorización y tales que $(a_1) \subset (a_2) \subset \cdots$ es una cadena estrictamente creciente de ideales de D. Para el primer paso simplemente elegimos un elemento arbitrario a_1 de D que no admita factorización en irreducibles. Supongamos ahora que hemos elegido $a_1, \ldots, a_n$ satisfaciendo las condiciones requeridas. Entonces a_n no es irreducible, luego existen $x, y \in D \setminus D^*$ tales que $a_n = xy$. Como a_n no es producto de irreducibles, al menos uno de los factores x ó y (digamos que x) no es producto de irreducibles. Entonces, poniendo $a_{n+1} = x$, tenemos $(a_n) \subset (a_{n+1})$ con la inclusión estricta porque y no es una unidad.

Una vez construida la sucesión (a_i), tomamos $I = (a_1, a_2, \ldots) = \cup_{i \in \mathbb{Z}^+}(a_i)$ (dejamos que el lector compruebe la igualdad anterior). Como D es un DIP, existe $x \in D$ tal que $I = (x)$; en particular $x \in I = \cup_{i \in \mathbb{Z}^+}(a_i)$ y por tanto existe un índice i tal que $x \in (a_i)$; como es claro que $a_i \in (x)$, se tiene $(a_i) = (x) = I$ y por lo tanto $(a_i) = (a_{i+1})$, en contra de la construcción realizada. Este absurdo concluye la demostración. ∎

El recíproco del Teorema 2.25 es falso: $\mathbb{Z}[X]$ es un DFU que no es un DIP. Que no es DIP se sigue del Ejemplo 1.25.(2). De hecho ese ejemplo es un caso particular de un hecho mucho más general (Problema 2.4.2). La demostración de que $\mathbb{Z}[X]$ es DFU es bastante más complicada y también es consecuencia de un resultado más general. La veremos en el Capítulo 3.

Problemas

2.4.1 Sea D un DIP y sean S un subconjunto de D y $a, b, c \in D$. Demostrar

(1) S tiene un mínimo común múltiplo.

(2) S tiene un máximo común divisor d y además existe una identidad de Bezout para S.

(3) El elemento d es un máximo común divisor de $a_1, \ldots, a_n$ si y solo si $d \mid a_i$ para cada $i = 1, \ldots, n$ y existen $r_1, \ldots, r_n \in D$ tales que

$$r_1 a_1 + \cdots + r_n a_n = d.$$

(4) Los elementos $a_1, \ldots, a_n$ son coprimos si y solo si existen $r_1, \ldots, r_n \in D$ tales que

$$r_1 a_1 + \cdots + r_n a_n = 1.$$

(5) Si $d = \text{mcd}(a, b)$, entonces $\text{mcd}(\frac{a}{d}, \frac{b}{d}) = 1$.

(6) Si $\text{mcd}(a, b) = \text{mcd}(a, c) = 1$, entonces $\text{mcd}(a, bc) = 1$.

(7) Si $\text{mcd}(a, b) = 1$ y $a \mid bc$, entonces $a \mid c$.

(8) Si $\text{mcd}(a, b) = 1$, $a \mid c$ y $b \mid c$, entonces $ab \mid c$.

(9) ab y $\text{mcd}(a, b)\text{mcm}[a, b]$ son asociados.

2.4.2 Sea A un anillo. Demostrar que si $A[X]$ es un DIP entonces A es un cuerpo.

2.4.3 Demostrar que si todos los ideales de un anillo A son principales e I es un ideal de A entonces todos los ideales de A/I son principales. ¿En qué condiciones si A es un DIP se verificará que A/I también es un DIP?

2.5 Dominios euclídeos

En esta sección D un dominio.

Definición 2.26 *Una* función euclídea *en D es una aplicación $\delta : D \setminus \{0\} \to \mathbb{Z}^{\geq 0}$ que cumple las siguientes condiciones:*

(DE1) Si $a, b \in D \setminus \{0\}$ verifican $a \mid b$ entonces $\delta(a) \leq \delta(b)$.

(DE2) Dados $a, b \in D$ con $b \neq 0$, existen $q, r \in D$ tales que $a = bq + r$ y o bien $r = 0$ o bien $\delta(r) < \delta(b)$.

Un dominio euclídeo *es un dominio que admite una función euclídea.*

Ejemplos 2.27 *(Dominios Euclídeos)*

(1) El valor absoluto es una función euclídea en $\mathbb{Z}$.

(2) Si K es un polinomio entonces el grado define una función euclídea en $K[X]$.

En efecto, la condición (DE1) se verifica cláramente. Para demostrar que se verifica la condición (DE2) tomamos $a, b \in D \setminus \{0\}$ con $b \neq 0$. Si $a = 0$ tomando $q = r = 0$ se tiene que $a = bq + r$. Por tanto, suponemos que $a \neq 0$ y denotamos por n al grado de a y por m al grado de n. Razonamos por inducción en n. Si $n < m$ podemos tomar $q = 0$ y $r = a$ y si $n = m = 0$ tomamos $q = ab^{-1}$ y $r = 0$ (¿por qué b es invertible?). Esto incluye el menor valor posible para n, o sea $n = 0$. Por hipótesis de inducción se tiene que para todo polinomio c de grado menor que n existen q' y r' en $K[X]$ con $c = q'b + r$ y o bien $r = 0$ o r tiene grado menor que b. Aplicamos esto a $c = a - \alpha\beta^{-1}X^{n-m}b$, donde α es el término principal de a y β es el término principal de b. Es fácil ver que c tiene grado menor que a con lo que tenemos $a + \alpha\beta X^{n-m}b = c = q'b' + r'$. Tomando $q = q' - \alpha\beta' X^{n-m}$ se tiene que $a = qb + r$, como deseábamos.

(3) El cuadrado del módulo complejo define una función euclídea en el anillo $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

En efecto, si $x = a + bi$ con a y b números enteros entonces $\delta(x) = |x|^2 = a^2 + b^2 \in \mathbb{Z}^{\geq 0}$. Además $\delta(x) = 0$ si y solo si $x = 0$ y $\delta xy = \delta x \delta y$ de donde fácilmente se deduce que δ verifica (DE1). Sean ahora $a = a_1 + a_2 i$ y $b = b_1 + b_2 i \neq 0$ con $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Sea $x = x_1 + x_2 i = \frac{a}{b}$. Elegimos dos números enteros q_1 y q_2 lo más próximos a x_1 y x_2 respectivamente y ponemos $q = q_1 + q_2 i$ y $r = a - bq$. De la elección de los q_i tenemos que

$$|x_i - q_i| \leq \frac{1}{2}.$$

Por tanto $a = bq + r$ y

$$\begin{aligned}\delta(r) &= |a - bq|^2 = |b|^2|x - q|^2 = \delta(b)((x_1 - q_1)^2 + (x_2 - q_2)^2) \\ &\leq \delta(b)\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{\delta(b)}{2} < \delta(b).\end{aligned}$$

Lema 2.28 *Sea δ una función euclídea en D, sea I un ideal de D y a un elemento de D diferente de 0. Entonces $I = (a)$ si y solo si $\delta(a) \leq \delta(x)$ para todo $x \in I$.*

Demostración. Supongamos que $I = (a)$ y sea $x \in I$. Entonces $a \mid x$, luego de (DE1) deducimos que $\delta(a) \leq \delta(x)$.

Para demostrar el recíproco imitamos la demostración de que $\mathbb{Z}$ es DIP (Proposición 1.15): Supongamos que $\delta(a) \leq \delta(x)$ para todo $x \in I$. Como $a \in I$ se tiene que $(a) \subseteq I$. Sea $x \in I$. Por (DE2) existen $q, r \in D$ tales que $x = aq + r$ y o bien $r = 0$ o bien $\delta(r) < \delta(a)$. Entonces $r = x - aq \in I$, y por tanto $\delta(a) \leq \delta(x)$, por la hipótesis. Necesariamente $r = 0$, con lo que $x \in (a)$. Esto demuestra que $I = (a)$. ∎

Del Lema 2.28 se deducen de forma inmediata los dos siguientes resultados:

Teorema 2.29 *Todo dominio euclídeo es DIP.*

Lema 2.30 *Si δ es una función euclídea en D entonces las siguientes condiciones son equivalentes para $a \in D$:*

(1) a es una unidad de D.

(2) $\delta(a) = \delta(1)$.

(3) $\delta(a) \leq \delta(x)$, para todo $x \in D \setminus \{0\}$.

Problemas

2.5.1 Demostrar que si D es un DIP entonces todo ideal se puede poner de forma única como producto de ideales maximales. ¿Qué ideales son intersección de ideales maximales.

2.5.2 Demostrar que si $f : A \to B$ es un homomorfismo suprayectiva entre dominios de ideales principales entonces o bien f es un isomorfismo o bien B es un cuerpo.

2.5.3 Sea D un DIP y sea $a = p_1^{e_1} \cdots p_k^{e_k}$ con $p_1, \ldots, p_k$ irreducibles no asociados de D. Demostrar que

$$\frac{D}{(a)} \cong \frac{D}{p_1^{e_1}} \times \cdots \times \frac{D}{p_k^{e_k}}.$$

2.6 El cuerpo de fracciones de un dominio

A lo largo de toda esta sección D es un dominio.

Ya sabemos que todo subanillo de un cuerpo es un dominio. En esta sección vamos a ver que el recíproco es cierto, es decir todo dominio D es un subanillo de un cuerpo. De hecho existe un cuerpo que, en cierto sentido, es el menor cuerpo que contiene a D. Dicho cuerpo es único salvo isomorfismos y se llama el *cuerpo de fracciones* de D. Comenzaremos con la construcción de ese cuerpo, que es una traducción literal de la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$, y analizaremos entonces sus propiedades. La idea de la construcción es la de formar un cuerpo $Q(D)$ cuyos elementos sean "fracciones" del tipo a/b con $a, b \in D$ y $b \neq 0$. De este modo, D estará contenido en $Q(D)$ (identificando cada elemento a de D con la fracción $a/1$), y los elementos no nulos de $Q(D)$ serán invertibles, pues si $a, b \in D \setminus \{0, \}$, entonces b/a será el inverso de a/b. Por supuesto, hay que definir con más rigor las fracciones y hay que dotar a $Q(D)$ de una estructura de cuerpo. El primer problema que se presenta, si pensamos en el caso $D = \mathbb{Z}$ y $Q(D) = \mathbb{Q}$, es el hecho de que dos fracciones aparentemente distintas pueden representar el mismo elemento, como en el caso $10/15 = 2/3$. Esto se resuelve identificando ciertas fracciones mediante una relación de equivalencia, y este será el primer paso en nuestra construcción.

Sean $S = D \setminus \{0\}$ y $X = D \times S$. Definimos en X la relación binaria

$$(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow a_1 s_2 = a_2 s_1$$

que, como el lector comprobará fácilmente, es una relación de equivalencia. La clase de equivalencia de (a, s) se denota por a/s o por $\frac{a}{s}$, y el conjunto cociente $X/\sim$ (es decir, el conjunto de las clases de equivalencia para esa relación) por $Q(D)$. Dotamos a $Q(D)$ de una estructura de anillo con las siguientes operaciones:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2} \qquad \frac{a_1}{s_1}\frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}. \tag{2.2}$$

Hay que asegurarse de que esas definiciones no dependen de los representantes elegidos para cada fracción. Es decir, si $a_1/s_1 = b_1/t_1$ y $a_2/s_2 = b_2/t_2$, hay que comprobar que se obtiene la misma suma y el mismo producto si aplicamos las fórmulas a a_1/s_1 y a_2/s_2 que si se las aplicamos a b_1/t_1 y b_2/t_2. Las igualdades anteriores significan que $a_1 t_1 = b_1 s_1$ y $a_2 t_2 = b_2 s_2$, de donde

$$(a_1 s_2 + a_2 s_1)(t_1 t_2) = a_1 s_2 t_1 t_2 + a_2 s_1 t_1 t_2 = b_1 s_2 s_1 t_2 + b_2 s_1 t_1 s_2 = (b_1 t_2 + b_2 t_1)(s_1 s_2)$$

y por tanto $\frac{a_1 s_2 + a_2 s_1}{s_1 s_2} = \frac{b_1 t_2 + b_2 t_1}{t_1 t_2}$. Esto demuestra que la suma está bien definida, y con el producto se procede de modo análogo.

La siguientes proposición recoge algunas propiedades elementales de $Q(D)$, todas las demostraciones son consecuencias sencillas de que D es un dominio.

Proposición 2.31 *Si D es un dominio entonces $Q(D)$ es un cuerpo con la suma y multiplicación definidas en* (2.2)*. Dados $a, b, s, t \in D$ con $s, t \neq 0$, se tiene:*

(1) El cero $Q(D)$ es $0/1$. Además, la igualdad $a/s = 0/1$ se verifica si y solo si $a = 0$.

(2) El uno de $Q(D)$ es $1/1$. Además, la igualdad $a/s = 1/1$ se verifica si y solo si $a = s$.

(3) $at/st = a/s$.

(4) La igualdad $a/s = b/s$ se verifica si y solo si $a = b$.

(5) La definición de suma se simplifica cuando hay "denominador común": $a/s + b/s = (a + b)/s$.

Usando adecuadamente la Proposición 2.31, la comprobación de que $Q(D)$ es un cuerpo es rutinaria. Demostramos como ejemplo la propiedad distributiva, y dejamos el resto para el lector:

$$\begin{aligned}\frac{a}{s}\left(\frac{b_1}{t_1}+\frac{b_2}{t_2}\right) &= \frac{a}{s}\left(\frac{b_1t_2+b_2t_1}{t_1t_2}\right)=\frac{ab_1t_2+ab_2t_1}{st_1t_2}=\frac{ab_1t_2}{st_1t_2}+\frac{ab_2t_1}{st_1t_2}\\ &= \frac{ab_1}{st_1}+\frac{ab_2}{st_2}=\frac{a}{s}\frac{b_1}{t_1}+\frac{a}{s}\frac{b_2}{t_2}.\end{aligned}$$

Definición 2.32 *El cuerpo $Q(D)$ se llama* cuerpo de fracciones *o* cuerpo de cocientes *del dominio D.*

Ejemplos 2.33 *Cuerpos de fracciones.*

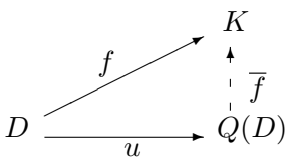
(1) Obviamente, $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$.

(2) Supongamos que un anillo de polinomios $A[X]$ es un dominio (lo que ocurre precisamente si A es un dominio por los Ejemplos 2.4). Su cuerpo de fracciones se suele denotar por $A(X)$ y se llama el *cuerpo de las funciones racionales* sobre A. Sus elementos son fracciones del tipo P/Q con $P, Q \in A[X]$ y $Q \neq 0$, que se suman y se multiplican de forma natural.

Usando el Proposición 2.31, es sencillo ver que la aplicación $u : D \to Q(D)$ dada por $u(a) = a/1$ es un homomorfismo inyectivo de anillos, lo que nos permite ver a D como un subanillo de $Q(D)$ si identificamos cada elemento a de D con la fracción $a/1$ de $Q(D)$. El par $(Q(D), u)$ verifica una interesante propiedad:

Proposición 2.34 *Sean D un dominio, $Q(D)$ su cuerpo de fracciones y $u : D \to Q(D)$ la aplicación dada por $u(a) = a/1$. Entonces:*

(1) **(Propiedad Universal del Cuerpo de Fracciones)** *Para toda pareja (K, f) formada por un cuerpo K y un homomorfismo inyectivo de anillos $f : D \to K$, existe un único homomorfismo de cuerpos $\bar{f} : Q(D) \to K$ tal que $\bar{f} \circ u = f$. Se dice que $\bar{f}$* completa de modo único *el diagrama*



(2) Si dos homomorfismos de cuerpos $g, h : Q(D) \to K$ coinciden sobre D entonces son iguales. Es decir, si $g \circ u = h \circ u$ entonces $g = h$.

(3) $Q(D)$ está determinado salvo isomorfismos por la Propiedad Universal. Explícitamente: supongamos que existen un cuerpo F y un homomorfismo inyectivo de anillos $v : D \to F$ tales que, para todo cuerpo K y todo homomorfismo inyectivo de anillos $f : D \to K$, existe un único homomorfismo de cuerpos $\bar{f} : F \to K$ tal que $\bar{f} \circ v = f$. Entonces existe un isomorfismo $\phi : F \to Q(D)$ tal que $\phi \circ v = u$.

Demostración. (1) Sea $f : D \to K$ como en el enunciado. Si $\bar{f} : Q(D) \to K$ es un homomorfismo de cuerpos tal que $\bar{f} \circ u = f$ entonces, para todo $a/s \in Q(D)$, se verifica

$$\bar{f}(a/s) = \bar{f}(u(a)u(s)^{-1}) = (\bar{f} \circ u)(a)(\bar{f} \circ u)(s)^{-1} = f(a)f(s)^{-1}.$$

Esto prueba que el único homomorfismo de cuerpos $\bar{f} : Q(D) \to K$ que puede satisfacer $\bar{f} \circ u = f$ tiene que venir dado por $\bar{f}(a/s) = f(a)f(s)^{-1}$. Sólo falta comprobar que la aplicación $\bar{f}$ así dada está bien definida y es un homomorfismo. Si $a_1/s_1 = a_2/s_2$ entonces $a_1 s_2 = a_2 s_1$, luego $f(a_1)f(s_2) = f(a_2)f(s_1)$ y, por tanto, $f(a_1)f(s_1)^{-1} = f(a_2)f(s_2)^{-1}$. Esto prueba que $\bar{f}$ está bien definido. Dejaremos que el lector compruebe que es efectivamente un homomorfismo.

(2) Si ponemos $f = g \circ u = h \circ u : D \to K$, los homomorfismos g y h completan el diagrama del apartado (1). Por la unicidad se tiene $g = h$.

(3) Sea $v : D \to F$ como en el enunciado. Aplicando (1) encontramos un homomorfismo $\bar{v} : Q(D) \to F$ tal que $\bar{v} \circ u = v$, y aplicando la hipótesis de (3) encontramos un homomorfismo $\bar{u} : F \to Q(D)$ tal que $\bar{u} \circ v = u$. Entonces la composición $\bar{u} \circ \bar{v} : Q(D) \to Q(D)$ verifica $(\bar{u} \circ \bar{v}) \circ u = \bar{u} \circ v = u$, y por (2) se obtiene $\bar{u} \circ \bar{v} = 1_{Q(D)}$. En particular $\bar{u}$ es suprayectiva, y como es inyectiva por ser un homomorfismo de cuerpos, $\phi = \bar{u}$ es el isomorfismo que buscamos. ∎

La Propiedad Universal permite afirmar que $Q(D)$ es "el menor cuerpo que contiene a D" en un sentido que se hace explícito en el siguiente resultado:

Proposición 2.35 *Sea D un dominio. Si K es un cuerpo y $f : D \to K$ es un homomorfismo inyectivo de anillos, entonces K contiene un subcuerpo isomorfo a $Q(D)$.*

Demostración. Por la Propiedad Universal del Cuerpo de Fracciones existe un homomorfismo de cuerpos $\bar{f} : Q(D) \to K$, y como $\bar{f}$ es inyectiva, Im $\bar{f}$ es un subcuerpo de K isomorfo a $Q(D)$. ∎

Ejemplo 2.36 *El cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$.*
Sea m un número entero que no es un cuadrado, y sea $f : \mathbb{Z}[\sqrt{m}] \to \mathbb{C}$ la inclusión. Si $\bar{f}$ es como en la demostración de la Proposición 2.35, entonces Im $\bar{f}$ es isomorfo al cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$. Un elemento genérico de Im $\bar{f}$ es de la forma $x = \frac{a+b\sqrt{m}}{c+d\sqrt{m}}$, con $a, b, c, d \in \mathbb{Z}$ y $c + d\sqrt{m} \neq 0$. Si ponemos $t = (c + d\sqrt{m})(c - d\sqrt{m}) \neq 0$ entonces $t = c^2 - d^2 m \in \mathbb{Z}$, y así

$$x = \frac{a + b\sqrt{m}}{c + d\sqrt{m}} = \frac{(a + b\sqrt{m})(c - d\sqrt{m})}{t} = \frac{r + s\sqrt{m}}{t} = \frac{r}{t} + \frac{s}{t}\sqrt{m},$$

donde $r, s \in \mathbb{Z}$, y por tanto $x \in \mathbb{Q}[\sqrt{m}]$. Esto demuestra que Im $\bar{f} \subseteq \mathbb{Q}[\sqrt{m}]$, y el otro contenido es claro, pues un elemento genérico $\frac{a}{s} + \frac{b}{t}\sqrt{m}$ de $\mathbb{Q}[\sqrt{m}]$ se reescribe como $\frac{at+bs\sqrt{m}}{st}$.

En conclusión, el cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$ es isomorfo a $\mathbb{Q}[\sqrt{m}]$. De hecho abusaremos de la notación y diremos que el cuerpo de fracción de $\mathbb{Z}[\sqrt{m}]$ es $\mathbb{Q}[\sqrt{m}]$.

Un interesante corolario de la Proposición 2.35 es el siguiente:

Corolario 2.37 *Todo cuerpo K posee un subcuerpo K', llamado el* subcuerpo primo *de K, que está contenido en cualquier otro subcuerpo de K (es decir, K' es "el menor subcuerpo de K"). Si la característica de K es un entero primo p, entonces K' es isomorfo a $\mathbb{Z}_p$; en caso contrario K' es isomorfo a $\mathbb{Q}$.*

Demostración. Si la característica es un primo p entonces el subanillo primo de K (isomorfo a $\mathbb{Z}_p$) es ya un cuerpo, y contiene a cualquier subcuerpo (de hecho, a cualquier subanillo) de K.

En otro caso, al ser K un cuerpo, la característica es cero; es decir, el homomorfismo de anillos $f : \mathbb{Z} \to K$ es inyectivo. El cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$, y el homomorfismo de cuerpos $\bar{f} : \mathbb{Q} \to K$ que nos da la Propiedad Universal viene dada por $\bar{f}(n/m) = f(n)f(m)^{-1}$. Como $\bar{f}$ es inyectivo, $K' = \text{Im } \bar{f}$ es un subcuerpo de K isomorfo a $\mathbb{Q}$, y ahora basta ver que K' está contenido en cualquier subcuerpo F de K. Dado un tal F, se tiene $f(m) \in F$ para cada $m \in \mathbb{Z}$, y si $m \neq 0$ entonces $f(m) \neq 0$ y $f(m)^{-1} \in F$. Por tanto, para cada $n/m \in \mathbb{Q}$ se tiene $\bar{f}(n/m) = f(n)f(m)^{-1} \in F$, lo que demuestra que $K' \subseteq F$. ∎

Problemas

2.6.1 Sea D un dominio y sea Q su cuerpo de fracciones. Demostrar que:

(1) Si D' es un subanillo de D con cuerpo de fracciones Q', entonces Q contiene un subcuerpo isomorfo a Q'.

(2) Si A es un subanillo de Q que contiene a D, entonces Q es un cuerpo de cocientes de A.

2.6.2 Sea D un dominio y sea K su cuerpo de fracciones. Supongamos que existe una aplicación $\delta : K \setminus \{0\} \to \mathbb{Q}$ que conserva productos y tal que $\delta(D) \subseteq \mathbb{Z}^{\geq 0}$. Demostrar que la restricción de δ a D es una función euclídea en D si y solo si para todo $x \in K \setminus D$ existe $y \in D$ tal que $\delta(x - y) < 1$. Indicación: Ver el Ejemplo 2.27.(3).

2.6.3 Usar el Problema 2.6.2 para decidir para que números naturales m la aplicación $\delta(x) = |x|^2$ define una función euclídea en $\mathbb{Z}[\sqrt{-m}]$.

2.6.4 Sea m un entero libre de cuadrados, es decir no es divisible por el cuadrado de ningún otro entero. Sea $A_m = \left\{ \frac{a+b\sqrt{m}}{2} : a \equiv b \bmod 2 \right\}$. Demostrar que A_m es un subanillo de los números complejos si y solo si $m \equiv 1 \bmod 4$. Usar el problema 2.6.2 para decidir para qué números primos p, A_{-p} es un subanillo de los números complejos y la función $\delta(x) = |x|^2$ define una función euclídea en A_{-p}.

2.6.5 Calcular las unidades de $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, A_{-3}, A_{-7} y A_{-11}.

2.6.6 Demostrar que $\mathbb{Z}[\sqrt{2}]$ es un dominio euclideo. Compara esto con tu solución del Problema 2.3.4. Demuestra $\mathbb{Z}[\sqrt{2}]$ que este anillo tiene infinitas unidades. Indicación: Aquí tienes una: $1+\sqrt{2}$.

2.6.7 Sea D un dominio y sea P un ideal primo de A. Consideremos el siguiente subconjunto del cuerpo de fracciones K de D:

$$D_P = \left\{ \frac{a}{b} : a \in D, b \in D \setminus P \right\}.$$

Demostrar las siguientes propiedades:

(1) D_P es un subanillo de K que contiene a D.

(2) Sea I un ideal de D entonces

   (a) $I_P = \left\{ \frac{a}{b} : a \in P, b \in D \setminus P \right\}$ es un ideal de D_P.
   (b) $I_P = D_P$ si y sólo si $I \not\subseteq P$.
   (c) Si I es principal entonces I_P también es principal.

(3) Si J es un ideal de D entonces $J = I_P$ para algún ideal de D.

(4) La aplicación $Q \to Q_P$ define una biyección del conjunto de ideales primos de D contenidos en P al conjunto de los ideales primos de D_P.

(5) P_P es el único ideal maximal de D_P.

(6) Demostrar que si D es un dominio de ideales principales entonces D_P los únicos ideales primos de D_P son 0 y P_P y que todos los ideales de D son de la forma $(P_P)^n$ para algún entero n.

2.6.8 Consideremos la aplicación $N : \mathbb{Z}[i] \to \mathbb{Z}^{\geq 0}$ dada por $N(x) = |x|^2 = x\,\overline{x}$. Demostrar

(1) $N(xy) = N(x)N(y)$ para todo $x, y \in \mathbb{Z}[i]$.

(2) Un número entero es suma de dos cuadrados (de números enteros) si y solo si está en la imagen de N.

(3) La imagen de N es cerrada para productos.

(4) Si $x \in \mathbb{Z}[i]$ entonces x es invertible en $\mathbb{Z}[i]$ si y solo si $N(x) = 1$ si y solo si $x \in \{1, -1, i, -i\}$.

(5) Si $N(x)$ es primo con $x \in \mathbb{Z}[i]$ entonces x es irreducible de $\mathbb{Z}[i]$.

(6) Las siguientes condiciones son equivalentes para primo p:

   (a) p es suma de dos cuadrados.

(b) $p \not\equiv 3 \bmod 4$.

(c) $p = 2$ ó $p \equiv 1 \bmod 4$.

(d) Existe un entero n tal que $n^2 \equiv -1 \bmod p$.

(e) p no es irreducible en $\mathbb{Z}[i]$.

(Indicación para la demostración de (3) implica (4) en el caso en que $p \equiv 1 \bmod 4$: Utilizar el Teorema de Wilson para demostrar que si $p = 4t+1$ entonces $-1 \equiv ((2t)!)^2 \bmod p$.)

(7) Un elemento a de $\mathbb{Z}[i]$ es irreducible si y solo si $N(a)$ es primo ó a es asociado en $\mathbb{Z}[i]$ a un entero primo p con $p \equiv 3 \bmod 4$.

(8) Un número natural n es suma de dos cuadrados si y solo si el exponente de todo primo $p \equiv 3 \bmod 4$ en la factorización de n es par.

Capítulo 3

Polinomios

3.1 Anillos de polinomios

Sea A un anillo. En el Ejemplo 1.4.4 definimos el anillo de polinomios $A[X]$ en una indeterminada con coeficientes en A como el conjunto de las expresiones del tipo

$$P = P(X) = p_0 + p_1X + p_2X^2 + \cdots + p_nX^n \tag{3.1}$$

donde n es un número entero no negativo y $p_i \in A$ para todo i. Si P es como en (3.1), entonces $p_0, p_1, p_2, \ldots$ se llaman coeficientes de P. Más precisamente, p_iX^i se llama *monomio* de grado i del polinomio P y p_i se llama *coeficiente* del monomio de grado i de P. Obsérvese que P tiene infinitos coeficientes, aunque todos menos un número finito son iguales a 0. Dos polinomios son iguales si sus coeficientes de los monomios del mismo grado son iguales. El *polinomio cero* o *polinomio nulo* es el polinomio que tiene todos los coeficientes iguales a 0.

La suma y el producto en $A[X]$ se definen

$$(a_0 + a_1X + a_2X^2 + \cdots) + (b_0 + b_1X + b_2X^2 + \cdots) = c_0 + c_1X + c_2X^2 + \cdots,$$

donde cada $c_n = a_n + b_n$, y

$$(a_0 + a_1X + a_2X^2 + \cdots) \cdot (b_0 + b_1X + b_2X^2 + \cdots) = d_0 + d_1X + d_2X^2 + \cdots,$$

donde cada $d_n = a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0 = \sum_{i=0}^{n} a_ib_{n-i}$.

Vamos a usar la siguiente notación: $\mathbb{N}_0 = \mathbb{N} \cup 0$.

Sea A un anillo y sea $p = \sum_{i\in\mathbb{N}_0} p_iX^i \in A[X]$ un polinomio no nulo de $A[X]$. Entonces, por definición de polinomio, el conjunto $\{i \in \mathbb{N}_0 : p_i \neq 0\}$ no es vacío y está acotado superiormente. Por tanto ese conjunto tiene un máximo, al que llamamos *grado* del polinomio p y denotamos por $\mathrm{gr}(p)$. Es decir,

$$\mathrm{gr}(p) = \max\{i \in \mathbb{N}_0 : p_i \neq 0\}.$$

El coeficiente de mayor grado, $p_{\mathrm{gr}(p)}$, se conoce como el *coeficiente principal* de p, y diremos que p es *mónico* si su coeficiente principal es 1. Por convenio, consideramos que el polinomio 0 tiene grado $-\infty$ y coeficiente principal 0. Es claro que los polinomios de grado 0 son precisamente los polinomios constantes no nulos. A veces llamaremos *lineales* a los polinomios de grado 1, *cuadráticos* a los de grado 2, *cúbicos* a los de grado 3, etcétera.

Lema 3.1 *Si P y Q son polinomios no nulos de $A[X]$ y sus términos principales son p y q respectivamente entonces se verifican las siguientes propiedades:*

(1) $\mathrm{gr}(P+Q) \leq \max(\mathrm{gr}(P), \mathrm{gr}(Q))$*, con la desigualdad estricta si y solo si* $\mathrm{gr}(P) = \mathrm{gr}(Q)$ *y* $p + q = 0$*.*

(2) $\mathrm{gr}(PQ) \leq \mathrm{gr}(P) + \mathrm{gr}(Q)$*, con igualdad si y solo si* $pq \neq 0$*.*

(3) Si p es regular (por ejemplo, si P es mónico, o si A es un dominio), entonces se tiene $\mathrm{gr}(PQ) = \mathrm{gr}(P) + \mathrm{gr}(Q)$*.*

(4) Las desigualdades de los apartados 1 y 2 pueden ser estrictas (buscar un ejemplo cuando $A = \mathbb{Z}_6$*).*

Demostración. Ejercicio. ∎

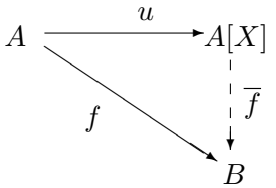
Una consecuencia inmediata del Lema 3.1 es:

Corolario 3.2 *Un anillo de polinomios $A[X]$ es un dominio si y solo si lo es el anillo de coeficientes A. En este caso se tiene $A[X]^* = A^*$; es decir, los polinomios invertibles de $A[X]$ son los polinomios constantes invertibles en A. En particular, los polinomios invertibles sobre un cuerpo son exactamente los de grado 0, y $A[X]$ nunca es un cuerpo.*

Hemos observado que un anillo A es un subanillo del anillo de polinomios $A[X]$, y por tanto la inclusión $u : A \to A[X]$ es un homomorfismo de anillos. También es claro que el subanillo de $A[X]$ generado por A y X es todo $A[X]$. Es decir, la indeterminada X y las constantes de A (las imágenes de u) generan todos los elementos de $A[X]$. El siguiente resultado nos dice que $A[X]$ puede caracterizarse por una propiedad en la que solo intervienen X y u.

Proposición 3.3 *Sean A un anillo, $A[X]$ el anillo de polinomios con coeficientes en A en la indeterminada X y $u : A \to A[X]$ el homomorfismo de inclusión.*

(1) **(Propiedad Universal del Anillo de Polinomios, PUAP)** *Para todo homomorfismo de anillos $f : A \to B$ y todo elemento b de B existe un único homomorfismo de anillos $\overline{f} : A[X] \to B$ tal que $\overline{f}(X) = b$ y $\overline{f} \circ u = f$. Para expresar la última igualdad dice que* $\overline{f}$ completa de modo único *el diagrama*



(2) Si dos homomorfismos de anillos $g, h : A[X] \to B$ coinciden sobre A y en X entonces son iguales. Es decir, si $g \circ u = h \circ u$ y $g(X) = h(X)$ entonces $g = h$.

(3) $A[X]$ y u están determinados salvo isomorfismos por la PUAP. Explícitamente: supongamos que existen un homomorfismo de anillos $v : A \to P$ y un elemento $T \in P$ tales que, para todo homomorfismo de anillos $f : A \to B$ y todo elemento $b \in B$, existe un único homomorfismo de anillos $\overline{f} : P \to B$ tal que $\overline{f} \circ v = f$ y $\overline{f}(T) = b$. Entonces existe un isomorfismo $\phi : A[X] \to P$ tal que $\phi \circ u = v$ y $\phi(X) = T$.

Demostración. (1) Sean $f : A \to B$ y $b \in B$ como en el enunciado. Si existe un homomorfismo $\overline{f} : A[X] \to B$ tal que $\overline{f} \circ u = f$ y $\overline{f}(X) = b$, entonces para un polinomio $P = \sum_{n\geq 0} p_n X^n$, se tendrá

$$\overline{f}(P) = \overline{f}\left(\sum_{n\geq 0} u(p_n)X^n\right) = \sum_{n\geq 0} f(p_n)b^n.$$

Por tanto, la aplicación dada por $\overline{f}(P) = \sum_{n\geq 0} f(p_n)b^n$ es la única que puede cumplir tales condiciones. El lector puede ahora comprobar que esta aplicación $\overline{f}$ es un homomorfismo de anillos, y es elemental ver que satisface $\overline{f}(X) = b$ y $\overline{f} \circ u = f$.

(2) Si ponemos $f = g \circ u = h \circ u : A \to B$, los homomorfismos g y h completan el diagrama del apartado (1) Por la unicidad se tiene $g = h$.

(3) Sean $v : A \to P$ y $T \in P$ como en (3). Aplicando (1) y la hipótesis de (3) deducimos que existen homomorfismos $\overline{v} : A[X] \to P$ y $\overline{u} : P \to A[X]$ tales que que se verifican las siguientes igualdades:

$$\overline{v} \circ u = v, \quad \overline{v}(X) = T, \qquad \overline{u} \circ v = u, \quad \overline{u}(T) = X.$$

Entonces la composición $\overline{u} \circ \overline{v} : A[X] \to A[X]$ verifica

$$(\overline{u} \circ \overline{v}) \circ u = \overline{u} \circ v = u \qquad \text{y} \qquad (\overline{u} \circ \overline{v})(X) = \overline{u}(T) = X,$$

y por (2) se obtiene $\overline{u} \circ \overline{v} = 1_{A[X]}$. De modo análogo, y observando que v y T verifican una condición similar a (2), se demuestra que $\overline{v} \circ \overline{u} = 1_P$, con lo que $\overline{v}$ es el isomorfismo que buscamos. ∎

La utilidad de la PUAP estriba en que, dado un homomorfismo $f : A \to B$, nos permite crear un homomorfismo $A[X] \to B$ que "respeta" a f y que "se comporta bien" sobre un elemento $b \in B$ que nos interese. Los siguientes ejemplos son aplicaciones de la PUAP a ciertos homomorfismos que aparecen con frecuencia y son importantes tanto en este capítulo como en algunos de los siguientes (y en otras muchas situaciones que no estudiaremos aquí).

Ejemplos 3.4 *Aplicaciones de la PUAP.*

(1) Sean A un subanillo de B y $b \in B$. Aplicando la PUAP a la inclusión $A \hookrightarrow B$ obtenemos un homomorfismo $S_b : A[X] \to B$ que es la identidad sobre A (decimos a veces que *fija* los elementos de A) y tal que $S_b(X) = b$. Se le llama el *homomorfismo de sustitución* (o de *evaluación*) en b. Dado $P \in A[X]$, escribiremos a menudo $P(b)$ en vez de $S_b(X)$. Podemos describir explícitamente la acción de S_b en un polinomio:

$$\begin{array}{ccc} A[X] & \xrightarrow{S_b} & B \\ P(X) = \sum_{n\geq 0} p_n X^n & \rightsquigarrow & S_b(P) = P(b) = \sum_{n\geq 0} p_n b^n. \end{array}$$

(2) Sean A un anillo y $a \in A$. Si en el ejemplo anterior tomamos $B = A[X]$ y $b = X + a$, obtenemos un homomorfismo $A[X] \to A[X]$ dado por

$$p(X) \mapsto p(X + a).$$

Este homomorfismo es un automorfismo cuyo inverso viene dado por $p(X) \mapsto p(X - a)$ (¿por qué?).

(3) Todo homomorfismo de anillos $f : A \to B$ induce un homomorfismo entre los correspondientes anillos de polinomios: Aplicándole la PUAP a la composición de f con la inclusión $B \hookrightarrow B[X]$ obtenemos $\overline{f} : A[X] \to B[X]$ tal que $\overline{f} \mid_A = f$ y $\overline{f}(X) = X$. Explícitamente,

$$\overline{f}\left(\sum_{n\geq 0} p_n X^n\right) = \sum_{n\geq 0} f(p_n)X^n.$$

Es fácil ver que, si f es inyectivo o suprayectivo, entonces lo es $\overline{f}$; como casos particulares de esta afirmación se obtienen los dos ejemplos siguientes:

(4) Si A es un subanillo de B entonces $A[X]$ es un subanillo de $B[X]$.

(5) Si I es un ideal del anillo A, la proyección $\pi : A \to A/I$ induce un homomorfismo suprayectivo $\overline{\pi} : A[X] \to (A/I)[X]$. Si ponemos $\overline{a} = a + I$, el homomorfismo $\overline{\pi}$ viene dado explícitamente por

$$\overline{\pi}\left(\sum_{n\geq 0} p_n X^n\right) = \sum_{n\geq 0} \overline{p_n} X^n.$$

A $\overline{\pi}$ se le llama el homomorfismo de *reducción de coeficientes módulo* I. Su núcleo, que es un ideal de $A[X]$, consiste en los polinomios con coeficientes en I, y lo denotaremos por $I[X]$. Del Primer Teorema de Isomorfía se tiene que $(A/I)[X] \simeq \dfrac{A[X]}{I[X]}$.

(6) Sea A un subanillo de B y sea $S_b : A[X] \to B$ el homomorfismo de sustitución en cierto elemento b de B. Entonces Im S_b es el subanillo de B generado por $A \cup \{b\}$, y consiste en las "expresiones polinómicas en b con coeficientes en A"; es decir, en los elementos de la forma

$$\sum_{i=0}^{n} a_i b^i,$$

donde $n \geq 0$ y $a_i \in A$ para cada i. Este subanillo se suele denotar por $A[b]$ y es el menor subanillo de B que contiene a $A \cup \{b\}$.

Por ejemplo, si $A = \mathbb{Z}$, $B = \mathbb{C}$ y $b = \sqrt{m}$ para cierto $m \in \mathbb{Z}$, entonces la notación anterior es compatible con la que se usó anteriormente (es decir, $\mathbb{Z}[\sqrt{m}]$ representa el mismo subanillo atendiendo a cualquiera de las dos definiciones). Lo mismo ocurre si se toma $A = \mathbb{Q}$. Si además $m \equiv 1 \bmod 4$ entonces $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ es el anillo A_m del Problema 2.6.4 y $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}\left[\frac{1+\sqrt{m}}{2}\right]$.

Problemas

3.1.1 Demostrar el Lema 3.1.

3.1.2 Sea A un anillo y sean $a, u \in A$. Demostrar que el homomorfismo $A[X] \to A[X]$ de sustitución en $uX + a$ es un automorfismo si y sólo si u es invertible en A.

3.1.3 Sean D un dominio, K su cuerpo de fracciones y $P, Q \in D[X]$. Demostrar que si P y Q son coprimos en $D[X]$ entonces también son coprimos en $D[X]$ y existen $A, B \in D[X]$ con $AP + BQ \in D \setminus \{0\}$.

3.2 Raíces de polinomios

Empezaremos esta sección con el siguiente lema. Recuérdese que consideramos el polinomio cero como un polinomio de grado $-\infty$.

Lema 3.5 *Sea A un anillo y sean $f, g \in A[X]$. Si el coeficiente principal de g es invertible en A, entonces existen dos únicos polinomios $q, r \in A[X]$ tales que $f = gq + r$ y $\operatorname{gr}(r) < \operatorname{gr}(g)$.*

En esta situación, q y r se llaman cociente *y* resto *de la división de f entre g.*

Demostración. Para la existencia simplemente usamos el argumento que vimos en el Ejemplo 2.27.(2) Sea $m = \operatorname{gr}(g)$ y sea b el coeficiente principal de g que es invertible en A, por hipótesis. Dado $f \in A[X]$ vamos a ver, por inducción en $n = \operatorname{gr}(f)$, que existen $q, r \in A[X]$ satisfaciendo las propiedades del Lema. Si $n < m$ podemos tomar $q = 0$ y $r = f$. Supongamos pues que $n \geq m$ y que la propiedad se verifica si f se sustituye por un polinomio de grado menor. Si a es el término principal de f, es claro que el polinomio $f_1 = f - ab^{-1}X^{n-m}g \in A[X]$ tiene grado menor que el de f. Por hipótesis de inducción existen $q_1, r \in A[X]$ tales que $f_1 = gq_1 + r$ y $r = 0$ o $\operatorname{gr}(r) < m$. Entonces $f = g(q_1 + ab^{-1}X^{n-m}) + r$, lo que termina la demostración de la existencia de cociente y resto.

En cuanto a la unicidad, supongamos que $f = gq_1 + r_1 = gq_2 + r_2$ con $\operatorname{gr}(r_i) < \operatorname{gr}(g)$ para cada $i = 1, 2$. Como el término principal de g es regular, del Lema 3.1 se deduce que

$$\operatorname{gr}(g) + \operatorname{gr}(q_1 - q_2) = \operatorname{gr}(g(q_1 - q_2)) = \operatorname{gr}(r_2 - r_1) \leq \max\{\operatorname{gr}(r_2), \operatorname{gr}(r_1)\} < \operatorname{gr}(g).$$

Luego $\operatorname{gr}(q_1 - q_2) < 0$ y en consecuencia $q_1 = q_2$, de donde $r_1 = r_2$. ∎

Proposición 3.6 *Sean A un anillo, $a \in A$ y $f \in A[X]$. Entonces:*

(1) **(Teorema del Resto)** *El resto de la división de f entre $X - a$ es $f(a)$.*

(2) **(Teorema de Ruffini)** *f es divisible por $X - a$ precisamente si $f(a) = 0$. En tal caso se dice que a es una* raíz *de f.*

Demostración. Dividiendo f entre $X-a$ tenemos $f = q(X-a)+r$ con $\mathrm{gr}(r) < 1$, por lo que r es constante y así $r = r(a) = f(a) - q(a)(a-a) = f(a)$. Esto demuestra (1), y (2) es entonces inmediato. ∎

Fijemos $a \in A$. Como, para cada $k \in \mathbb{N}_0$, el polinomio $(X-a)^k$ es mónico de grado k, se tiene $\mathrm{gr}((X-a)^k q) = k + \mathrm{gr}(q)$ para cada $q \in A[X]$. Por tanto, para cada $f \in A[X]$ no nulo, existe un mayor $m \in \mathbb{N}_0$ tal que $(X-a)^m$ divide a f. Este entero m, que verifica $0 \leq m \leq \mathrm{gr}(f)$, se llama la *multiplicidad de a en f*. Por el Teorema de Ruffini, a es raíz de f precisamente si $m \geq 1$. Cuando $m = 1$ se dice que a es una *raíz simple* de f, y cuando $m > 1$ se dice que a es una *raíz múltiple* de f.

Lema 3.7 *Sean $a \in A$ y $f \in A[X]$. La múltiplicidad de a en f es el único entero no negativo m tal que $f = (X-a)g$ para algún polinomio $g \in A[X]$ del que a no es raíz.*

Demostración. Sea n la multiplicidad de a en f. Entonces $f = (X-a)^n h$ para un polinomio h pero $(X-a)^{n+1}$ no divide a f. Si a es raíz de g, entonces $X-a$ divide a h y por tanto $(X-a)^{n+1}$ divide a f, que acabamos de decir que no pasa. Luego a no es raíz de h.

Recíprocamente, supongamos que $f = (X-a)^m g$ con $g \in A[X]$ y $g(a) = 0$. Por la definición de multiplicidad, $m \leq n$. Como $X-a$ es mónico también es cancelable en $A[X]$, y por tanto de $(X-a)^m g = (X-a)^n h$ deducimos que $(X-a)^{n-m} h = g$. Si $n > m$ entonces $g(a) = 0$, en contra de la suposición. Luego $m = n$. ∎

Cuando D es un dominio, del Teorema de Ruffini se deduce que $X-a$ es primo para cualquier $a \in D$. Esto es esencial en la demostración del siguiente resultado.

Proposición 3.8 (Acotación de raíces) *Sean D un dominio y $0 \neq f \in D[X]$. Entonces:*

(1) Si $a_1, \ldots, a_n \in D$ son distintos dos a dos y $\alpha_1, \ldots \alpha_n \geq 1$ son enteros con cada $(X-a_i)^{\alpha_i} \mid f$, entonces $(X-a_1)^{\alpha_1} \cdots (X-a_n)^{\alpha_n} \mid f$. Por tanto $\sum_{i=1}^n \alpha_i \leq \mathrm{gr}(f)$.

(2) La suma de las multiplicidades de todas las raíces de f es menor o igual que $\mathrm{gr}(f)$. En particular, el número de raíces distintas de f es menor o igual que $\mathrm{gr}(f)$.

Demostración. Es claro que basta con demostrar la primera afirmación de (1), cosa que hacemos por inducción en $s = \sum_{i=1}^n \alpha_i$ con el caso $s = 1$ evidente. Cuando $s > 1$, usando la hipótesis $(X-a_1)^{\alpha_1} \mid f$ y la hipótesis de inducción, sabemos que existen polinomios g y h tales que

$$g(X-a_1)^{\alpha_1} = f = h(X-a_1)^{\alpha_1 - 1}(X-a_2)^{\alpha_2} \cdots (X-a_n)^{\alpha_n}.$$

Cancelando $(X-a_1)^{\alpha_1-1}$ y usando el hecho de que $X-a_1$ es primo y no divide a ningún otro $X-a_i$ (¿por qué?), deducimos que $X-a_1$ divide a h, y esto nos da el resultado. ∎

Si D no es un dominio, siempre podemos encontrar un polinomio en $D[X]$ para el que falle la acotación de raíces (es decir, "con más raíces que grado"). En efecto, si $0 \neq a, b \in D$ y $ab = 0$, entonces aX es un polinomio de grado 1 con al menos 2 raíces, 0 y b. Otro ejemplo se obtiene considerando el polinomio $X^2 - 1$, que tiene 4 raíces en $\mathbb{Z}_8$.

El siguiente corolario evidente de la Proposición 3.8 se conoce como el *principio de las identidades polinómicas*. Ya hemos comentado que su segundo apartado falla sobre cualquier anillo finito.

Corolario 3.9 *Sea D un dominio, y sean $f, g \in D[X]$. Entonces:*

(1) Si las funciones polinómicas $f, g : D \to D$ coinciden en m elementos de D y se tiene que $m > \mathrm{gr}(f)$ y $m > \mathrm{gr}(g)$, entonces $f = g$ (como polinomios).

(2) Si D es infinito entonces dos polinomios distintos definen funciones polinómicas distintas en D.

La necesidad de la hipótesis de infinitud del dominio D en el Corolario 3.9 resulta obvia si observamos que si K es un cuerpo (recuérdese que todo dominio finito es un cuerpo) entonces hay infinitos polinomios con coeficientes en K pero solo un número finito de aplicaciones de K en K. Para un ejemplo explícito recordemos el Pequeño Teorema de Fermat que afirma que si p es primo, entonces $a^p \equiv a \bmod p$. Eso implica que todos los elementos del cuerpo $\mathbb{Z}/p\mathbb{Z}$ son raíces del polinomio no nulo $X^p - X$.

El siguiente concepto es útil para calcular multiplicidades: Si A es un anillo, la *derivada* de $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ se define como

$$D(P) = P' = a_1 + 2a_2X + 3a_3X^2 + \cdots + na_nX^{n-1}.$$

Obsérvese que la derivada no se ha definido a partir de ningún concepto topológico, y por ejemplo no es cierto en general que un polinomio con derivada nula sea constante (considérese por ejemplo $X^n \in \mathbb{Z}_n[X]$). Sin embargo, esta *derivada formal* satisface las mismas propiedades algebraicas que la derivada del Análisis.

Lema 3.10 *Dados $a, b \in A$ y $P, Q \in A[X]$, demostrar que:*

(1) $(aP + bQ)' = aP' + bQ'$.

(2) $(PQ)' = P'Q + PQ'$.

(3) $(P^n)' = nP^{n-1}P'$.

Demostración. Ejercicio. ∎

Proposición 3.11 *Un elemento $a \in A$ es una raíz múltiple de $P \in A[X]$ si y solo si $P(a) = P'(a) = 0$.*

Demostración. Ya sabemos que a es una raíz de P si y solo si $P(a) = 0$. Si a es raíz simple se tiene $P = (X - a)Q$ para cierto $Q \in A[X]$ con $Q(a) \neq 0$, por lo que, del Lema 3.10 tenemos que $P' = Q + (X - a)Q'$ y así $P'(a) = Q(a) \neq 0$. Si a es raíz múltiple se tiene $P = (X - a)^2Q$ para cierto $Q \in A[X]$, por lo que $P' = 2(X - a)Q + (X - a)^2Q'$ y así $P'(a) = 0$. ∎

En dominios de característica cero, la idea de la demostración anterior puede usarse para determinar la multiplicidad de a en P (no solo para decidir si a es simple o múltiple). Para ello, necesitamos considerar las *derivadas sucesivas* de un polinomio: Para cada $n \geq 0$ se define la derivada n-ésima $P^{(n)}$ de $P \in A[X]$, de forma recurrente, por las fórmulas:

$$P^{(0)} = P \quad \text{y} \quad P^{(n+1)} = (P^{(n)})'.$$

Proposición 3.12 *Sea D un dominio de característica 0, y sean $P \in D[X]$ y $a \in D$. Entonces la multiplicidad de a en P es el menor $m \in \mathbb{N}_0$ tal que $P^{(m)}(a) \neq 0$.*

Demostración. Haremos inducción en la multiplicidad m de a en P, con el caso $m = 0$ claro. Si $m \geq 1$ entonces a es raíz de P y por tanto $P = (X-a)Q$ para cierto $Q \in D[X]$. Entonces la multiplicidad de a en Q es $m-1$, y por hipótesis de inducción $Q^{(i)}(a) = 0 \neq Q^{(m-1)}(a)$ para todo $i < m-1$. Además, usando el Lema 3.10 es fácil demostrar por inducción que para cada $t \geq 1$ se tiene

$$P^{(t)} = tQ^{(t-1)} + (X-a)Q^{(t)}.$$

Ahora el lector podrá completar fácilmente la demostración. ∎

La hipótesis sobre la característica de D en la Proposición 3.12 es necesaria. Por ejemplo, si p es un número primo, $K = \mathbb{Z}_p$ y $P = X^p$, entonces $P' = 0$ y así $P^{(n)}(0) = 0$ para todo n.

No todos los polinomios con coeficientes en un anillo A tienen raíces en A. Por ejemplo, los polinomios de grado 0 no tienen ninguna raíz, y un polinomio lineal $aX + b$ (con $a \neq 0$) tiene una raíz en A si y solo si a divide a b. En particular, todo polinomio lineal sobre un cuerpo tiene una raíz, pero puede haber polinomios de grado positivo sin raíces: por ejemplo, $X^2 + 1$ no tiene raíces en $\mathbb{R}$, y para todo entero primo p y todo $n \geq 2$ el polinomio $X^n - p$ no tiene raíces en $\mathbb{Q}$.

Problemas

3.2.1 Demostrar el Lema 3.10.

3.2.2 Sea $P \in \mathbb{Z}_2[X]$. Demostrar que $X - 1$ divide a P precisamente si P tiene un número par de coeficientes no nulos.

3.2.3 Justificar la *regla de Ruffini* para el cálculo del cociente y el resto en la división de $p = p_0 + p_1X + \ldots + p_nX^n$ entre $X - a$. La regla está representada por la tabla

	p_n	p_{n-1}	p_{n-2}	$\cdots$	p_1	p_0
a	0	aq_{n-1}	aq_{n-2}	$\ldots$	aq_1	aq_0
	q_{n-1}	q_{n-2}	q_{n-3}	$\cdots$	q_0	r

en la que los q_i se obtienen, de izquierda a derecha, sumando los dos elementos que están encima. Entonces $q = q_0 + q_1X + \cdots + q_{n-1}X^{n-1}$ es el cociente de la división de p entre $X - a$, y r es su resto.

3.2.4 ¿Para qué cuerpos es válida la fórmula usual ($\frac{-b\pm\sqrt{b^2-4ac}}{2a}$) para el cálculo de las raíces de un polinomio aX^2+bX+c de grado 2?

3.2.5 Sea p un entero primo. Demostrar que los polinomios X^p-X y $\prod_{i=1}^{p}(X-i)$ de $\mathbb{Z}_p[X]$ son iguales y deducir una nueva demostración del Teorema de Wilson: $(p-1)!\equiv -1 \bmod p$. (Indicación: Para la primera parte, considerar las raíces de ambos polinomios.)

3.2.6 Hemos observado que la Proposición 3.8 no se verifica para polinomios sobre un anillo que no sea un dominio. Comprobar que en este caso ni siquiera se verifica la afirmación sobre la finitud del número de raíces; es decir, dar un ejemplo de un polinomio no nulo en una indeterminada con infinitas raíces.

3.2.7 [*] Sea A un anillo. Demostrar que si $P\in A[X]$ es un divisor de cero en $A[X]$, entonces existe $0\neq a\in A$ tal que $aP=0$. (Indicación: Elegir un polinomio $Q\neq 0$ de grado mínimo entre los que satisfacen $PQ=0$ y demostrar por inducción que $p_iQ=0$, donde $p_0,p_1,\ldots,p_n$ son los coeficientes de P.)

3.2.8 Si K es un cuerpo de característica 0, ¿qué polinomios $P\in K[X]$ verifican $P'=0$? ¿Y si la característica es un primo p?

3.2.9 Sea D un dominio y sea $P\in D[X]$ el polinomio

$$P=nX^{n+2}-(n+2)X^{n+1}+(n+2)X-n$$

($n\in\mathbb{Z}^+$). Demostrar que la multiplicidad de 1 como raíz de P es al menos 3, y que es exactamente 3 si la característica de D es 0. (Advertencia: El caso de característica 2 ha de ser considerado aparte.)

3.2.10 Demostrar que si $0\neq a\in K$, siendo K un cuerpo de característica 0, entonces X^n-a no tiene raíces múltiples en ningún cuerpo que contenga a K como subcuerpo. ¿Qué se puede afirmar si K es un cuerpo de característica p, con p primo.

3.2.11 Dados dos polinomios $P,Q\in A[X]$, se define su *composición* $P(Q)$ de forma natural utilizando la PUAP. Demostrar que se satisface la *regla de la cadena* para la derivada de la composición: $(P(Q))'=P'(Q)\cdot Q'$.

3.2.12 Demostrar la fórmula de Leibnitz para el cálculo de las derivadas sucesivas de un producto de polinomios:

$$(PQ)^{(n)}=\sum_{i=0}^{n}\binom{n}{i}P^{(n-i)}Q^{(i)}.$$

3.2.13 Sean K un cuerpo, $P\in K[X]$ un polinomio no constante y $K_1=K[X]/(P)$. ¿Cuál es la dimensión de K_1 como espacio vectorial sobre K? Si K es finito, ¿qué cardinal tendrá K_1?

3.2.14 Demostrar que si P es un polinomio irreducible con coeficientes en $\mathbb{Z}_p$ entonces $\mathbb{Z}_p[X]/(P)$ es un cuerpo con p^n elementos. Construir cuerpos de 4, 8, 16, 9, 27 y 121 elementos.

3.2.15 (Kronecker) Sea K un cuerpo y sea $P \in K[X] \setminus K$. Demostrar existe un cuerpo K' que contiene a K como subcuerpo y tiene una raíz de P. Deducir que existe un cuerpo K' que contiene a K como subcuerpo de forma que P es producto de polinomios de grado 1 con coeficientes en K.

3.2.16 En el Problema 2.1.12 se ha visto que el cardinal de un cuerpo finito K es una potencia de un número primo (de hecho, una potencia de la característica de K). En este problema, fijado un entero primo positivo p, vamos a ver que existen cuerpos[1] de cardinal p^n para cada $n \in \mathbb{Z}^+$.

(1) Sea K un cuerpo de característica p (entero positivo primo), y sea $n \in \mathbb{Z}^+$. Demostrar que el conjunto de las raíces en K del polinomio $X^{p^n} - X$ es un subcuerpo finito de K. (Indicación: Usar el Problema 2.1.11.)

(2) Deducir que, para cada $n \in \mathbb{Z}^+$, existe un cuerpo de cardinal p^n.

3.2.17 Calcular todos los polinomios mónicos irreducibles de grado ≤ 4 en $K[X]$, cuando K es cada uno de los cuerpos $\mathbb{Z}_p$ con p primo menor o igual que 11. ¿Te atreves con los cuerpos K construidos en el Problema 3.2.14?

3.3 Divisibilidad en anillos de polinomios

La siguiente proposición caracteriza cuándo un anillo de polinomios es un DIP o dominio euclídeo y cuáles son los irreducibles en tal caso.

Proposición 3.13 *Para un anillo A, las condiciones siguientes son equivalentes:*

(1) $A[X]$ es un dominio euclídeo.

(2) $A[X]$ es un dominio de ideales principales.

(3) A es un cuerpo.

En este caso, un polinomio $f \in A[X]$ es irreducible si y solo si es primo si y solo si $\mathrm{gr}(f) > 0$ *y f no es producto de dos polinomios de grado menor; es decir, si una igualdad $f = gh$ en $A[X]$ implica que* $\mathrm{gr}(g) = \mathrm{gr}(f)$ *(y* $\mathrm{gr}(h) = 0$*) ó* $\mathrm{gr}(h) = \mathrm{gr}(f)$ *(y* $\mathrm{gr}(g) = 0$*).*

[1] De hecho, salvo isomorfismos, existe un único cuerpo de cardinal q para cada entero positivo $q > 1$ que sea potencia de primo. La demostración de este hecho se verá en la asignatura *Ecuaciones Algebraicas*. Este único cuerpo de cardinal q se suele denotar por $\mathbb{F}_q$; en particular, para p primo, se tiene $\mathbb{F}_p = \mathbb{Z}_p$.

Demostración. Ya sabemos que (1) implica (2) por el Teorema 2.29 y que (3) implica (1) por el Ejemplo 2.27.(2). Claramente el polinomio X es irreducible, con lo que si $A(X)$ es DIP entonces el ideal (X) es máximal. Si $a \in A\setminus\{0\}$ entonces $a \notin (X)$ con lo que de la maximalidad de (X) deducimos que $(a, X) = A[X]$ y por tanto $1 = aP + XQ$ para ciertos $P, Q \in A[X]$. Luego $1 = aP(0)$, con lo que a es invertible en A. Esto demuestra que A es un cuerpo.

Dejamos que el lector demuestre la afirmación sobre los polinomios irreducibles. ∎

Obsérvese que si $a \in A$ y $f \in A[X]$ entonces $a|f$ si y solo si a divide a todos los coeficientes de A.

Lema 3.14 *Sea D un dominio y sea $p \in D$.*

(1) p es irreducible en D si y solo si lo es en $D[X]$.

(2) Si p es primo en $D[X]$ entonces lo es en D.

(3) Si además D es un DFU entonces las condiciones siguientes son equivalentes:

(a) p es irreducible en D.

(b) p es irreducible en $D[X]$.

(c) p es primo en D.

(d) p es primo en $D[X]$.

Demostración. (1) y (2) son consecuencias casi inmediatas del Lema 3.1. Para demostrar (3) basta demostrar (c) implica (d) pues ya sabemos que (d) implica (b) (Proposición 2.13), que (a) y (c) son equivalentes, (Lema 2.21) y que (a) y (b) son equivalentes (apartado 1).

Supongamos por tanto que p es primo en D, y veamos que lo es en $D[X]$. Para ello, sean

$$a = a_0 + \cdots + a_n X^n \qquad \text{y} \qquad b = b_0 + \cdots + b_m X^m$$

polinomios de $D[X]$ tales que $p \nmid a$ y $p \nmid b$, y veamos que $p \nmid ab$. Por hipótesis, existen un menor índice i tal que $p \nmid a_i$, y un menor índice j tal que $p \nmid b_j$. El coeficiente de grado $i + j$ de ab es

$$c_{i+j} = a_0 b_{i+j} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0,$$

y las condiciones dadas implican que p divide a todos los sumandos excepto a $a_i b_j$, por lo que $p \nmid c_{i+j}$ y en consecuencia $p \nmid ab$. ∎

En el resto de la sección D será un DFU y K su cuerpo de fracciones.

Consideramos la función

$$\varphi : D \setminus \{0\} \to \mathbb{N}_0$$

que a cada $0 \neq a \in D$ le asocia el número $\varphi(a)$ de factores irreducibles en la expresión de a como producto de irreducibles de D, contando repeticiones. Por ejemplo, si $D = \mathbb{Z}$ entonces $\varphi(12) = 3$ y $\varphi(-80) = 5$. Es claro que, si $a, b \in D \setminus \{0\}$, entonces

$$\varphi(ab) = \varphi(a) + \varphi(b) \qquad \text{y} \qquad \varphi(a) = 0 \Leftrightarrow a \in D^*.$$

Lema 3.15 *Si $a \in D$ y $f, g, h \in D[X]$ verifican $af = gh \neq 0$, entonces existen $g_1, h_1 \in D[X]$ tales que*

$$f = g_1 h_1, \qquad \mathrm{gr}(g_1) = \mathrm{gr}(g), \qquad \mathrm{gr}(h_1) = \mathrm{gr}(h).$$

Demostración. Razonamos por inducción en $\varphi(a)$. Si $\varphi(a) = 0$ podemos tomar $g_1 = a^{-1}g$ y $h_1 = h$. Si $\varphi(a) > 0$, existen $p, b \in D$ tales que $a = pb$ y p es primo. Entonces $p \mid af = gh$ en $D[X]$ y, por el Lema 3.14, podemos asumir que $p \mid g$ en $D[X]$. Es decir, existe $\overline{g} \in D[X]$ tal que $g = p\overline{g}$, de donde $\mathrm{gr}(g) = \mathrm{gr}(\overline{g})$. Cancelando p en la igualdad $pbf = af = gh = p\overline{g}h$ obtenemos $bf = \overline{g}h$. Como $\varphi(b) = \varphi(a) - 1 < \varphi(a)$, la hipótesis de inducción nos dice que existen $g_1, h_1 \in D[X]$ tales que $f = g_1 h_1$, $\mathrm{gr}(g_1) = \mathrm{gr}(\overline{g}) = \mathrm{gr}(g)$, y $\mathrm{gr}(h_1) = \mathrm{gr}(h)$, lo que nos da el resultado. ∎

El siguiente resultado relaciona la irreducibilidad de un polinomio sobre D con su irreducibilidad sobre K. Aunque su recíproco es falso en general (piénsese en $2X$ como polinomio sobre $\mathbb{Z}$), pronto veremos que es válido con una condición extra sobre el polinomio (Proposición 3.20).

Lema 3.16 *Si $f \in D[X]$ es irreducible en $D[X]$, entonces es irreducible (y primo) en $K[X]$.*

Demostración. Supongamos que f no es irreducible en $K[X]$. Por la Proposición 3.13, existen $G, H \in K[X]$ tales que

$$f = GH, \qquad \mathrm{gr}(G) > 0, \qquad \mathrm{gr}(H) > 0.$$

Si $0 \neq b \in D$ es un múltiplo común de los denominadores de los coeficientes de G, se tiene $g = bG \in D[X]$, y análogamente existe $0 \neq c \in D$ tal que $h = cH \in D[X]$. Aplicando el Lema 3.15 a la igualdad $(bc)f = gh$ obtenemos $g_1, h_1 \in D[X]$ tales que $f = g_1 h_1$, $\mathrm{gr}(g_1) = \mathrm{gr}(g) = \mathrm{gr}(G) > 0$, y $\mathrm{gr}(h_1) = \mathrm{gr}(h) = \mathrm{gr}(H) > 0$, lo que nos da una factorización no trivial de f en $D[X]$. ∎

Podemos ya demostrar el resultado principal de esta sección:

Teorema 3.17 *D es un DFU si y solo si lo es $D[X]$.*

Demostración. Supongamos primero que $D[X]$ es un DFU. Entonces D es un dominio (Corolario 3.2), y cada $0 \neq a \in D \setminus D^*$ es producto de irreducibles de $D[X]$, que tendrán grado 0 pues lo tiene a. Por el Lema 3.14, ésa será una factorización de a en irreducibles de D. Del mismo lema se deduce que todo irreducible de D es primo en D, por lo que D es un DFU.

Supongamos ahora que D es un DFU y veamos que lo es $D[X]$. Empezaremos demostrando que cada $a = a_0 + \cdots + a_n X^n \in D[X]$ (con $a_n \neq 0$) no invertible es producto de irreducibles, y lo haremos por inducción en $n + \varphi(a_n)$. Obsérvese que a es invertible si y solo si $n + \varphi(a_n) = 0$. El caso $n + \varphi(a_n) = 1$ se resuelve fácilmente. Supongamos pues que $n + \varphi(a_n) > 1$ y que a no es irreducible. Entonces existen

$$b = b_0 + \cdots + b_m X^m \quad (b_m \neq 0) \qquad \text{y} \qquad c = c_0 + \cdots + c_k X^k \quad (c_k \neq 0)$$

en $D[X]$, no invertibles, con $a = bc$ y b y c elementos de $D[X]$ que no son unidades de $D[X]$. Entonces

$$0 < m + \varphi(b_m), \quad 0 < k + \varphi(c_k) \quad \text{y} \quad n + \varphi(a_n) = m + k + \varphi(b_m) + \varphi(c_k).$$

En consecuencia, podemos aplicar la hipótesis de inducción a b y c, y pegando las factorizaciones así obtenidas conseguimos una factorización en irreducibles de a.

Por la Proposición 2.22, solo falta demostrar que todo irreducible f de $D[X]$ es primo, y por el Lema 3.14 podemos suponer que $\mathrm{gr}(f) \geq 1$. Sean pues $g, h \in D[X]$ tales que $f \mid gh$ en $D[X]$, y veamos que $f \mid g$ ó $f \mid h$ en $D[X]$. Obviamente, $f \mid gh$ en $K[X]$, y como f es primo en $K[X]$ por el Lema 3.16, podemos asumir que $f \mid g$ en $K[X]$. Es decir, existe $G \in K[X]$ tal que $g = fG$, y si demostramos que $G \in D[X]$ habremos terminado. Para ello, tomando $a \in D$ con $aG \in D[X]$ y $\varphi(a)$ mínimo, basta ver que $\varphi(a) = 0$. Supongamos que $\varphi(a) > 0$ y sean $p, b \in D$ con $a = pb$ y p primo. Entonces, en $D[X]$, se tiene $p \mid ag = f(aG)$. Como p es primo en $D[X]$ (Lemma 3.14) y $p \nmid f$ (pues f es irreducible y $\mathrm{gr}(f) \geq 1$), deducimos que $p \mid aG$ en $D[X]$. Si $g_1 \in D[X]$ verifica $aG = pg_1$ entonces $bG = g_1 \in D[X]$, contra la minimalidad de $\varphi(a)$, y esta contradicción termina la demostración. ∎

De la Proposición 3.13 y el Teorema 3.17 se deduce que $\mathbb{Z}[X]$ es un DFU pero no un DIP, lo que muestra que el recíproco del Teorema 2.25 no es cierto.

En el resto de la sección suponemos que D es un DFU y K es su cuerpo de fracciones.

Definimos una relación de equivalencia $\sim$ en K de la siguiente forma para $x, y \in K$:

$$x \sim y \Leftrightarrow y = ux \text{ para algún } u \in D^*.$$

Claramente la clase de equivalencia que contiene a x es $xD^* = \{xu : u \in D^*\}$. En particular, si $x \in D$ entonces la clase de equivalencia que contiene a x está formada por los elementos que son asociados de x en D. Por ejemplo, $0D^* = \{0\}$, $1D^* = D^*$. Obsérvese que $xyD^* = \{xa : a \in yD^*\} = x(yD^*)$.

Podemos definir una multiplicación de elementos de K por elementos de $K/\sim$ poniendo

$$a(bD^*) = (ab)D^*.$$

Esto está bien definido pues si $b_1 \sim b_2$ entonces $ab_1 \sim ab_2$. Además se verifica $a(b(cD^*)) = (ab)(cD^*)$.

Vamos a definir una aplicación

$$c : K[X] \to K/\sim$$

Empezamos definiendo $c(p)$ para $p \in D[X]$ como la clase que contiene a un máximo común divisor de los coeficientes de p, o sea, si $p = \sum_{i \geq 0} p_i X^i$ entonces

$$c(p) = \mathrm{mcd}(p_i : i \geq 0)D^*.$$

Para definir $c(p)$ para un elemento $p \in K[X]$ elegimos $a \in D \setminus \{0\}$ con $ap \in D[X]$ y definimos

$$c(p) = a^{-1}c(ap).$$

Esto está bien definido pues si $a_1p, a_2p \in D[X]$ entonces $c(a_1a_2p) = a_1c(a_2p) = a_2c(a_1p)$ con lo que $a_1^{-1}c(a_1p) = a_2^{-1}c(a_2p)$.

Si $c(p) = aD^*$, entonces decimos que a es el *contenido* y abusaremos de la notación escribiendo $a = c(p)$. En realidad deberíamos decir "un contenido" pero estamos abusando de la notación, de la misma forma que lo hacíamos al hablar "del máximo común divisor" o "el mínimo común múltiplo". En todos los casos se trata de un concepto que es único salvo multiplicación por unidades de D.

Obsérvese que si $a \in D$ y $p \in D[X]$ entonces las notaciones $a \mid c(p)$ y $c(p) \mid a$ no son ambiguas pues todos los valores posibles para $c(p)$ son asociados.

Veamos ahora algunas propiedades del contenido.

Proposición 3.18 *Sean D un DFU y K su cuerpo de fracciones. Sean $a \in K$ y $p \in K[X]$.*

(1) Si $a \in D$ y $p \in D[X]$ entonces $a \mid p$ en $D[X]$ si y solo si $a \mid c(p)$ en D.

(2) $c(ap) = ac(p)$.

(3) $p \in D[X]$ si y solo si $c(p) \in D$.

Demostración. Pongamos $b = c(p)$.

(1) Supongamos que $a \in D$ y $p \in D[X]$. Entonces b es máximo común divisor de los coeficientes de p. Luego $a \mid p$ en $D[X]$ si y solo si a divide a cada uno de los coeficientes de p (en D) si y solo si a divide a b.

(2) Es consecuencia inmediata de la fórmula $\operatorname{mcd}(ap_0, ap_1, \ldots, ap_n) = a \operatorname{mcd}(p_0, p_1, \ldots, p_n)$.

(3) Obviamente si $p \in D[X]$ entonces $b \in D$. Para demostrar la otra implicación ponemos $p = \sum_{i=0}^{k} \frac{r_i}{s_i} X^i$ donde cada $\frac{r_i}{s_i}$ es una fracción reducida, entendiendo que si $r_i = 0$ entonces $s_i = 1$. Supongamos que $p \notin D[X]$. Eso implica que algún s_i nos es unidad de D con lo que es divisible por un irreducible q y por tanto $q \nmid r_i$. Ponemos $s_i = q^{n_i}h_i$ con $q \nmid h_i$ para cada i y tomamos $n = n_i = \max(n_0, n_1, \ldots, n_k) \geq 1$ y $m = \operatorname{mcm}(s_0, \ldots, s_k)$. Entonces $m = q^n h$ con $h \in D$ y $q \nmid h$ en D. Además $mp \in D[X]$ y $c(mp) = mbD^*$. Pero $m\frac{r_i}{s_i} = \frac{hr_i}{h_i}$ es el coeficiente de X^i en mp, que es un elemento de D que no es múltiplo de q. Luego mb, que es el máximo común divisor de los coeficientes de mp, no es múltiplo de q en D. Pero m es un elemento de D que sí es múltiplo de q en D. Por tanto $b \notin D$. ∎

Diremos que un polinomio es *primitivo* si $c(p) = 1$. Es decir $p \in D[X]$ es primitivo si los únicos divisores de p en $D[X]$ que tienen grado 0 son las unidades de $D[X]$. Obsérvese que para todo $0 \neq p \in D[X]$ se tiene que $p/c(p)$ es primitivo y de hecho $c = c(p)$ si y solo si $p = cp_1$ con $p_1 \in D[X]$, primitivo.

Lema 3.19 (Lema de Gauss) *Si $f, g \in K[X]$, entonces $c(fg) = c(f)c(g)$. En particular, fg es primitivo si y solo si f y g son primitivos.*

Demostración. Tenemos $f = c(f)f_1$ y $g = c(g)g_1$ con f_1 y g_1 primitivos. Por tanto $fg = c(f)c(g)f_1g_1$, luego para demostrar que $c(fg) = c(f)c(g)$ basta probar que f_1g_1 es primitivo. En caso contrario $c(f_1g_1)$ tendría un divisor irreducible p en D. Eso implica que $p|f_1g_1$. Por

el Lema 3.14, p es primo en $D[X]$ y por tanto $p|f_1$ ó $p|g_1$, lo que implica que $p|c(f_1)$ ó $p|c(g_1)$, en contra de que $c(f_1) = c(g_1) = 1$. ∎

Proposición 3.20 *Para un polinomio primitivo $f \in D[X] \setminus D$, las condiciones siguientes son equivalentes:*

(1) f es irreducible en $D[X]$.

(2) f es irreducible en $K[X]$.

(3) Si $f = GH$ con $G, H \in K[X]$ entonces $\mathrm{gr}(G) = 0$ ó $\mathrm{gr}(H) = 0$.

(4) Si $f = gh$ con $g, h \in D[X]$ entonces $\mathrm{gr}(g) = 0$ ó $\mathrm{gr}(h) = 0$.

Demostración. El Lema 3.16 y la Proposición 3.13 aseguran que (1) implica (2) y que (2) implica (3), respectivamente, y es claro que (3) implica (4). Finalmente, como f es primitivo, sus únicos divisores de grado 0 son unidades, por lo que (4) implica (1). ∎

Como consecuencia del Lema 3.14 y la Proposición 3.20 se deduce el siguiente corolario.

Corolario 3.21 *Si D es un DFU y K es su cuerpo de fracciones, entonces los irreducibles de $D[X]$ son los irreducibles de D y los polinomios primitivos de $D[X] \setminus D$ que son irreducibles en $K[X]$.*

Problemas

3.3.1 ¿Es cierto que, si D es un DFU y b es un elemento de D, entonces sólo hay una cantidad finita de ideales de D que contienen a b? ¿Y si D es DIP?

3.3.2 Dar un ejemplo de un ideal primo no nulo de un DFU que no sea maximal.

3.3.3 Demostrar que toda raíz racional de un polinomio mónico con coeficientes enteros es entera.

3.4 Factorización en el anillo de polinomios de un DFU

Nuestro siguiente objetivo es factorizar polinomios en $D[X]$ y en $K[X]$, donde D sigue siendo un DFU y K su cuerpo de fracciones. Para ello es necesario disponer de métodos que nos digan cuándo un polinomio es irreducible. Como se verá, pocos de los resultados prácticos que obtendremos nos dan condiciones necesarias y suficientes para que un polinomio sea irreducible. Asumiremos que disponemos de un método para factorizar los elementos de D, y en particular para decidir si son irreducibles o no. Esto es teóricamente posible si $D = \mathbb{Z}$ ó $D = \mathbb{Z}[i]$ (y también lo es en la práctica en los casos que se nos presentarán), y nos permite además decidir si un polinomio de $D[X]$ es o no primitivo.

En general, dado un polinomio $0 \neq f \in D[X]$, calcularemos $d = c(f)$ y obtendremos $f = df_1$, con $f_1 \in D[X]$ primitivo. El polinomio constante d es una unidad en $K[X]$, mientras

que en $D[X]$ tiene la misma factorización en irreducibles que tenga como elemento de D. En cuanto a f_1, para decidir su irreducibilidad, la Proposición 3.20 nos permite considerarlo como polinomio sobre D o sobre K según nos convenga. Por tanto, es importante tener criterios de irreducibilidad como los que siguen para polinomios sobre cuerpos. Para polinomios de grado pequeño esto es fácil.

Lema 3.22 *Sea K un cuerpo y sea $f \in K[X]$. Entonces*

(1) Si $\mathrm{gr}(f) = 1$ entonces f es irreducible en $K[X]$.

(2) Si $\mathrm{gr}(f) > 1$ y f tiene una raíz en K, entonces f no es irreducible en $K[X]$.

(3) Si $\mathrm{gr}(f) = 2$ ó 3 entonces f es irreducible en $K[X]$ si y solo si f no tiene raíces en K.

Demostración. Ejercicio. ∎

El Lema 3.22 pone de manifiesto la importancia de encontrar raíces de un polinomio para decidir si es irreducible. Cuando los coeficientes están en un DFU podemos seleccionar los "candidatos a raíces":

Proposición 3.23 *Sea D un DFU con cuerpo de fracciones K, y sea $f = a_0 + a_1X + \cdots + a_nX^n \in D[X]$ con $a_n \neq 0$. Entonces todas las raíces de f en K son de la forma r/s, donde $r \mid a_0$ y $s \mid a_n$.*

Demostración. Sea $t = \frac{r}{s}$ una raíz de f con $r, s \in D$ primos entre sí. Multiplicando la igualdad $f(t) = 0$ por s^n obtenemos

$$a_0s^n + a_1rs^{n-1} + a_2r^2s^{n-2} + \cdots + a_{n-1}r^{n-1}s + a_nr^n = 0,$$

luego $r \mid a_0s^n$ y $s \mid a_nr^n$. Como r y s son coprimos, deducimos que $r \mid a_0$ y $s \mid a_n$. ∎

Ejemplos 3.24 *Factorizaciones de polinomios.*

(1) La no existencia de raíces no garantiza la irreducibilidad de polinomios de grado mayor que 3. Por ejemplo, $X^4 + 2X^2 + 1 = (X^2 + 1)^2$ es reducible en $\mathbb{R}[X]$ pero no tiene raíces reales.

(2) Las posibles raíces en $\mathbb{Q}$ del polinomio $f = 3X^3 + X^2 + X - 2$ son ± 2, ± 1, $\pm 2/3$ y $\pm 1/3$, y de hecho $f(2/3) = 0$. Por tanto $(X - 2/3) \mid f$, y así $(3X - 2) \mid f$. Dividiendo se obtiene $f = (3X - 2)(X^2 + X + 1)$. Como ambos factores son primitivos sobre $\mathbb{Z}$ e irreducibles sobre $\mathbb{Q}$ y sobre $\mathbb{R}$, deducimos que la anterior es una factorización en irreducibles de f en cualquiera de los anillos $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ ó $\mathbb{R}[X]$. La factorización en $\mathbb{C}[X]$ es $f = (3X - 2)(X - \omega)(X - \overline{\omega})$, donde $\omega = \frac{-1+\sqrt{-3}}{2}$.

(3) El polinomio $f = 6X^4 + 6X^2 + 18X - 30 = 2 \cdot 3 \cdot (X^4 + X^2 + 3X - 5)$ tiene al 1 por raíz, y dividiendo se tiene $X^4 + X^2 + 3X - 5 = (X - 1)(X^3 + X^2 + 2X + 5)$. El factor cúbico es primitivo y no tiene raíces en $\mathbb{Q}$ (al sustituir ± 1 ó ± 5 se obtiene un entero impar), por lo que

$$f = 2 \cdot 3 \cdot (X - 1)(X^3 + X^2 + 2X + 5) \qquad \text{y} \qquad f = 6(X - 1)(X^3 + X^2 + 2X + 5)$$

son las factorizaciones de f en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$, respectivamente (en la segunda el 6 no es un factor irreducible, sino una unidad). El polinomio cúbico no es irreducible en $\mathbb{R}[X]$ ni en $\mathbb{C}[X]$. De hecho, un análisis del crecimiento de la función polinómica $f : \mathbb{R} \to \mathbb{R}$ nos lleva a la conclusión de que f tiene una raíz real y dos complejas conjugadas.

(4) El polinomio $f = X^4+X^3+2X^2+X+1$ no tiene raíces racionales, pero esto no implica que sea irreducible sobre $\mathbb{Q}$. De hecho, se tiene $f(i) = 0$, y por tanto $(X-i)(X+i) = X^2+1$ divide a f; el otro factor es $X^2 + X + 1$, por lo que $f = (X^2 + 1)(X^2 + X + 1)$ es una factorización en irreducibles en $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ ó $\mathbb{R}[X]$, y $f = (X - i)(X + i)(X - \omega)(X - \overline{\omega})$ (con $\omega = \frac{-1+\sqrt{-3}}{2}$) es una factorización en $\mathbb{C}[X]$.

(5) Supongamos que el polinomio sin raíces racionales $f = X^4-2X^3+6X-3$ no es irreducible en $\mathbb{Z}[X]$. Por la Proposición 3.20, existen $g, h \in \mathbb{Z}[X]$, ambos de grado ≥ 1, tales que $f = gh$. Podemos asumir que g y h son mónicos (¿por qué?), y por tanto no pueden tener grado 1 (¿por qué?). En consecuencia, ambos tienen grado 2 y por tanto existen $a, b, c, d \in \mathbb{Z}$ tales que $f = (X^2 + aX + b)(X^2 + cX + d)$. Igualando coeficientes, se obtienen las ecuaciones

$$bd = -3, \quad ad + bc = 6, \quad b + ac + d = 0, \quad a + c = -2.$$

La primera ecuación nos da 4 opciones para los valores de b y d. Una de ellas es $b = 1$ y $d = -3$, que sustituida en la segunda ecuación y combinada con la cuarta nos dice que $a = -2$ y $c = 0$; pero estos valores no satisfacen la tercera ecuación. De modo similar se ve que las otras opciones tampoco funcionan, lo que significa que no existen tales $a, b, c, d \in \mathbb{Z}$ y en consecuencia f es irreducible en $\mathbb{Z}[X]$, y por tanto también en $\mathbb{Q}[X]$.

El último ejemplo muestra lo penoso que puede resultar estudiar la irreducibilidad de un polinomio, incluso de grado bajo, con los métodos que hemos desarrollado hasta ahora. El resto de esta sección lo dedicamos a presentar otros dos criterios de irreducibilidad para polinomios sobre un DFU que son a menudo útiles.

En el primero de ellos usaremos el Ejemplo 3.4.(3).

Un homomorfismo de anillos $\phi : A \to B$ induce otro $A[X] \to B[X]$ dado por

$$f = \sum a_i X^i \mapsto \phi(f) = \sum \phi(a_i) X^i.$$

En general se tiene $\text{gr}(\phi(f)) \leq \text{gr}(f)$, con igualdad si el coeficiente principal de f no está en Ker ϕ.

Proposición 3.25 (Criterio de Reducción) *Sea $\phi : D \to K$ un homomorfismo de anillos, donde D es un DFU y K es un cuerpo, y sea f un polinomio primitivo de $D[X] \setminus D$. Si $\phi(f)$ es irreducible en $K[X]$ y $\mathrm{gr}(\phi(f)) = \mathrm{gr}(f)$, entonces f es irreducible en $D[X]$ (o lo que es lo mismo en $K[X]$).*

Demostración. Por la Proposición 3.20 basta ver que, si $f = gh$ con $g, h \in D[X]$, entonces $\mathrm{gr}(g) = 0$ ó $\mathrm{gr}(h) = 0$. Sean a, b y c los coeficientes principales de f, g y h, respectivamente. Entonces $a = bc \notin \mathrm{Ker}\ \phi$ y por tanto $b, c \notin \mathrm{Ker}\ \phi$, por lo que $\mathrm{gr}(\phi(g)) = \mathrm{gr}(g)$ y $\mathrm{gr}(\phi(h)) = \mathrm{gr}(h)$. Como K es un cuerpo y $\phi(f)$ es irreducible en $K[X]$, la igualdad $\phi(f) = \phi(g)\phi(h)$ implica que $\mathrm{gr}(\phi(g)) = 0$ ó $\mathrm{gr}(\phi(h)) = 0$, de donde se sigue el resultado. ∎

Cuando consideramos la proyección $\mathbb{Z} \to \mathbb{Z}_p$, con p un número primo positivo, el homomorfismo $\mathbb{Z}[X] \to \mathbb{Z}_p[X]$ viene dado por

$$f = \sum a_i X^i \mapsto \overline{f} = \sum \overline{a_i} X^i,$$

donde $\overline{a}$ es la clase de a en $\mathbb{Z}_p$. Aplicando el Criterio de Reducción se obtiene:

Corolario 3.26 *Sea p un entero primo y sea $f = a_0 + \cdots + a_n X^n$ un polinomio primitivo de $\mathbb{Z}[X]$. Si $p \nmid a_n$ y $\overline{f}$ es irreducible en $\mathbb{Z}_p[X]$, entonces f es irreducible en $\mathbb{Z}[X]$.*

Ejemplos 3.27 *Aplicaciones del Criterio de Reducción.*

(1) Reduciendo módulo 2 el polinomio $f = 7X^3+218X^2+121X+625$ obtenemos el polinomio $\overline{f} = X^3 + X + 1$ de $\mathbb{Z}_2[X]$, que es irreducible porque no tiene raíces. Por tanto f es irreducible en $\mathbb{Z}[X]$ (y en $\mathbb{Q}[X]$).

(2) Reduciendo $f = X^4 + 5X + 1 \in \mathbb{Z}[X]$ módulo 2 obtenemos $\overline{f} = X^4 + X + 1 \in \mathbb{Z}_2[X]$. Como $\overline{f}$ no tiene raíces en $\mathbb{Z}_2$, si no fuera irreducible se factorizaría como producto de dos polinomios irreducibles de grado 2 en $\mathbb{Z}_2[X]$. Pero en $\mathbb{Z}_2[X]$ solo hay 4 polinomios de grado 2, y de ellos solo $X^2 + X + 1$ es irreducible (¿por qué?). Como $\overline{f}$ no es el cuadrado de éste, deducimos que $\overline{f}$ es irreducible en $\mathbb{Z}_2[X]$ y por tanto f es irreducible en $\mathbb{Z}[X]$.

(3) Consideremos el polinomio $f = X^5 - X - 1$ de $\mathbb{Z}[X]$. Reduciendo módulo 2 obtenemos un polinomio que es divisible por $X^2 + X + 1$, por lo que no podemos aplicar el Criterio de Reducción. Reduciendo módulo 3 obtenemos $\overline{f} = X^5 + 2X + 2 \in \mathbb{Z}_3[X]$, que no tiene raíces. Si no fuera irreducible tendría un factor irreducible de grado 2; es fácil ver que los únicos irreducibles mónicos de grado 2 de $\mathbb{Z}_3[X]$ son

$$X^2 + 1, \qquad X^2 + X - 1, \qquad X^2 - X - 1.$$

Comprobando que ninguno de ellos divide a $\overline{f}$ deducimos que $\overline{f}$ es irreducible en $\mathbb{Z}_3[X]$, y por tanto f es irreducible en $\mathbb{Z}[X]$.

(4) Dado el polinomio $f = X^4 + 4X + 1$ en $\mathbb{Z}[X]$, se tiene $\overline{f} = (X + 1)^4$ en $\mathbb{Z}_2[X]$ y $\overline{f} = (X + 2)(X^3 + X^2 + X + 2)$ en $\mathbb{Z}_3[X]$, con el factor cúbico irreducible porque no tiene raíces. Por tanto, no podemos aplicar el Criterio de Reducción. Sin embargo, la

factorización en $\mathbb{Z}_3[X]$ nos va a permitir demostrar que f es irreducible en $\mathbb{Z}[X]$. En efecto, como f no tiene raíces en $\mathbb{Q}$, si no fuera irreducible en $\mathbb{Z}[X]$ se tendría $f = gh$ con $\mathrm{gr}(g) = \mathrm{gr}(h) = 2$. Esto nos daría, en $\mathbb{Z}_3$, la factorización $\overline{f} = \overline{g}\overline{h}$ con $\mathrm{gr}(\overline{g}) = \mathrm{gr}(\overline{h}) = 2$, incompatible con la factorización en irreducibles (única salvo asociados) que acabamos de obtener.

Veamos nuestro último criterio de irreducibilidad:

Proposición 3.28 (Criterio de Eisenstein) *Sea D un DFU y sea $f = a_0 + a_1X + \cdots + a_nX^n$ (con $a_n \neq 0$) un polinomio primitivo de $D[X]$. Si existe un irreducible $p \in D$ tal que*

$$p \mid a_i \text{ para todo } i < n, \qquad y \qquad p^2 \nmid a_0,$$

entonces f es irreducible en $D[X]$.

Demostración. Veamos que, si $f = gh$ en $D[X]$, entonces $\mathrm{gr}(g) = n$ ó $\mathrm{gr}(h) = n$. Pongamos $g = b_0 + \cdots + b_mX^m$ y $h = c_0 + \cdots + c_kX^k$, con $b_mc_k \neq 0$. Como $p^2 \nmid a_0 = b_0c_0$, entonces $p \nmid b_0$ ó $p \nmid c_0$. Supongamos que se da la segunda opción. Como f es primitivo se tiene $p \nmid g$, y por tanto existe

$$i = \min\{j : p \nmid b_j\}.$$

Entonces p no divide a $a_i = (\sum_{j=0}^{i-1} b_jc_{i-j}) + b_ic_0$, y por tanto $i = n$, de modo que $\mathrm{gr}(g) = n$. La opción $p \nmid b_0$ nos llevaría a $\mathrm{gr}(h) = n$, lo que demuestra el resultado. ∎

Ejemplos 3.29 *Aplicaciones del Criterio de Eisenstein.*

(1) Sean a un entero y p un primo cuya multiplicidad en a es 1. Entonces $X^n - a$ es irreducible.

(2) Un argumento similar al del Ejemplo 3.27.(4) nos permitiría ver que el polinomio $f = X^4 - 3X^3 + 6X - 3$ es irreducible en $\mathbb{Z}[X]$. Ahora podemos asegurar lo mismo con menos trabajo aplicando el Criterio de Eisenstein con $p = 3$.

(3) A menudo, el Criterio de Eisenstein se combina con un automorfismo de $\mathbb{Z}[X]$ de sustitución en $X + a$ (Ejemplos 3.4). Por ejemplo, el criterio no es aplicable a $f(X) = X^4+4X^3+10X^2+12X+7$, pero sí se puede aplicar (con $p = 2$) a $f(X-1) = X^4+4X^2+2$. Por tanto $f(X - 1)$ es irreducible, y en consecuencia lo es $f(X)$.

(4) Dado un entero $n \geq 3$, las raíces en $\mathbb{C}$ del polinomio $X^n - 1$ se llaman *raíces n-ésimas* de la unidad (o de 1). Considerando la interpretación geométrica de la multiplicación en $\mathbb{C}$, es fácil ver que estas raíces son exactamente los n vértices del n-ágono regular inscrito en el círculo unidad de $\mathbb{C}$ que tiene un vértice en la posición del 1. Estos números complejos son útiles en muy diversas circunstancias. El polinomio $X^n - 1$ se factoriza como

$$X^n - 1 = (X - 1)\Phi_n(X), \qquad \text{donde } \Phi_n(X) = X^{n-1} + X^{n-2} + \cdots + X^2 + X + 1.$$

El polinomio $\Phi_n(X)$ se conoce como el n-ésimo *polinomio ciclotómico*, y sus raíces son las raíces n-ésimas de 1 distintas de 1. $\Phi_n(X)$ no es en general irreducible sobre $\mathbb{Q}$ (por ejemplo, $\Phi_4(X)$ es divisible por $X+1$), pero sí lo es cuando $n=p$ es primo. Como en el apartado anterior, esto quedará demostrado si podemos aplicar el Criterio de Eisenstein a $\Phi_p(X+1)$. Ahora bien, $\Phi_p(X) = (X^n-1)/(X-1)$, y por tanto

$$\Phi_p(X+1) = \frac{(X+1)^p-1}{X} = X^{p-1} + \binom{p}{p-1}X^{p-2} + \binom{p}{p-2}X^{p-3} + \cdots + \binom{p}{2}X + p.$$

Cuando $1 \leq i < p$, el primo p no divide a $i!$ ni a $(p-i)!$, y por tanto sí divide a $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$, por lo que podemos aplicar el Criterio de Eisenstein, como queríamos.

Problemas

3.4.1 Sea D un DFU y sea $f = a_o + a_1X + \cdots + a_nX^n$ un polinomio primitivo en $D[X]$. Demostrar que, si existe un irreducible $p \in D$ tal que

$$p \mid a_i \text{ para todo } i > 0, \qquad p \nmid a_0 \qquad \text{y} \qquad p^2 \nmid a_n,$$

entonces P es irreducible en $D[X]$ (es decir, el Criterio de Eisenstein se puede aplicar "al revés").

3.4.2 Descomponer en factores irreducibles el polinomio X^4-4 en cada uno de los siguientes anillos: $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{Z}_2[X]$ y $\mathbb{Z}_3[X]$.

3.4.3 Descomponer los siguientes anillos cociente como producto de anillos "conocidos":

(1) $\mathbb{R}[X]$ módulo el ideal principal generado por el polinomio $X^3 - X^2 + X - 1$.

(2) $\mathbb{Q}[X]$ módulo el ideal principal generado por el polinomio $X^3 - X^2 + X - 1$.

(3) $\mathbb{Q}[X]$ módulo el ideal principal generado por el polinomio $3X^2 - 6$.

3.4.4 Calcular el máximo común divisor y el mínimo común múltiplo en $\mathbb{Z}[X]$ de las siguientes parejas de polinomios:

(1) $X^3 - 6X^2 + X + 4$ y $X^5 - 6X + 1$.

(2) $X^2 + 1$ y $X^6 + X^3 + X + 1$.

(3) $26X^2 - 104X + 104$ y $195X^2 + 65X - 910$.

3.4.5 Demostrar que los siguientes polinomios son irreducibles en los anillos que se indican:

(1) $X^4 + X + 1$, $4X^3 - 3X - \frac{1}{2}$, $X^4 + 1$, $X^6 + X^3 + 1$, $X^3 + 6X + 3X + 3$, $X^5 - 5X + 15$ y $X^4 + 5X + 12$ en $\mathbb{Q}[X]$.

(2) $X^2 + X + 1$ en $\mathbb{Z}_2[X]$.

(3) $X^2 + Y^2 - 1$ y $X^5Y^3 - X^3 + XY^2 - Y^2 + 1$ en $\mathbb{Q}[X, Y]$.

(4) $X^4 + X + a$ con a impar, en $\mathbb{Q}[X]$.

(5) $X^5 + 3aX^4 - 4X + 4$ con $a \in \mathbb{Z}$, en $\mathbb{Q}[X]$.

(6) $Y^3 + X^2Y^2 + X^3Y + X$, en $D[X, Y]$ donde D es un DFU arbitrario.

3.4.6 Factorizar los siguientes polinomios en los anillos que se indican:

(1) $3X^4 - 3X^2 + 6$, en $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

(2) $X^3 + 3X^2 + 3X + 4$ en $\mathbb{Z}_5[X]$.

3.4.7 Decidir cuáles de los siguientes polinomios son irreducibles en los anillos que se indican:

(1) $2X^2 + 2X + 2$ en $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ y $\mathbb{Z}_5[X]$.

(2) $X^4 + 2$ en $\mathbb{Z}_7[X]$ y $\mathbb{Q}[X]$.

(3) $X^3 - 18X^2 + 106X - 203$ en $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$.

(4) $X^5 + X + 2$ en $\mathbb{R}[X]$, $\mathbb{Q}[X]$ y $\mathbb{Z}_3[X]$.

(5) $X^5 + X - 2$ en $\mathbb{R}[X]$, $\mathbb{Q}[X]$ y $\mathbb{Z}_3[X]$.

(6) $2X^5 - 6X^3 + 9X^2 - 15$ en $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$.

(7) $X^4 + 15X^3 + 7$ en $\mathbb{Z}[X]$.

(8) $X^n - p$, donde $n > 0$ y p es un entero primo con $p \equiv 1 \bmod 3$, en $\mathbb{R}[X]$, $\mathbb{Q}[X]$ y $\mathbb{Z}_3[X]$.

3.5 Polinomios en varias indeterminadas

Dados un anillo A y un entero $n \geq 2$, definimos el *anillo de polinomios en n indeterminadas con coeficientes en A*, denotado por $A[X_1, \ldots, X_n]$, mediante la fórmula recurrente

$$A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n].$$

Los elementos $X_1, \ldots, X_n$ de $A[X_1, \ldots, X_n]$ se llaman *indeterminadas* y los elementos de $A[X_1, \ldots, X_n]$ se llaman *polinomios en n indeterminadas*.

Por inducción a partir del Corolario 3.2, de la Proposición 3.13 y del Teorema 3.17, se obtienen fácilmente las siguientes propiedades:

Proposición 3.30 *Para un anillo A y un entero positivo n se verifican:*

(1) $A[X_1, \ldots, X_n]$ nunca es un cuerpo.

(2) $A[X_1, \ldots, X_n]$ es un dominio si y solo si lo es A.

(3) Si A es un dominio, entonces $A[X_1, \ldots, X_n]^* = A^*$.

(4) $A[X_1, \ldots, X_n]$ es un DFU si y solo si lo es A.

(5) $A[X_1, \ldots, X_n]$ es un DIP si y solo si $n = 1$ y A es un cuerpo.

Si $a \in A$ e $i = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$, el elemento $aX_1^{i_1} \cdots X_n^{i_n}$ de $A[X_1, \ldots, X_n]$ se llama *monomio* de *tipo* i y coeficiente a.

Lema 3.31 *Sean A un anillo y n un entero positivo. Entonces todo elemento p de $A[X_1, \ldots, X_n]$ se escribe de forma única como suma de monomios de distinto tipo, casi todos con coeficiente nulo. Es decir, se tiene una única expresión*

$$p = \sum_{i \in \mathbb{N}_0^n} p_i X_1^{i_1} \cdots X_n^{i_n} \tag{3.2}$$

con $p_i = 0$ para casi todo $i = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$.

Demostración. Aplicamos inducción en n, con el caso $n = 1$ obvio por la propia definición de anillo de polinomios en una variable. Cuando $n > 1$, un elemento de $A[X_1, \ldots, X_n]$ es, por definición, de la forma $\sum_{t \in \mathbb{N}_0} p_t X_n^t$ con cada $p_t \in A[X_1, \ldots, X_{n-1}]$ y casi todos los p_t nulos. Por hipótesis de inducción, cada p_t se expresa como

$$p_t = \sum_{(i_1, \ldots, i_{n-1}) \in \mathbb{N}_0^{n-1}} (p_t)_{(i_1, \ldots, i_{n-1})} X_1^{i_1} \cdots X_{n-1}^{i_{n-1}},$$

donde cada $(p_t)_{(i_1, \ldots, i_{n-1})}$ está en A y casi todos son nulos. Definiendo $p_i = (p_{i_n})_{(i_1, \ldots, i_{n-1})}$ (para $i = (i_1, \ldots, i_n)$) tenemos la expresión deseada.

Recíprocamente, una expresión como (3.2) puede reescribirse como un polinomio en X_n con coeficientes en $A[X_1, \ldots, X_{n-1}]$ sin más que definir cada coeficiente como $p_t = \sum p_i X_1^{i_1} \cdots X_{n-1}^{i_{n-1}}$, con la suma extendida a todos los $i = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$ con $i_n = t$. Usando esto es sencillo demostrar que estas expresiones son únicas, asumiendo que lo son en $A[X_1, \ldots, X_{n-1}]$. ∎

Usando la Proposición 3.3 se demuestra fácilmente la siguiente generalización de la Propiedad Universal del Anillo de Polinomios, por inducción en el número de indeterminadas.

Proposición 3.32 *Sean A un anillo, $n \geq 1$ un entero y $u : A \to A[X_1, \ldots, X_n]$ la inclusión.*

(1) **(PUAP en n indeterminadas)** *Dados un homomorfismo de anillos $f : A \to B$ y n elementos $b_1, \ldots, b_n \in B$ (no necesariamente distintos) existe un único homomorfismo de anillos $\overline{f} : A[X_1, \ldots, X_n] \to B$ tal que $\overline{f} \circ u = f$ y $\overline{f}(X_j) = b_j$ para cada $j = 1, \ldots, n$.*

(2) Si dos homomorfismos de anillos $g, h : A[X_1, \ldots, X_n] \to B$ coinciden sobre A y en X_j para cada $j = 1, \ldots, n$ entonces son iguales.

(3) La PUAP en n indeterminadas determina $A[X_1, \ldots, X_n]$ salvo isomorfismos. Supongamos que existen un anillo P con elementos $T_1, \ldots, T_n$ y un homomorfismo de anillos $v : A \to P$ tales que, dados un homomorfismo de anillos $f : A \to B$ y elementos $b_1, \ldots, b_n \in B$, existe un único homomorfismo de anillos $\overline{f} : P \to B$ tal que $\overline{f} \circ v = f$ y $\overline{f}(T_j) = b_j$ para cada $j = 1, \ldots, n$. Entonces existe un isomorfismo $\phi : A[X_1, \ldots, X_n] \to P$ tal que $\phi \circ u = v$ y $\phi(X_j) = T_j$ para cada $j = 1, \ldots, n$.

Como en el caso de una indeterminada, se tiene:

Ejemplos 3.33 *Aplicaciones de la PUAP en n indeterminadas.*

(1) Dados anillos $A \subseteq B$ y elementos $b_1, \ldots, b_n \in B$, existe un homomorfismo $S : A[X_1, \ldots, X_n] \to B$ que es la identidad sobre A y tal que $S(X_j) = b_j$ para cada $j = 1, \ldots, n$. Dado $p \in A[X_1, \ldots, X_n]$, escribiremos a menudo $p(b_1, \ldots, b_n)$ en lugar de $S(p)$. Si $p = \sum_{i \in \mathbb{N}_0^n} p_i X_1^{i_1} \cdots X_n^{i_n}$ es la expresión de p como suma de monomios, entonces

$$S(p) = p(b_1, \ldots, b_n) = \sum_{i \in \mathbb{N}_0^n} p_i b_1^{i_1} \cdots b_n^{i_n}.$$

La imagen de este homomorfismo es el subanillo de B generado por $A \cup \{b_1, \ldots, b_n\}$ y que denotamos por $A[b_1, \ldots, b_n]$.

Supongamos que $f, g : A[b_1, \ldots, b_n] \to C$ son dos homomorfismos de anillos. Entonces $f = g$ si y solo si $f|A = g|A$ y $f(b_i) = g(b_i)$ para todo i. Para demostrar esto basta aplicar la Proposición 3.32 para deducir que $f \circ S = g \circ S$ y concluir que $f = g$, pues S es suprayectiva.

(2) Sea A un anillo y sea σ una biyección del conjunto $\mathbb{N}_n = \{1, \ldots, n\}$ en sí mismo con inversa $\tau = \sigma^{-1}$. Si en el ejemplo anterior tomamos $B = A[X_1, \ldots, X_n]$ y $b_j = X_{\sigma(j)}$, obtenemos un homomorfismo $\overline{\sigma} : A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_n]$ que "permuta las indeterminadas". Es claro que $\overline{\sigma}$ es de hecho un automorfismo con inverso $\overline{\tau}$. Usando estos isomorfismos y la definición de los anillos de polinomios en varias indeterminadas, es fácil establecer isomorfismos

$$A[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \simeq A[X_1, \ldots, X_n][Y_1, \ldots, Y_m] \simeq A[Y_1, \ldots, Y_m][X_1, \ldots, X_n],$$

por lo que, en la práctica, no hay que distinguir entre estos anillos.

(3) Todo homomorfismo de anillos $f : A \to B$ induce un homomorfismo $\overline{f} : A[X_1, \ldots, X_n] \to B[X_1, \ldots, X_n]$ que coincide con f sobre A y verifica $\overline{f}(X_j) = X_j$ para cada $j = 1, \ldots, n$. Si $p = \sum_{i \in \mathbb{N}_0^n} p_i X_1^{i_1} \cdots X_n^{i_n}$ es la expresión de p como suma de monomios, entonces

$$\overline{f}(p) = \sum_{i \in \mathbb{N}_0^n} f(p_i) X_1^{i_1} \cdots X_n^{i_n}.$$

En el futuro este homomorfismo lo denotaremos por f.

Veamos cómo pueden usarse las identificaciones del apartado 2 de los Ejemplos 3.33.

Ejemplo 3.34 *El Criterio de Eisenstein aplicado a polinomios en dos indeterminadas*
El polinomio $f = X^3Y + X^2Y^2 - X^2 + Y^3 + Y^2 \in \mathbb{Q}[X,Y]$ puede considerarse como un polinomio en $\mathbb{Q}[X][Y]$, poniendo $f = Y^3 + (X^2+1)Y^2 + X^3Y - X^2$, o como un polinomio en $\mathbb{Q}[Y][X]$, poniendo $f = YX^3 + (Y^2-1)X^2 + (Y^3+Y^2)$. A esta última expresión le podemos aplicar el Criterio de Eisenstein con el polinomio irreducible $p = Y + 1 \in \mathbb{Q}[Y]$ para deducir que f es irreducible en $\mathbb{Q}[X,Y]$.

Por definición, el *grado de un monomio* $aX_1^{i_1}\cdots X_n^{i_n}$ de $A[X_1,\ldots,X_n]$ es $i_1+\cdots+i_n$. El grado $\mathrm{gr}(p)$ de un polinomio $p \neq 0$ de $A[X_1,\ldots,X_n]$ se define como el mayor de los grados de los monomios que aparecen con coeficiente no nulo en la expresión de p como suma de monomios de distinto tipo. Es claro que, dados dos polinomios p y q, se tiene

$$\mathrm{gr}(p+q) \leq \max\{\mathrm{gr}(p),\mathrm{gr}(q)\} \qquad \text{y} \qquad \mathrm{gr}(pq) \leq \mathrm{gr}(p)+\mathrm{gr}(q).$$

Sin embargo, no es tan fácil como en el caso de una indeterminada ver que, cuando A es un dominio, la segunda desigualdad es de hecho una igualdad. Para esto, y para otras cosas, es interesante considerar el siguiente concepto:

Un polinomio $p \neq 0$ de $A[X_1,\ldots,X_n]$ se dice *homogéneo de grado* $n \geq 0$ si es suma de monomios de grado n. Por ejemplo, de los polinomios de $\mathbb{Z}[X,Y,Z]$

$$X^2Y + Y^3 - 3XYZ + 6YZ^2, \quad X^6 + Y^6 + Z^6 + X^3Y^3 + X^3Z^3 + Y^3Z^3, \quad XYZ + X + Y + Z,$$

los dos primeros son homogéneos (de grados 3 y 6, respectivamente) y el último no lo es.

Proposición 3.35 *Dados un anillo A y un entero $n \geq 1$, todo polinomio de $A[X_1,\ldots,X_n]$ se escribe de modo único como suma de polinomios homogéneos de distintos grados.*

Demostración. Si $p = \sum_{i\in\mathbb{N}_0^n} p_i X_1^{i_1}\cdots X_n^{i_n}$ es la expresión de p como suma de monomios y ponemos $h_j = \sum_{i_1+\cdots+i_n=j} p_i X_1^{i_1}\cdots X_n^{i_n}$, es claro que $p = h_0 + h_1 + \cdots + h_k$ (donde $k = \mathrm{gr}(p)$) es la expresión buscada. La unicidad es consecuencia inmediata del Lema 3.31. ∎

Corolario 3.36 *Si D es un dominio y $n \geq 1$, se tiene* $\mathrm{gr}(pq) = \mathrm{gr}(p)+\mathrm{gr}(q)$ *para cualesquiera $p, q \in D[X_1,\ldots,X_n]$.*

Problemas

3.5.1 Sea D un dominio. Demostrar que el ideal (X^2, XY, Y^2) del anillo de polinomios en dos indeterminadas $D[X,Y]$ no es principal. ¿Tiene un conjunto de generadores con dos elementos? Determinar los ideales de $A = K[X,Y]/(X^2,XY,Y^2)$, siendo K un cuerpo y demostrar que A tiene ideales que no son principales.

3.5.2 Sea A un anillo. Demostrar que si $P \in A[X_1,\ldots,X_n]$ tiene grado 1 y uno de los coeficiente diferentes del término independiente es una unidad de A, entonces $A[X_1,\ldots,X_n]/(P) \cong A[X_1,\ldots,X_{n-1}]$.

3.5.3 Sea K un cuerpo y sea $P \in K[X,Y]$. Supongamos que el coeficiente principal de P, considerado como polinomio en $K[X][Y]$, no es divisible por $X-1$. Demostrar que, si $P(X,1)$ es irreducible en $K[X]$, entonces $P(X,Y)$ es irreducible en $K[X,Y]$.

3.5.4 Demostrar que si K es un cuerpo y P, Q son elementos coprimos de $K[X,Y]$ entonces el conjunto $\{(a,b) \in K^2 : P(a,b) = Q(a,b) = 0\}$ es finito. (Indicación: Usar el Problema 3.1.3.)

3.5.5 Consideremos el anillo $A = K[X,Y,Z]/(X(YZ-1))$ con K un cuerpo. Si $P \in K[X,Y,Z]$ entonces $\bar{P}$ denota la imagen canónica de P en A. Sean $a = \bar{X}$ y $b = \bar{X}\bar{Y}$.

(1) Demostrar que a y b son asociados en A.

(2) Sea $P \in K[X,Y,Z]$. Demostrar que $b = a\overline{P}$ si y solo si $YZ-1$ divide a $Y-P$ en $K[X,Y,Z]$.

(3) Sea $f : K[X,Y,Z] \to K[Y,Z]$ el homomorfismo dado por $f(X,Y,Z) = f(0,Y,Z)$. Demostrar que si $P \in K[X,Y,Z]$ es tal que $\bar{P}$ es una unidad en A entonces $f(P) \in K \setminus \{0\}$.

(4) Demostrar que A no tiene ninguna unidad u tal que $b = au$. (Indicación: Sea $P \in K[X,Y,Z]$ tal que $u = \bar{P}$ es una unidad de A tal que $b = au$. Demuestra que existe $Q \in K[X,Y,Z]$ tal que $Y - P = Q(YZ-1)$ y deduce que $Y - f(Q)(YZ-1) \in K \setminus \{0\}$. Con esto último deberías obtener una contradicción.)

Capítulo 4

Grupos

4.1 Definiciones y ejemplos

Definición 4.1 *Un* grupo *es una pareja $(G, \cdot)$, formada por un conjunto no vacío G junto una operación interna, es decir una aplicación*

$$\begin{array}{rcl} G \times G & \to & G \\ (g,h) & \mapsto & g \cdot h \end{array}$$

que satisface los siguientes axiomas:

- *(Asociativa) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todo $a, b, c \in G$.*
- *(Neutro) Existe un elemento $e \in G$, llamado* elemento neutro del grupo *tal que $e \cdot a = a = a \cdot e$, para todo $a \in G$.*
- *(Inverso) Para todo $a \in G$ existe otro elemento $a_1 \in G$, llamado* elemento inverso *de a, tal que $a \cdot a_1 = e = a_1 \cdot a$.*

Si además se verifica el siguiente axioma se dice que el grupo es abeliano *o* conmutativo

- *(Conmutativa) $a \cdot b = b \cdot a$, para todo $a, b \in G$.*

Lema 4.2 *Sea $(G, \cdot)$ un grupo.*

(1) (Unicidad del neutro). El neutro de G es único, de hecho, si $e, e' \in G$ satisfacen que $e' \cdot a = a = a \cdot e$ para todo $a \in G$, entonces $e = e'$.

(2) (Unicidad del inverso). El inverso de un elemento de G es único, de hecho, si $a \cdot a_1 = e = a_2 \cdot a$, entonces $a_1 = a_2$. A partir de ahora el (único) inverso de a lo denotaremos con a^{-1}.

(3) (Propiedad Cancelativa). Si $a \cdot x = a \cdot y$ ó $x \cdot a = y \cdot a$, con $a, x, y \in G$, entonces $x = y$.

(4) Para todo $a, b \in G$, las ecuaciones $a \cdot X = b$ y $X \cdot a = b$, tienen una única solución en G.

(5) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Demostración. Ejercicio. ∎

Habitualmente no haremos referencia a la operación del grupo y hablaremos simplemente del grupo G, donde la operación se sobreentiende. Siempre utilizaremos notación multiplicativa, de forma que para un grupo genérico el resultado de operar dos elementos a y b se denota como ab, el neutro lo denotaremos con 1 y en inverso de a con a^{-1}. Además, si n es un entero positivo definimos a^n como el resultado de operar n veces a consigo mismo. Además ponemos $a^0 = 1$ y $a^{-n} = (a^n)^{-1} = (a^{-1})^n$. De esta forma quedan definidas potencias de elementos de G por exponentes enteros se verifica la siguiente igualdad para cualesquiera $a \in G$ y $n, m \in \mathbb{Z}$:

$$a^{n+m} = a^n a^m, (a^n)^m = a^{nm}.$$

Excepcionalmente utilizaremos notación aditiva para grupos abelianos. En tal caso el neutro lo denotaremos con 0, el inverso de a, lo llamaremos opuesto de a y lo denotamos $-a$ y escribiremos na, en lugar de a^n.

Ejemplos 4.3 (1) Si A es un anillo, entonces $(A, +)$ y $(A^*, \cdot)$ son dos grupos abelianos llamados respectivamente *grupo aditivo* y *grupo de unidades* de A. Por ejemplo, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ y $(\mathbb{Z}_n, +)$ son grupos aditivos y los grupos de unidades de los correspondientes anillos son $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ y

$$\mathbb{Z}_n^* = \{i : 1 \leq i \leq n, \mathrm{mcd}(i, n) = 1\}.$$

Obsérvese que si K es un cuerpo, entonces $K^* = K \setminus \{0\}$.

(2) Sea K un anillo y n un entero positivo. Entonces el conjunto $\mathrm{GL}_n(K)$ formado por todas las matrices invertibles cuadradas de tamaño n con entradas en K es un grupo con el producto habitual de matrices. Si $n = 1$, entonces $\mathrm{GL}_1(K) = K^*$ es abeliano. Sin embargo si $n \geq 2$ y $K \neq 0$, entonces $\mathrm{GL}_n(K)$ no es abeliano pues las dos siguientes matrices no conmutan:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Este ejemplo se puede generalizar cambiando el cuerpo K por un anillo arbitrario.

(3) Sea X un conjunto y S_X el conjunto de todas las biyecciones de X en si mismo. Entonces $(S_X, \circ)$ es un grupo, llamado *grupo simétrico o* de las permutaciones de X.

(4) Si $(G, \star)$ y $(H, *)$ son dos grupos, entonces el producto directo $G \times H$ es un producto directo en el que la operación viene dada componente a componente:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \star g_2, h_1 * h_2).$$

Más generalmente, si $(G_i)_{i \in I}$ es una familia arbitraria de grupos, entonces el producto directo $\prod_{i \in I} G_i$ tiene una estructura de grupo en el que el producto se realiza componente a componente.

(5) Para cada número natural positivo n vamos a definir un grupo C_n formado por n elementos

$$C_n = \{1, a, a^2, \ldots, a^{n-1}\},$$

donde a es un símbolo, y en el que la multiplicación viene dada por la siguiente regla:

$$a^i a^j = a^{[i+j]_n}$$

donde $[x]_n$ denota el resto de dividir x entre n. Este *grupo* se llama *cíclico* de orden n.

También definimos el *grupo cíclico infinito* como el conjunto $C_\infty = \{a^n : n \in \mathbb{Z}\}$, donde a es un símbolo y consideramos $a^n = a^m$ si y sólo si $n = m$, y en el que el producto viene dado por $a^n \cdot a^m = a^{n+m}$.

(6) Para cada número natural positivo n vamos a definir un grupo formado por $2n$ elementos

$$D_n = \{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$$

en el que la multiplicación viene dada por la siguiente regla:

$$(a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) = a^{[i_1+(-1)^{j_1}i_2]_n}b^{[j_1+j_2]_2}$$

con notación como en el ejemplo anterior. Este grupo se llama *grupo diédrico* de orden $2n$.

El *grupo diédrico infinito* D_∞ está formado por elementos de la forma a^nb^m, con $n \in \mathbb{Z}$ y $m = 0, 1$ con el producto $(a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) = a^{i_1+(-1)^{j_1}i_2}b^{[j_1+j_2]_2}$.

4.2 Subgrupos

Definición 4.4 *Sea G un grupo. Un subconjunto S de G se dice que es un* subgrupo *si la operación que define la estructura de grupo en G induce también una estructura de grupo en S.*

El siguiente lema muestra cuáles son las propiedades que hay que comprobar para demostrar que un subconjunto de un grupo es un subgrupo.

Lema 4.5 *Sea G un grupo y S un subconjunto de G. Las siguientes condiciones son equivalentes:*

(1) S es un subgrupo de G.

(2) $1 \in S$ y para todo $a, b \in S$, se verifican $ab, a^{-1} \in S$.

(3) $S \neq \emptyset$ y para todo $a, b \in S$, se verifican $ab, a^{-1} \in S$.

(4) $1 \in S$ y para todo $a, b \in S$, se verifican $ab^{-1} \in S$.

(5) $S \neq \emptyset$ y para todo $a, b \in S$, se verifican $ab^{-1} \in S$.

Demostración. Ejercicio. ∎

Ejemplos 4.6 (1) Si G es un grupo, entonces $\{1\}$ y G son subgrupos de G. El primero se llama *subgrupo trivial*, denotado 1 y el segundo *subgrupo impropio* de G. Los subgrupos de G diferentes de G se dice que son *subgrupos propios*.

(2) Si $(A, +)$ es el grupo aditivo de un anillo, entonces todo subanillo y todo ideal de A son subgrupos de este grupo.

Si S es un subgrupo de $(\mathbb{Z}, +)$, entonces $nx \in S$, para todo $n \in \mathbb{Z}$ y todo $x \in I$. Eso implica que S es un ideal de $\mathbb{Z}$ y por tanto los subgrupos de $(\mathbb{Z}, +)$ son los de la forma $n\mathbb{Z}$ para n un entero no negativo.

(3) Sea $\mathrm{GL}_n(K)$ el grupo de las matrices invertibles de tamaño n con entradas en el cuerpo K. Entonces el $\mathrm{SL}_n(K)$ conjunto formado por las matrices de determinante 1 es un subgrupo de $\mathrm{GL}_n(K)$.

(4) Supongamos que A es un anillo y sea S_A el grupo de las permutaciones de A. Entonces el conjunto $\mathrm{Aut}(A)$ formado por los automorfismos de A es un subgrupo de S_A.

Ejemplos similares se pueden obtener con casi todas las estructuras matemáticas. Por ejemplo, si G es un grupo, entonces decimos que $f : G \to G$ es un automorfismo si f es biyectivo y $f(gh) = f(g)f(h)$ para todo $g, h \in G$. Entonces el conjunto $\mathrm{Aut}(G)$ formado por todos los automorfismos de G es un subgrupo del grupo simétrico S_G de G.

Si X es un espacio topológico entonces el conjunto de todos los homeomorfismos de X (es decir las aplicaciones biyectivas continuas con inversa continua) de X en si mismo es un subgrupo de S_X.

Si X es un espacio métrico con distancia d, entonces el conjunto de las isometrías (es decir, las aplicaciones biyectivas de X en si mismo tales que $d(f(x), f(y)) = d(x, y)$) es un subgrupo de S_X.

(5) Si G es un grupo y $g \in G$, entonces

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

es un subgrupo de G, llamado *grupo cíclico* generado por g.

Un *grupo* G se dice que es *cíclico* si tiene un elemento g tal que $G = \langle g \rangle$. En tal caso se dice que g es un generador de G.

Por ejemplo, $(\mathbb{Z}, +)$ es cíclico generado por 1 y $(\mathbb{Z}_n, +)$ es otro grupo cíclico generado por la clase de 1. Otros ejemplos de grupos cíclicos son los grupos C_n y C_∞ del Ejemplo 5 de 4.3.

(6) Si X es un subconjunto arbitrario de G, entonces el conjunto formado por todos los elementos de G de la forma $x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$, con $x_1, \dots x_m \in X$ y $n_1, \dots, n_m \in \mathbb{Z}$, es un subgrupo de G, que resulta ser el menor subgrupo de G que contiene a X y por tanto se llama *subgrupo generado* por X y se denota $\langle X \rangle$.

El subgrupo generado por X se puede construir de otra forma. Es un sencillo ejercicio comprobar que la intersección de subgrupos de G, es un subgrupo. Por tanto la intersección de todos los subgrupos de G que contienen a X es un subgrupo de G y es el menor subgrupo de G que contiene a X, con lo que es el subgrupo generado por X.

(7) Si $(G_i)_{i\in I}$ es una familia arbitraria de grupos, entonces el subconjunto $\oplus_{i\in I}G_i$ formado por los elementos $(g_i) \in \prod_{i\in I} G_i$ tales que $g_i = 1$ para todo i, es un subgrupo de $\prod_{i\in I} G_i$.

(8) Si G es un grupo arbitrario, entonces

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

es un subgrupo abeliano de G, llamado *centro*.

Más generalmente, si $x \in G$, entonces

$$C_G(x) = \{g \in G : gx = xg\}$$

es un subgrupo de G, llamado *centralizador* de x en G. Obsérvese que $Z(G)$ es la intersección de todos los centralizadores de los elementos de G en G.

Sea G un grupo y H un subgrupo de G. Se define la siguiente relación binaria en G:

$$a \equiv_i b \bmod H \quad \Leftrightarrow \quad a^{-1}b \in H. \qquad\qquad (a, b \in G).$$

Se puede comprobar fácilmente que esta relación es de equivalencia y por tanto define una partición de G en clases de equivalencia. Las clase de equivalencia que contiene a a es

$$aH = \{ah : h \in H\}$$

y se llama *clase lateral de a módulo H por la izquierda*.

Análogamente se puede definir otra relación de equivalencia:

$$a \equiv_d b \bmod H \quad \Leftrightarrow \quad ab^{-1} \in H. \qquad\qquad (a, b \in G)$$

para la que las clase de equivalencia que contiene a a es

$$Ha = \{ah : h \in H\}$$

y se llama *clase lateral de a módulo H por la derecha*.

El conjunto de las clases laterales por la izquierda de G módulo H se denota por G/H y el de clases laterales por la derecha $H\backslash G$.

Como consecuencia del Lema 4.2 las aplicaciones

$$\begin{array}{ccc} H & \to & aH \\ h & \mapsto & ah \end{array} \qquad \begin{array}{ccc} H & \to & Ha \\ h & \mapsto & ha \end{array}$$

son biyectivas, con lo que todas las clases laterales tienen el mismo cardinal. Además la aplicación

$$\begin{array}{ccc} G/H & \to & H\backslash G \\ aH & \mapsto & Ha^{-1} \end{array}$$

es otra biyección.

Denotamos con $|X|$ el cardinal de un conjunto cualquiera. En el caso en que G sea un grupo el cardinal de G se suele llamar *orden* de G. Acabamos de ver que para cada subgrupo H de G se verifica:

$$|aH| = |Ha| = |H| \quad \text{y} \quad |G/H| = |H\backslash G|$$

El cardinal de G/H (y $H\backslash G$) se llama *índice* de H en G y se denota $[G : H]$. Una consecuencia inmediata de estas fórmulas es el siguiente Teorema.

Teorema 4.7 (Teorema de Lagrange) *Si G es un grupo finito y H es un subgrupo de G entonces $|G| = |H|[G : H]$.*

4.3 El orden de un elemento de un grupo

Definición 4.8 *Sea G un grupo y $a \in G$. Por definición el orden de a es el orden del subgrupo $\langle a\rangle$ generado por a, y se denota $o(a)$.*

Si consideremos el homomorfismo $f : \mathbb{Z} \to G$ dado por $f(n) = a^n$, entonces la imagen de f es $\langle a\rangle$ y el núcleo de f es un subgrupo de $\mathbb{Z}$. Por tanto Ker $f = n\mathbb{Z}$ para algún entero no negativo n. Si $n = 0$, entonces f es inyectivo y $(\mathbb{Z}, +) \simeq \langle a\rangle$. En caso contrario $\mathbb{Z}_n \simeq \langle a\rangle$, con lo que $n = o(a)$. Luego

$$a^n = 1 \quad \Leftrightarrow \quad o(a)|n. \tag{4.1}$$

Más aún $a^k = a^l$ si y sólo si $k \equiv l \bmod n$ y por tanto $o(a)$ es el menor entero no negativo n tal que $a^n = 1$.

Por el Teorema de Lagrange, si G es finito, entonces $o(a)$ divide a $|G|$. Además, si a tiene orden finito entonces la siguiente fórmula relaciona el orden de un elemento con el de sus potencias:

$$o(a^n) = \frac{o(a)}{\text{mcd}(o(a), n)} \tag{4.2}$$

Demostración. Obsérvese que $m = o(a)$ y $d = \text{mcd}(m, n)$, entonces $\text{mcd}(\frac{m}{d}, \frac{n}{d}) = 1$. Aplicando (4.1) tenemos que $(a^n)^k = 1$ si y sólo si $a^{nk} = 1$ si y sólo si $m|nk$, si y sólo si $\frac{m}{d}$ divide a $\frac{nk}{d} = \frac{n}{d}k$ si y sólo si $\frac{m}{d}$ divide a k. Lo que muestra que $o(a^n) = \frac{m}{d}$. ∎

Recordando como son los subgrupos de $\mathbb{Z}$ y de $\mathbb{Z}_n$ tenemos que

Proposición 4.9 *Sea G un grupo cíclico generado por a.*

(1) Si G tiene orden infinito entonces $G \simeq (\mathbb{Z}, +)$ y los subgrupos de G son los de la forma $\langle a^n\rangle$ con $n \in \mathbb{N}$. Además, si $n, m \in \mathbb{N}$, entonces $\langle a^n\rangle \subseteq \langle a^m\rangle$ si y sólo si $m|n$.

G tiene un subgrupo para cada número entero no negativo n: $\langle a^n\rangle$.

(2) Si G tiene orden n, entonces $G \simeq (\mathbb{Z}_n, +)$ y G tiene exactamente un subgrupo de orden d para cada divisor de n, a saber $\langle a^{n/d}\rangle$.

En particular todo subgrupo y todo cociente de G son cíclicos.

Teorema 4.10 (Teorema Chino de los Restos para grupos) *Si G y H son dos subgrupos cíclicos de ordenes n y m, entonces $G \times H$ es cíclico si y sólo si* $\mathrm{mcd}(n, m) = 1$.

Más generalmente, si g y h son dos elementos de un grupo G de órdenes coprimos n y m y $gh = hg$, entonces $\langle g, h\rangle$ es cíclico de orden nm.

Demostración. Por la Proposición 4.9, $G \simeq (\mathbb{Z}_n, +)$ y $H \simeq (\mathbb{Z}_m, +)$. Si $\mathrm{mcd}(n, m) = 1$, entonces, por el Teorema Chino de los Restos, $\mathbb{Z}_n \times \mathbb{Z}_m$ y $\mathbb{Z}/nm\mathbb{Z}$ son isomorfos como anillos y por tanto también lo son sus grupos aditivos. Por tanto $G \times H \simeq (\mathbb{Z}_n, +) \times (\mathbb{Z}_m, +) \simeq (\mathbb{Z}/nm\mathbb{Z}, +)$. Sin embargo, si n y m no son coprimos y $d = \mathrm{mcd}(n, m)$, entonces G tiene un subgrupo G_1 de orden d y H tiene otro subgrupo H_1 de orden d. Entonces $G_1 \times 1$ y $1 \times H_1$ son dos subgrupos distintos de $G \times H$ del mismo orden, en contra de la Proposición 4.9.

Supongamos ahora que $g, h \in G$ tienen órdenes coprimos n y m. Entonces la aplicación $f : \mathbb{Z}_n \times \mathbb{Z}_m \to G$ dada por $f(i, j) = g^i h^j$ es un homomorfismo de grupos cuya imagen es $\langle g, h\rangle$. (Observa la importancia de la hipótesis $gh = hg$ aquí.) Por el Teorema de Lagrange, el orden de $\langle g\rangle \cap \langle h\rangle$ divide a n y m. Como n y m son coprimos, este orden es 1. Si $f(i, j) = 1$, entonces $a^{-i} = b^j \in \langle g\rangle \cap \langle h\rangle = 1$. Por tanto $n|i$ y $m|j$, lo que muestra que f es inyectiva. Por tanto f es un isomorfismo, lo que prueba que $\langle g, h\rangle \simeq \mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}/nm\mathbb{Z}$. ∎

El siguiente teorema que veremos sin demostración describe todos los grupos abelianos finitos salvo isomorfismo.

Teorema 4.11 (Estructura de los grupos abelianos finitos) *Si G es un grupo abeliano finito, entonces existen enteros positivos $d_1|d_2|\ldots|d_n$ tales que*

$$G \simeq C_{d_1} \times C_{d_2} \times \cdots \times C_{d_n}.$$

Además, si $d_1|d_2|\ldots|d_n$ y $e_1|e_2|\ldots|e_m$ son enteros positivos tales que

$$C_{d_1} \times C_{d_2} \times \cdots \times C_{d_n} \simeq C_{e_1} \times C_{e_2} \times \cdots \times C_{e_m}$$

entonces $n = m$ y $d_i = e_i$ para todo i.

Capítulo 5

Subgrupos normales y homomorfismos

5.1 Subgrupos normales y grupos cociente

Dados subconjuntos A y B de un grupo G, pondremos $AB = \{ab : a \in A, b \in B\}$. Si $X = \{x\}$ pondremos xA en lugar de XA y Ax en lugar de AX, lo que es consistente con la notación usada para las clases laterales. Por otra parte, la asociatividad de G implica que $(AB)C = A(BC)$ para subconjuntos A, B y C arbitrarios, lo que nos permite escribir ABC sin ambigüedad; obviamente $ABC = \{abc : a \in A, b \in B, c \in C\}$.

Proposición 5.1 *Las condiciones siguientes son equivalentes para un subgrupo N de un grupo G:*

(1) $N\backslash G = G/N$.

(2) Para cada $x \in G$ se tiene $Nx = xN$ (o equivalentemente $x^{-1}Nx = N$).

(3) Para cada $x \in G$ se tiene $Nx \subseteq xN$ (o equivalentemente $x^{-1}Nx \subseteq N$).

(4) Para cada $x \in G$ se tiene $xN \subseteq Nx$ (o equivalentemente $xNx^{-1} \subseteq N$).

(5) Para cualesquiera $a, b \in G$ se tiene $aNbN = abN$.

(6) Para cualesquiera $a, b \in G$ se tiene $NaNb = Nab$.

Demostración. Ejercicio ∎

Supongamos que se cumplen las condiciones de la Proposición 5.1. Entonces el producto de dos elementos de G/N (o de $N\backslash G$) es un elemento de G/N, y es elemental comprobar que esta operación dota a G/N de una estructura de grupo. Obsérvese que, para realizar un producto $aN \cdot bN$ en G/N, no necesitamos describir el conjunto resultante, pues éste queda determinado por cualquier representante suyo, por ejemplo ab. El elemento neutro de G/N es la clase $N = 1N$, y el inverso de aN es $a^{-1}N$.

Definición 5.2 *Un subgrupo N de un grupo G es un* subgrupo normal *de G (también se dice que N* es normal en *G) si verifica las condiciones equivalentes de la Proposición 5.1. En ocasiones escribiremos $N \trianglelefteq G$ (respectivamente $N \triangleleft G$) para indicar que N es un subgrupo normal (respectivamente normal y propio) de G.*

Si N es normal en G, el grupo G/N recién descrito se llama grupo cociente *de G módulo N.*

Ejemplos 5.3 *Subgrupos normales.*

(1) Es claro que, en un grupo abeliano, todo subgrupo es normal.

(2) Si I es un ideal de un anillo A, entonces el grupo cociente A/I es el grupo aditivo del anillo cociente.

(3) Si G es un grupo y H es un subgrupo contenido en el centro $Z(G)$, entonces H es normal en G. En particular, el centro es un subgrupo normal.

(4) Si H es un subgrupo de G de índice 2, entonces H es normal en G. En efecto, como las clases por la derecha módulo H constituyen una partición de G, sólo hay dos, y una de ellas es H, la otra ha de ser el complementario $\{g \in G : g \notin H\}$. El mismo argumento vale para las clases por la izquierda y en consecuencia $G/N = N\backslash G$.

(5) Sea $G = \mathrm{GL}_n(\mathbb{R})$ el grupo lineal general sobre $\mathbb{R}$. Usando el hecho de que, si $a, b \in G$, entonces
$$\det(ba) = \det(b)\det(a) = \det(a)\det(b) = \det(ab),$$
es fácil ver que $\mathrm{SL}_n(\mathbb{R})$ es un subgrupo normal de G.

(6) El siguiente es el diagrama de todos los subgrupos de D_4 ordenados por inclusión: una línea entre dos subgrupos significa que el de arriba contiene al de abajo. Los subgrupos de la segunda fila tienen orden 4, y los de la tercera fila tienen orden 2. En el diagrama están subrayados los subgrupos que *no* son normales en D_4:

Los que aparecen son subgrupos y las relaciones de inclusión son claras, pero el lector deberá comprobar esos subgrupos son distintos entre sí y que no hay más, así como la normalidad de los subgrupos no subrayados. Otro ejercicio interesante consiste en demostrar que los subgrupos $\langle a^2, b\rangle$ y $\langle a^2, ab\rangle$ no son cíclicos.

Obsérvese que cualquier subgrupo del diagrama es normal en cualquiera de los subgrupos que lo contengan y estén en el nivel inmediatamente superior. Por ejemplo, $\langle b\rangle \trianglelefteq \langle a^2, b\rangle$ y $\langle a^2, b\rangle \trianglelefteq D_4$; como $\langle b\rangle$ no es normal en D_4, este ejemplo muestra que la relación "ser normal en" no es transitiva.

Acabamos la sección con una versión para grupos del Teorema de la Correspondencia (1.23).

Teorema 5.4 (Teorema de la Correspondencia) *Sea N un subgrupo normal de un grupo G. La asignación $H \mapsto H/N$ establece una biyección entre el conjunto $\mathcal{A}$ de los subgrupos de G que contienen a N y el conjunto $\mathcal{B}$ de los subgrupos de G/N.*

Además, esta biyección conserva las inclusiones, las intersecciones y la normalidad. Es decir, dados $H, K \in \mathcal{A}$, se tiene:

(1) $H \subseteq K$ si y sólo si $(H/N) \subseteq (K/N)$.

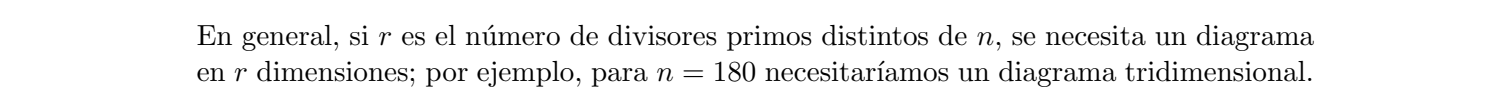
(2) $(H \cap K)/N = (H/N) \cap (K/N)$.

(3) $H \trianglelefteq G$ si y sólo si $(H/N) \trianglelefteq (G/N)$.

Demostración. Adaptar la demostración del Teorema 1.23. ∎

Ejemplos 5.5 *Aplicaciones del Teorema de la Correspondencia.*

(1) Dado un entero positivo n, vamos a describir los subgrupos del grupo cociente $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$. Escribiremos $\overline{a} = a + \langle n\rangle$. Sabemos que los subgrupos de $\mathbb{Z}$ son precisamente los de la forma $\langle d\rangle$ con $d \geq 0$, y que $\langle d\rangle \subseteq \langle d'\rangle$ si y sólo si $d' \mid d$. Por tanto, los subgrupos de $\mathbb{Z}_n$ son precisamente los de la forma $\frac{\langle d\rangle}{\langle n\rangle} = \langle \overline{d}\rangle$, donde d es un divisor positivo de n, y además $\langle \overline{d}\rangle \subseteq \langle \overline{d'}\rangle$ si y sólo si $d' \mid d$. Así, el diagrama de los subgrupos de $\mathbb{Z}_n$ puede construirse de modo elemental a partir de los divisores de n como muestran los siguientes diagramas (en el de la izquierda se ha tomado $n = 125$, y en el de la derecha $n = 72$):



En general, si r es el número de divisores primos distintos de n, se necesita un diagrama en r dimensiones; por ejemplo, para $n = 180$ necesitaríamos un diagrama tridimensional.

(2) Aplicando el Teorema de la Correspondencia al diagrama de los subgrupos de D_4 (Ejemplo 6 de 5.3), obtenemos el siguiente diagrama de los subgrupos de $D_4/\langle r^2\rangle$.

5.2 Homomorfismos y Teoremas de Isomorfía

Definición 5.6 *Un* homomorfismo *del grupo $(G, \cdot)$ en el grupo $(H, *)$ es una aplicación $f : G \to H$ que conserva la operación; es decir, que verifica*

$$f(a \cdot b) = f(a) * f(b)$$

para cualesquiera $a, b \in G$. Si $G = H$ decimos que f es un endomorfismo *de G.*

Si $f : G \to H$ es un homomorfismo biyectivo, diremos que es un isomorfismo *y que los grupos G y H son* isomorfos. *Un isomorfismo de G en G se dirá un* automorfismo *de G.*

Dado un homomorfismo de grupos $f : G \to H$, se definen su imagen *y su* núcleo *como*

$$\text{Im } f = f(G) = \{f(x) : x \in G\} \quad y \quad \text{Ker } f = f^{-1}(1_H) = \{x \in G : f(x) = 1_H\}.$$

Lema 5.7 *Si $f : G \to H$ es un homomorfismo de grupos entonces se verifican las siguientes propiedades para $a, a_1, \ldots, a_n \in G$:*

(1) (f conserva el neutro) $f(1_G) = 1_H$.

(2) (f conserva inversos) $f(a^{-1}) = f(a)^{-1}$.

(3) (f conserva productos finitos) $f(a_1 \cdots a_n) = f(a_1) \cdots f(a_n)$.

(4) (f conserva potencias) *Si $n \in \mathbb{Z}$ entonces* $f(a^n) = f(a)^n$.

(5) Si f es un isomorfismo entonces la aplicación inversa $f^{-1} : H \to G$ también lo es.

(6) Si $g : H \to K$ es otro homomorfismo de grupos entonces $g \circ f : G \to K$ es un homomorfismo de grupos.

(7) Si H_1 es un subgrupo de H entonces $f^{-1}(H_1) = \{x \in G : f(x) \in H_1\}$ es un subgrupo de G.

Si además H_1 es normal en H entonces $f^{-1}(H_1)$ es normal en G; en particular, Ker f *es un subgrupo normal de G.*

(8) f es inyectivo si y sólo si Ker $f = \{1\}$.

(9) Si G_1 es un subgrupo de G entonces $f(G_1)$ es un subgrupo de H; en particular, Im f *es un subgrupo de H.*

Si además G_1 es normal en G y f es suprayectiva entonces $f(G_1)$ es normal en H.

Demostración. Ejercicio. ∎

Ejemplos 5.8 *Homomorfismos de grupos.*

(1) Si H es un subgrupo de G, la inclusión de H en G es un homomorfismo inyectivo.

(2) Si N es un subgrupo normal de G, la aplicación $\pi : G \to G/N$ dada por $\pi(x) = xN$ es un homomorfismo suprayectivo que recibe el nombre de *proyección canónica* de G sobre G/N. Su núcleo es Ker $\pi = N$.

(3) Dados dos grupos G y H, la aplicación $f : G \to H$ dada por $f(a) = 1_H$ para cada $a \in G$ es un homomorfismo llamado *homomorfismo trivial* de G en H. Su núcleo es todo G.

(4) La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(n) = 2n$ es un homomorfismo inyectivo y no suprayectivo.

(5) Si G es cualquier grupo y $x \in G$ es cualquier elemento, la aplicación $\mathbb{Z} \to G$ dada por $n \mapsto x^n$ es un homomorfismo de grupos; como en $\mathbb{Z}$ usamos notación aditiva y en G multiplicativa, la afirmación anterior es equivalente al hecho, que ya conocemos, de que $x^{n+m} = x^n x^m$.

(6) Otro ejemplo en el que se mezclan las notaciones aditiva y multiplicativa es el siguiente: Fijado un número real positivo α, la aplicación $\mathbb{R} \to \mathbb{R}^+$ dada por $r \mapsto \alpha^r$ es un isomorfismo de grupos cuya inversa es la aplicación $\mathbb{R}^+ \to \mathbb{R}$ dada por $s \mapsto \log_\alpha s$.

Claramente, si $f : G \to H$ es un homomorfismo inyectivo de grupos entonces $f : G \to \text{Im } f$ es un isomorfismo de grupos que nos permite ver a G como un subgrupo de H.

Los Teoremas de Isomorfía que vimos para anillos tienen una versión para grupos. Las demostraciones son análogas.

Teorema 5.9 *(Teoremas de Isomorfía para grupos)*

(1) Si $f : G \to H$ es un homomorfismo de grupos entonces existe un único isomorfismo de grupos $\bar{f} : G/\text{Ker } f \to \text{Im } f$ que hace conmutativo el diagrama

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ G/\text{Ker } f & \overset{\bar{f}}{\dashrightarrow} & \text{Im } f \end{array}$$

es decir, $i \circ \bar{f} \circ p = f$, donde i es la inclusión y p es la proyección canónica. En particular

$$\frac{G}{\text{Ker } f} \simeq \text{Im } f.$$

(2) Sean N y H subgrupos normales de un grupo G con $N \subseteq H$. Entonces H/N es un subgrupo normal de G/N y se tiene

$$\frac{G/N}{H/N} \simeq G/H.$$

(3) Sean G un grupo, H un subgrupo de G y N un subgrupo normal de G. Entonces $N \cap H$ es un subgrupo normal de H y se tiene

$$\frac{H}{N \cap H} \simeq \frac{NH}{N}.$$

Usando el Teorema de la Correspondencia se obtiene el siguiente corolario.

Corolario 5.10 *Si $f : G \to H$ es un homomorfismo de grupos entonces $K \mapsto f(K)$ define una biyección entre el conjunto de los subgrupos de G que contienen a* Ker f *y el de los subgrupos de H contenidos en* Im f.

Ejemplos 5.11 *Aplicaciones de los Teoremas de Isomorfía.*

(1) Consideremos los grupos multiplicativos $\mathbb{C}^*$ y $\mathbb{R}^*$, y la aplicación norma $\delta : \mathbb{C}^* \to \mathbb{R}^*$ dada por $\delta(a + bi) = a^2 + b^2$. Entonces δ es un homomorfismo que tiene por núcleo a la circunferencia de radio 1 en $\mathbb{C}$, y por imagen a $\mathbb{R}^+$. Por tanto, el grupo cociente de $\mathbb{C}^*$ por la circunferencia de radio 1 es isomorfo a $\mathbb{R}^+$.

(2) La aplicación $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ que lleva una matriz a su determinante es un homomorfismo suprayectivo de grupos con núcleo $\mathrm{SL}_n(\mathbb{R})$. Esto nos dice que el cociente de $\mathrm{GL}_n(\mathbb{R})$ por $\mathrm{SL}_n(\mathbb{R})$ es isomorfo a $\mathbb{R}^*$

(3) Sea n un entero positivo. Hemos visto (Ejemplos 5.5) que todo subgrupo de $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$ es de la forma $\langle \overline{d}\rangle = \langle d\rangle/\langle n\rangle$, para cierto divisor positivo d de n. El Segundo Teorema de Isomorfía nos permite identificar el cociente $\mathbb{Z}_n/\langle \overline{d}\rangle$, pues

$$\frac{\mathbb{Z}_n}{\langle \overline{d}\rangle} = \frac{\mathbb{Z}/\langle n\rangle}{\langle d\rangle/\langle n\rangle} \simeq \frac{\mathbb{Z}}{\langle d\rangle} = \mathbb{Z}_d.$$

5.3 Conjugación y acciones de grupos en conjuntos

Sea G un grupo. Si $a, g \in G$, entonces se define el *conjugado* de g por a como $g^a = a^{-1}ga$. Si X es un subconjunto de G, entonces el conjugado de X por a es $X^a = \{x^a : x \in X\}$. Se dice que dos elementos o subconjuntos x y y de G son *conjugados* en G si $x^a = y$ para algún $a \in G$.

La aplicación $\iota_a : G \to G$ dada por $\iota_a(x) = x^a$ es un automorfismo de G, llamado *automorfismo interno* definido por a, con inverso $\iota_{a^{-1}}$. Eso implica que dos elementos o subconjuntos conjugados de un grupos tienen propiedades similares. Por ejemplo todos dos elementos conjugados de G tiene el mismo orden y el conjugado de un subgrupo de G es otro subgrupo de G del mismo orden.

Es fácil ver que

$$g^{ab} = (g^a)^b \quad \text{para todo } g, a, b \in G,$$

y utilizando esto se demuestra de forma fácil que la relación ser conjugados (tanto de elementos, como de subconjuntos de G) es una relación de equivalencia. Las clases de equivalencia de esta relación de equivalencia en G se llaman *clases de conjugación* de G. La clase de conjugación de G que contiene a a se denota por a^G. Es decir

$$a^G = \{a^g : g \in G\}.$$

Sean G un grupo y X un conjunto. Una *acción* de G en X es una aplicación

$$\begin{array}{rcl} \cdot : G \times X & \to & X \\ (g, x) & \mapsto & g \cdot x \end{array}$$

que satisface las siguientes propiedades:

(1) $(gh) \cdot x = g \cdot (h \cdot x)$, para todo $x \in X$ y todo $g, h \in G$.

(2) $1 \cdot x = x$, para todo $x \in X$.

Análogamente se define una acción por la derecha.

Vamos a ver una definición alternativa. Sea $\cdot : G \times X \to X$ una acción por la derecha del grupo G en el conjunto X. Entonces la aplicación $f : G \to S_X$ dada por $f(g)(x) = g \cdot x$ es un homomorfismo de grupos. Recíprocamente, si $f : G \to S_X$ es un homomorfismo de grupos, entonces la aplicación $\cdot : G \times X \to X$, dada por $g \cdot x = f(g)(x)$ es una acción por la derecha

de G en X. Por tanto, es lo mismo hablar de una acción de un grupo G en un conjunto X que de un homomorfismo de grupos $G \to S_X$. Análogamente podemos identificar las acciones por la izquierda de G en X con los antihomomorfismos de grupos $f : G \to S_X$, es decir las aplicaciones $f : G \to S_X$ que satisfacen $f(gh) = f(h)f(g)$, para todo $g, h \in G$.

Sea $\cdot : G \times X \to X$ una acción por la izquierda de un grupo G en un conjunto X. Si $x \in X$ entonces $G \cdot x = \{g \cdot x : g \in G\}$ se llama *órbita* de x y $\mathrm{Estab}_G(x) = \{g \in G : g \cdot x = x\}$ se llama *estabilizador* de x en G. Obsérvese que las órbitas forman una partición de G.

Veamos algunos ejemplos de acciones de grupos en conjuntos.

Ejemplos 5.12 Sea G un grupo arbitrario.

(1) Consideremos la acción por la derecha de G en si mismo dada por $g \cdot x = gx$. Esta acción se llama *acción por la derecha de* G en si mismo por *translación*. Análogamente se define una acción por la izquierda por traslación. Obsérvese que $\mathrm{Estab}_G(x) = 1$ y $G \cdot x = G$, para todo $x \in G$.

Más generalmente, si H es un subgrupo de G, entonces G actúa por la derecha en G/H mediante la regla: $g \cdot xH = (gx)H$. Análogamente se define una acción por la izquierda de G en $H\backslash G$. En ambos casos todos los elementos están en la misma órbita y $\mathrm{Estab}_G(xH) = \{g \in G : xgx^{-1} \in H\} = x^{-1}Hx = H^x$.

(2) La *acción por conjugación* de G en si mismo viene dada por $g \cdot a = g^a = a^{-1}ga$. La órbita $G \cdot x$ es x^G, la clase de conjugación de x en G y el estabilizador es $\mathrm{Estab}_G(x) = C_G(x)$, el centralizador de x en G.

(3) G actúa por la derecha en el conjunto S de sus subgrupos mediante la regla $H \cdot g = H^g$. El estabilizador de H es $\mathrm{Estab}_G(H) = \{g \in H : H^g = H\} = N_G(H)$, el *normalizador* de H en G, es decir, el mayor subgrupo de G que contiene a H como subgrupo normal.

(4) Para cada entero positivo n, consideramos S_n actuando por la derecha en en $\{1, 2, \ldots, n\}$ mediante: $\sigma \cdot x = \sigma(x)$. Claramente, todo elemento está en la misma órbita y $\mathrm{Estab}_{S_n}(i) = \{\sigma \in S_n : \sigma(i) = i\} \simeq S_{n-1}$.

(5) El grupo simétrico S_n también actúa por la derecha en $A[X_1, \ldots, X_n]$ por la regla $\sigma \cdot p = \overline{\sigma}(p)$ definida en la Sección **??**. Recuérdese que la órbita de p por esta acción es precisamente lo que habíamos llamado órbita del polinomio p.

Proposición 5.13 *Sea G un grupo actuando en un conjunto X y sean $x \in X$ y $g \in G$. Entonces*

(1) $\mathrm{Estab}_G(x)$ *es un subgrupo de G.*

(2) $[G : \mathrm{Estab}_G(x)] = |G \cdot x|$. *En particular, si G es finito, entonces el número de elementos de cada órbita es un divisor del orden de G.*

(3) $\mathrm{Estab}_G(g \cdot x) = \mathrm{Estab}_G(x)^{g^{-1}}$. *En particular* $C_G(a^g) = C_G(a)^{g^{-1}}$.

Demostración. 1 y 3 se hacen con un simple cálculo.

2. Sea $H = \text{Estab}_G(x)$, entonces la aplicación $gH \mapsto g \cdot x$ induce una biyección entre G/H y $G \cdot x$. ∎

La primera parte del corolario es un caso particular de la Proposición 5.13 y la segunda es una consecuencia obvia de la primera.

Corolario 5.14 *Sea G un grupo y $a \in G$.*

(1) $|a^G| = [G : C_G(a)]$. En particular, a^G tiene un único elemento si y sólo si a es un elemento del centro $Z(G)$ de G.

*(2) (*Ecuación de Clases*). Si G es finito y X es un subconjunto de G que contiene exactamente un elemento de cada clase de conjugación con al menos dos elementos, entonces*

$$|G| = |Z(G)| + \sum_{x \in X} [G : C_G(x)].$$

Si p es un primo, entonces un *p-grupo finito* es un grupo finito de orden una potencia de p.

Proposición 5.15 *Si G es un p-grupo no trivial para p un primo entonces $Z(G) \neq 1$.*

Demostración. Utilizando la notación del Corolario 5.14 tenemos $|G| = |Z(G)| + \sum_{x \in X} [G : C_G(x)]$. Entonces $|G|$ y $[G : C_G(x)]$ es una potencia de p para todo $x \in X$, con lo que $|Z(G)|$ es múltiplo de p y por tanto $Z(G) \neq 1$. ∎

5.4 Problemas

(1) Construir la tabla de multiplicación de los siguientes grupos.

(a) Los grupos de unidades de $\mathbb{Z}_7$ y $\mathbb{Z}_{16}$.

(b) $\text{GL}_2(\mathbb{Z}_2)$.

(c) El subgrupo de $\text{GL}_2(\mathbb{C})$ generado por las matrices

$$a = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Este grupo se llama *grupo de cuaterniones* y se denota Q_8.

(d) El subgrupo de $\text{GL}_2(\mathbb{C})$ generado por las matrices

$$a = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

donde $\omega = \frac{1+\sqrt{-3}}{2}$.

(e) El subgrupo de $\mathrm{GL}_2(\mathbb{Q})$ generado por las matrices

$$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

(f) El grupo cociente $G/\langle -I \rangle$, donde G es el grupo del apartado anterior e I es la matriz identidad.

(g) El grupo de los automorfismos del grupo $\mathbb{Z}_5$.

(h) El subgrupo del grupo de la permutaciones de $A = \mathbb{R} \setminus \{0, 1, 2\}$ generado por f y g, donde

$$f(x) = 2 - x \qquad \text{y} \qquad g(x) = \frac{2}{x}.$$

(i) $\mathbb{Z}_{16}$ con la operación $x * y = x + (-1)^x + y$.

Decidir si alguno de estos grupos es isomorfo a algún otro grupo conocido.

(2) Construir el diagrama de los subgrupos de los grupos anteriores, indicando cuáles de ellos son normales.

(3) Probar que todo grupo G de orden menor o igual a cinco es abeliano.

(4) Sea G un grupo. Probar que las siguientes afirmaciones son equivalentes:

(a) G es abeliano.

(b) $(ab)^2 = a^2b^2$ para cualesquiera $a, b \in G$.

(c) $(ab)^{-1} = a^{-1}b^{-1}$ para cualesquiera $a, b \in G$.

(d) $(ab)^n = a^nb^n$ para todo $n \in \mathbb{N}$ y para cualesquiera $a, b \in G$.

(5) Demostrar que si G es un grupo tal que $g^2 = 1$, para todo $g \in G$, entonces G es abeliano.

(6) Mostrar que la unión de dos subgrupos de un grupo no es necesariamente un subgrupo. Aún más, probar que un grupo nunca puede expresarse como unión de dos subgrupos propios.

(7) Para $n = 1, \ldots, 10$, determinar cuáles de los grupos $\mathbb{Z}_n^*$ son cíclicos.

(8) La función $\phi : \mathbb{N} \to \mathbb{N}$ que asocia a cada número n el cardinal de $\mathbb{Z}_n^*$ se llama función de Euler. Demostrar que:

(a) Si n y m son coprimos, entonces $\phi(nm) = \phi(n)\phi(m)$.

(b) Si p es primo, entonces $\phi(p^n) = p^{n-1}(p-1)$.

(c) Si $n = p_1^{a_1} \cdots p_k^{a_k}$, con $p_1, \ldots, p_k$ primos distintos entonces $\phi(n) = n\frac{p_1-1}{p_1} \cdots \frac{p_k-1}{p_k}$.

(9) Demostrar que si G es cíclico entonces el número de generadores de G es 2, si G tiene orden infinito y $\phi(|G|)$, si G tiene orden finito. Describir los generadores en todos los casos.

(10) Encontrar todos los grupos cíclicos G, salvo isomorfismos, que tengan exactamente dos generadores (es decir, tales que existan exactamente dos elementos $x \in G$ con $G = \langle x \rangle$).

(11) Demostrar que si p es un primo positivo, entonces todos los subgrupos de orden p son cíclicos isomorfos a C_p.

(12) Calcular el orden de cada elemento de los grupos diédricos D_n.

(13) ¿Es cíclico el producto directo de dos grupos cíclicos infinitos?

(14) Demostrar que la intersección de una familia de subgrupos normales de un grupo también es un subgrupo normal.

(15) Demostrar que todo subgrupo de un subgrupo cíclico normal de G es normal en G.

(16) Sean N y M subgrupos normales de un grupo G tales que $N \cap M = \{1\}$. Probar que $nm = mn$ para todo $n \in N$ y $m \in M$.

(17) Sea N un subgrupo normal de índice n de un grupo G. Demostrar que $g^n \in N$ para todo $g \in G$, y dar un ejemplo que muestre que esta propiedad falla si N no es normal en G.

(18) Si N es un subgrupo normal en un grupo G y $a \in G$ tiene orden n, probar que el orden de Na en G/N es un divisor de n.

(19) Un subgrupo H del grupo G es *característico* si, para cualquier automorfismo f de G, se verifica $f(H) \subseteq H$. Se pide:

- (a) Demostrar que todo subgrupo característico de G es un subgrupo normal de G.
- (b) Dar un ejemplo de un grupo con un subgrupo normal que no sea característico.
- (c) Demostrar que si H es un subgrupo característico de G y K es un subgrupo característico de H, entonces K es un subgrupo característico de G.
- (d) Si H es un subgrupo característico de K y K es un subgrupo normal de G, entonces H es normal en G.
- (e) Demostrar que el centro de un grupo es un subgrupo característico.
- (f) Supongamos que H es un subgrupo de un grupo G, y que ningún otro subgrupo de G contiene un subgrupo del mismo cardinal que H. Demostrar que H es un subgrupo característico (y por tanto normal) de G.

(20) Si G y H son grupos, $\mathrm{Hom}(G, H)$ denota el conjunto de los homomorfismos de G a H.

- (a) Demostrar que si H es abeliano, entonces $\mathrm{Hom}(G, H)$ es un grupo con la operación natural:
$$(\varphi\phi)(g) = \varphi(g)\phi(g), \quad (g \in G).$$
- (b) Demostrar que si G es abeliano, entonces $\mathrm{Hom}(\mathbb{Z}, G) \simeq G$ y $\mathrm{Hom}(\mathbb{Z}_n, G) \simeq \{g \in G : g^n = e\}$.
- (c) Calcular $\mathrm{Hom}(\mathbb{Z}_3, \mathbb{Z}_8)$ y $\mathrm{Hom}(\mathbb{Z}_3, \mathbb{Z}_{21})$.

(d) Probar que $\mathrm{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*$.

(e) Mostrar que, aun cuando G sea cíclico, $\mathrm{Aut}(G)$ no tiene por qué ser cíclico.

(f) Describir $\mathrm{Aut}(\mathbb{Z})$.

(21) Probar que si $n \mid m$ entonces existen un homomorfismo inyectivo $\mathbb{Z}_n \to \mathbb{Z}_m$ y un homomorfismo suprayectivo $\mathbb{Z}_m \to \mathbb{Z}_n$.

(22) Demostrar que, si el grupo G no es abeliano, entonces existe un subgrupo abeliano de G que contiene estrictamente al centro $Z(G)$.

(23) Demostrar que, si G el grupo diédrico D_4 o el de cuaterniones Q_8, entonces $Z(G) \simeq \mathbb{Z}_2$ y $G/Z(G) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, y sin embargo $D_4 \not\simeq Q_8$.

(24) Probar que, salvo isomorfismos, sólo hay dos grupos no abelianos de orden 8. ¿Cuáles son?

(25) Probar que todo grupo no abeliano de orden 6 es isomorfo a S_3.

(26) Demostrar que si H es un subgrupo abeliano de un grupo G tal que $HZ(G) = G$, entonces G es abeliano. Deducir que si $G/Z(G)$ es cíclico, entonces G es abeliano.

(27) Describir todos los subgrupos normales del grupo diédrico D_n.

(28) Calcular los centros de $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{C})$, $\mathrm{SL}_n(\mathbb{R})$ y $\mathrm{SL}_n(\mathbb{C})$.

(29) Calcular las clases de conjugación de los grupos del Problema 1 y de los grupos diédricos.

(30) Demostrar que p es primo, entonces todos los grupos de orden p^2 son abelianos.

(31) Si p es primo, probar que el centro de cualquier grupo no abeliano de orden p^3 tiene orden p.

(32) Sea G un grupo abeliano finito en el que, para cada $n \in \mathbb{Z}^+$, la ecuación $x^n = e$ tiene a lo sumo n soluciones. Demostrar que G es cíclico. Deducir que un subgrupo finito del grupo de unidades de un dominio es cíclico. (Indicación: Elegir un elemento de orden máximo y observar que para cada $g \in G$ de orden n, el subgrupo $\langle g \rangle$ contiene n soluciones de la ecuación $x^n = e$.)

(33) (a) Mostrar que las siguientes son acciones del grupo que se indica en el conjunto correspondiente.

i. De $\mathrm{Aut}(G)$ en un grupo G, dada por $\sigma \cdot x = \sigma(x)$ (por la izquierda).

ii. De un grupo G en G/H, donde H es un subgrupo, dada por $g \cdot xH = (gx)H$ (por la izquierda).

iii. De un grupo G en $H\backslash G$, donde H es un subgrupo, dada por $Hx \cdot g = H(xg)$ (por la derecha).

iv. De un grupo G en el conjunto S de sus subgrupos dada por $H \cdot g = H^g$ (por la derecha).

(b) Sea $\cdot : G \times X \to X$ una acción por la izquierda de un grupo G en un conjunto X. Si $x \in X$ entonces $G \cdot x = \{g \cdot x : g \in G\}$ se llama *órbita* de x y $\mathrm{Estab}_G(x) = \{g \in G : g \cdot x\}$ se llama *estabilizador* de x en G.

Demostrar las siguientes propiedades para cada $x \in X$ y $g \in G$.

i. La regla $x \cdot g = g^{-1} \cdot x$ define una acción por la derecha de G en X.

ii. Para cada $g \in G$, la aplicación $\overline{g} : X \to X$ dada por $\overline{g}(x) = g \cdot x$ es biyectiva y la aplicación $G \to S_X$ dada por $g \mapsto \overline{g}$ es un homomorfismo de grupos. Recíprocamente, mostrar como todo homomorfismo de grupos $G \to S_X$ induce una acción por la izquierda de G en X.

iii. $\mathrm{Estab}_G(x)$ es un subgrupo de G y $[G : \mathrm{Estab}_G(x)] = |G \cdot x|$, en particular si G es finito, entonces el cardinal de cada órbita es un divisor del orden de G.

iv. $\mathrm{Estab}_G(g \cdot x) = \mathrm{Estab}_G(x)^{g^{-1}}$. Concluir que $C_G(a^g) = C_G(a)^{g^{-1}}$

(c) Identificar las órbitas y los estabilizadores para las acciones de los Ejemplos 5.12 y del apartado (a).

(34) (Teorema de Cauchy) Demostrar que si G es un grupo finito cuyo orden es múltiplo de un primo p, entonces G tiene un elemento de orden p. (Indicación: Considérese $X = \{(x_1, x_2, \ldots, x_p) : x_1 x_2 \cdots x_p = 1\}$ y la siguiente acción del grupo cíclico $C_p = \langle g \rangle$ en X: $g \cdot (x_1, x_2, \ldots, x_p) = (x_p, x_1, x_2, \ldots, x_{p-1})$.)

(35) (Primer Teorema de Sylow) Demostrar que si G es un grupo de orden finito n y $n = p^m k$ con $p \nmid k$, entonces G tiene un subgrupo de orden p^m. Estos subgrupos se llaman *subgrupos de Sylow* de G. (Indicación: Razonar por inducción en n, aplicando la Ecuación de Clase en el caso en que p divide a $[G : C_G(g)]$ para todo $g \in G \setminus Z(G)$.

Capítulo 6

Grupos de permutaciones

Este es un capítulo recopilatorio de las principales propiedades del grupo simétrico que suponemos bien conocidas por lo que muchas de las demostraciones las omitiremos.

6.1 Ciclos y trasposiciones

Recordemos que, para cada número natural n, S_n denota el grupo simétrico sobre $\mathbb{N}_n = \{1, 2, \ldots, n\}$; es decir, el grupo de las aplicaciones biyectivas $f : \mathbb{N}_n \to \mathbb{N}_n$ con la composición de aplicaciones como operación. Describiremos a veces un elemento $f \in S_n$ dando la lista de sus imágenes en la forma

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}.$$

Definición 6.1 *Diremos que una permutación $\sigma \in S_n$* fija *un entero $i \in \mathbb{N}_n$ si $\sigma(i) = i$; en caso contrario diremos que σ* cambia *o* mueve *i, y denotaremos por $M(\sigma)$ al conjunto de los enteros cambiados por σ:*

$$M(\sigma) = \{i \in \mathbb{N}_n : \sigma(i) \neq i\}.$$

Es claro que $M(\sigma)$ es vacío si y sólo si $\sigma = 1$, y que $M(\sigma)$ no puede tener exactamente un elemento.

Diremos que dos permutaciones σ y τ de S_n son disjuntas *si lo son los conjuntos $M(\sigma)$ y $M(\tau)$. Es decir, si todos los elementos que cambia una de ellas son fijados por la otra.*

Cuando digamos que ciertas permutaciones $\sigma_1, \ldots, \sigma_r$ son disjuntas entenderemos que lo son dos a dos.

Lema 6.2 *Si σ y τ son permutaciones disjuntas entonces $\sigma\tau = \tau\sigma$ y se tiene $M(\sigma\tau) = M(\sigma) \cup M(\tau)$.*

Definición 6.3 *La permutación $\sigma \in S_n$ es un* ciclo *de longitud s (o un s-ciclo) si $M(\sigma)$ tiene s elementos y éstos pueden ordenarse de manera que se tenga $M(\sigma) = \{i_1, i_2, \ldots, i_s\}$ y*

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \ldots \quad \sigma(i_{s-1}) = i_s, \quad \sigma(i_s) = i_1.$$

Este s-ciclo σ se denota como

$$\sigma = (i_1\ i_2\ i_3\ \ldots\ i_s) \qquad ó \qquad \sigma = (i_1, i_2, i_3, \ldots, i_s).$$

Los 2-ciclos también se llaman transposiciones.

Por ejemplo, los siguientes elementos de S_4 son ciclos de longitudes 2, 3 y 4, respectivamente:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \qquad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

Lema 6.4 *Sea $\sigma = (i_1 \ldots i_s)$ un ciclo de longitud s en S_n.*

(1) Para cada $t \in \{1, 2, \ldots, s\}$ se tiene $\sigma = (i_t \ldots i_s\ i_1 \ldots i_{t-1})$.

(2) Para cada $t \in \{1, 2, \ldots, s\}$ se tiene $i_t = \sigma^{t-1}(i_1)$.

(3) El orden de σ (como elemento del grupo simétrico) coincide con su longitud s.

Teorema 6.5 *Toda permutación $\sigma \neq 1$ de S_n se puede expresar de forma única (salvo el orden) como producto de ciclos disjuntos.*

Ejemplo 6.6 *Factorización de una permutación como producto de ciclos disjuntos.*
Consideremos la permutación de S_{11}

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 6 & 5 & 1 & 4 & 2 & 7 & 3 & 8 & 11 & 9 & 10 \end{pmatrix}.$$

Elegimos un elemento arbitrario cambiado por σ, por ejemplo el 1, y calculamos sus imágenes sucesivas por σ:

$$\sigma(1) = 6,\ \sigma^2(1) = \sigma(6) = 7,\ \sigma^3(1) = \sigma(7) = 3,\ \sigma^4(1) = \sigma(3) = 1.$$

Entonces (1 6 7 3) es uno de los factores de σ. Elegimos ahora un elemento de $M(\sigma)$ que no haya aparecido aún, por ejemplo el 2, y le volvemos a seguir la pista, lo que nos da un nuevo factor (2 5). Empezando ahora con el 9 obtenemos un tercer ciclo (9 11 10) que agota el proceso (el 4 y el 8 son fijados por σ) y nos dice que $\sigma = (1\ 6\ 7\ 3)(2\ 5)(9\ 11\ 10)$.

Veamos cómo se puede calcular el orden de una permutación en términos de su factorización como producto de ciclos disjuntos:

Proposición 6.7 *Sea $\sigma = \tau_1 \cdots \tau_k$ la factorización de una permutación σ como producto de ciclos disjuntos, y sea s_i la longitud del ciclo τ_i. Entonces*

$$o(\sigma) = \text{mcm}(s_1, \ldots, s_k).$$

Demostración. Sea $m \in \mathbb{N}$. Como los τ_i conmutan entre sí, se tiene $\sigma^m = \tau_1^m \cdots \tau_k^m$. Por otra parte, para cada i se tiene $M(\tau_i^m) \subseteq M(\tau_i)$ y por tanto los τ_i^m son disjuntos. Esto implica, por la unicidad en el Teorema 6.5, que $\sigma^m = 1$ precisamente si cada $\tau_i^m = 1$, y entonces el resultado es claro, pues s_i es el orden de τ_i. ∎

A continuación vamos a describir las clases de conjugación de S_n.

Definición 6.8 *El* tipo *de una permutación $\sigma \neq 1$ de S_n es la lista $[s_1, \ldots, s_k]$ de las longitudes de los ciclos que aparecen en su factorización en ciclos disjuntos, ordenadas en forma decreciente. Por convenio, la permutación identidad tiene tipo* [1].

Por ejemplo, el tipo de un s-ciclo es $[s]$, el de la permutación $(1\ 2)(3\ 4\ 5)(6\ 7) \in S_7$ es $[3, 2, 2]$, y el de la permutación de S_{11} del Ejemplo 6.6 es $[4, 3, 2]$.

Teorema 6.9 *Dos elementos de S_n son conjugados precisamente si tienen el mismo tipo. En consecuencia, cada clase de conjugación de S_n está formada por todos los elementos de un mismo tipo.*

Observación 6.10 *La factorización en ciclos disjuntos de σ^α se obtiene sustituyendo, en la de σ, cada elemento $i \in \mathbb{N}_n$ por $\alpha^{-1}(i)$.*

Por ejemplo, si $\alpha = (1\ 4\ 3)(2\ 5\ 6)$ y $\sigma = (1\ 3)(2\ 4\ 7)$, entonces $\sigma^\alpha = (3\ 4)(6\ 1\ 7)$.

Ejemplo 6.11 *Clases de conjugación de S_n.*

Las 6 permutaciones de S_3 se dividen en una permutación de tipo [1] (la identidad), tres 2-ciclos o permutaciones de tipo [2] (a saber, (1 2), (1 3) y (2 3)), y dos 3-ciclos o permutaciones de tipo [3] (a saber, (1 2 3) y (1 3 2)).

En S_4 hay más variedad, y en particular aparecen permutaciones que no son ciclos. Sus 24 permutaciones se dividen en los siguientes tipos:

Tipo	Permutaciones
[1]	1
[2]	(1 2), (1 3), (1 4), (2 3), (2 4), (3 4)
[3]	(1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3)
[4]	(1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2)
[2,2]	(1 2)(3 4), (1 3)(2 4), (1 4)(2 3)

Por tanto, cada fila de elementos a la derecha de la barra es una clase de conjugación de S_4.

Además de los ciclos, en S_5 hay permutaciones de los tipos $[2, 2]$ y $[3, 2]$; y en S_6 las hay de los tipos $[2, 2]$, $[3, 2]$, $[2, 2, 2]$ y $[3, 3]$. En estos casos, por el gran número de elementos en los grupos, es pesado construir tablas como la que acabamos de dar para S_4, pero se puede al menos calcular cuántas permutaciones hay de cada tipo (véase el Problema 7).

Proposición 6.12 *Para $n > 2$, los siguientes son conjuntos generadores de S_n:*

(1) El conjunto de todos los ciclos.

(2) El conjunto de todas las trasposiciones.

(3) El conjunto de $n-1$ trasposiciones: $\{(1\ 2), (1\ 3), (1\ 4), \ldots, (1\ n-1), (1\ n)\}$.

(4) El conjunto de $n-1$ trasposiciones: $\{(1\ 2), (2\ 3), (3\ 4), \ldots, (n-1\ n)\}$.

(5) El conjunto de una trasposición y un n-ciclo: $\{(1\ 2), (1\ 2\ 3\ \ldots\ n-1\ n)\}$.

Demostración. 1. Es una consecuencia inmediata del Teorema 6.5.

Para demostrar el resto de apartados bastará con comprobar que los elementos del conjunto dado en cada apartado se expresan como productos de los elementos del conjunto del apartado siguiente.

2. Cada ciclo $\sigma = (i_1\ i_2\ \ldots\ i_s)$ puede escribirse como producto de trasposiciones (no disjuntas):

$$\sigma = (i_1\ i_s)(i_1\ i_{s-1})\cdots(i_1\ i_3)(i_1\ i_2).$$

3. Es consecuencia de la igualdad $(i\ j) = (1\ i)(1\ j)(1\ i)$.

4. Dado $j \geq 2$, sea $\alpha = (2\ 3)(3\ 4)(4\ 5)\cdots(j-1\ j)$. Usando la Observación 6.10 se obtiene $(1\ 2)^\alpha = (1\ j)$.

5. Sean $\tau = (1\ 2)$ y $\sigma = (1\ 2\ \ldots\ n-1\ n)$. Como σ^{j-1} lleva $1 \mapsto j$ y $2 \mapsto j+1$, la Observación 6.10 nos dice que $\sigma^{j-1}\tau\sigma^{1-j} = (j, j+1)$. ∎

Corolario 6.13 *Sean p un número primo y H un subgrupo de S_p. Si H contiene una trasposición y un p-ciclo, entonces $H = S_p$.*

Demostración. Podemos suponer que H contiene a $(1\ 2)$ y un p-ciclo $\sigma = (a_1\ a_2\ \ldots\ a_p)$. Por el Lema 6.4, podemos suponer que $a_1 = 1$. Si $a_i = 2$, entonces $\sigma^{i-1} = (1\ 2\ b_3\ \ldots\ b_p)$ y podemos renombrar los b_i de forma que $b_i = i$. Por tanto $(1\ 2), (1\ 2\ \ldots\ p) \in H$. Deducimos de la Proposición 6.12 que $H = S_p$. ¿Dónde hemos utilizado que p es primo? ∎

Aunque toda permutación de S_n se puede expresar como un producto de trasposiciones, estas expresiones no tienen las buenas propiedades que vimos en las descomposiciones en ciclos. Por una parte, no podemos esperar que una permutación arbitraria sea producto de trasposiciones disjuntas (tendría orden 2). Por otra, tampoco se tiene conmutatividad (por ejemplo, $(1\ 3)(1\ 2) \neq (1\ 2)(1\ 3)$) ni unicidad, ni siquiera en el número de factores; por ejemplo

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 3)(1\ 3) = (1\ 3)(2\ 4)(1\ 2)(1\ 4) = (2\ 3)(2\ 3)(1\ 3)(2\ 4)(1\ 2)(1\ 4).$$

Nótese que en todas estas factorizaciones de $(1\ 2\ 3)$ hay un número par de trasposiciones; esto es consecuencia de un hecho general que analizaremos en la sección siguiente (Proposición 6.16).

6.2 El grupo alternado

Fijemos un entero positivo $n \geq 2$ y una permutación $\sigma \in S_n$. Por la Propiedad Universal de los Anillos de Polinomios, existe un homomorfismo de anillos $\bar{\sigma} : \mathbb{Z}[X_1, \ldots, X_n] \to \mathbb{Z}[X_1, \ldots, X_n]$ tal que $\bar{\sigma}(X_i) = X_{\sigma(i)}$ para cada i (Ejemplos 3.33). Es decir, dado un polinomio Q, su imagen $\bar{\sigma}(Q)$ se obtiene sustituyendo cada X_i por $X_{\sigma(i)}$ en la expresión de Q.

En lo que sigue, P designará al polinomio de $\mathbb{Z}[X_1, \ldots, X_n]$ dado por

$$P = \prod_{1 \leq i < j \leq n} (X_j - X_i).$$

La condición $i < j$ implica que cada diferencia entre dos indeterminadas distintas aparece, en cierto orden, exactamente una vez en esa factorización. Como $\bar{\sigma}$ es un homomorfismo de anillos, se tiene

$$\bar{\sigma}(P) = \prod_{i<j} \bar{\sigma}(X_j - X_i) = \prod_{i<j} (X_{\sigma(j)} - X_{\sigma(i)}).$$

Como σ es una biyección, cada diferencia entre dos indeterminadas distintas sigue apareciendo, en cierto orden, exactamente una vez en esta factorización. Fijados $i < j$ pueden ocurrir dos cosas:

- Que sea $\sigma(i) < \sigma(j)$, en cuyo caso el factor $X_{\sigma(j)} - X_{\sigma(i)}$ aparece en $\bar{\sigma}(P)$ igual que en P.
- Que sea $\sigma(i) > \sigma(j)$, en cuyo caso el factor $X_{\sigma(j)} - X_{\sigma(i)}$ aparece en $\bar{\sigma}(P)$ en el orden contrario que en P; en este caso diremos que σ *presenta una inversión* para el par (i, j).

Como cada inversión se traduce en un cambio de signo en $\bar{\sigma}(P)$ con respecto a P, se tiene $\bar{\sigma}(P) = \pm P$, donde el signo es $+$ si y sólo si el número de pares (i, j) (con $i < j$) para los que σ presenta una inversión es par. Esto sugiere las definiciones que siguen:

Definición 6.14 *La permutación $\sigma \in S_n$ es* par *si $\bar{\sigma}(P) = P$; es decir, si σ presenta un número par de inversiones; y es* impar *si $\bar{\sigma}(P) = -P$; es decir, si σ presenta un número impar de inversiones.*

El signo *de σ se define como $\operatorname{sg}(\sigma) = (-1)^k$, donde k es el número de inversiones que presenta σ. Es decir, $\operatorname{sg}(\sigma) = 1$ si σ es par y $\operatorname{sg}(\sigma) = -1$ si σ es impar. Por el comentario previo a esta definición se tiene $\bar{\sigma}(P) = \operatorname{sg}(\sigma)P$.*

Proposición 6.15 *La "aplicación signo" $\operatorname{sg} : S_n \to \mathbb{Z}^* = \{1, -1\}$ es un homomorfismo de grupos.*

Demostración. Sean $\sigma, \tau \in S_n$. Es claro que $\bar{\sigma} \circ \bar{\tau} = \overline{\sigma \circ \tau}$, y por tanto

$$\operatorname{sg}(\sigma \circ \tau)P = \overline{\sigma \circ \tau}(P) = \bar{\sigma}(\bar{\tau}(P)) = \bar{\sigma}(\operatorname{sg}(\tau)P) = \operatorname{sg}(\tau)\bar{\sigma}(P) = \operatorname{sg}(\tau)\operatorname{sg}(\sigma)P,$$

y por tanto $\operatorname{sg}(\sigma \circ \tau) = \operatorname{sg}(\sigma)\operatorname{sg}(\tau)$. ∎

Proposición 6.16 *En S_n se verifica:*

(1) El signo de una permutación σ es el mismo que el de su inversa σ^{-1} y que el de cualquiera de sus conjugadas σ^α.

(2) Toda trasposición es impar.

(3) Si $\sigma = \tau_1 \cdots \tau_r$, donde las τ_i son trasposiciones, entonces $\mathrm{sg}(\sigma) = (-1)^r$.

(4) Una permutación σ es par (respectivamente impar) si y sólo si es producto de un número par (respectivamente impar) de trasposiciones.

(5) Un ciclo de longitud s tiene signo $(-1)^{s-1}$; es decir, un ciclo de longitud par es impar, y viceversa.

(6) La paridad de una permutación coincide con la del número de componentes pares de su tipo.

Ejemplo 6.17 *Calculando la paridad en función del tipo.*

Del Ejemplo 6.11 y del último apartado de la Proposición 6.16 se deduce que, además de la identidad, las permutaciones pares de S_3 son las de tipo [3]; las de S_4 son las de los tipos [3] ó $[2,2]$; las de S_5 son las de los tipos [3], [5] ó $[2,2]$; y las de S_6 son las de los tipos [3], [5], $[2,2]$ ó $[3,3]$.

Definición 6.18 *El* grupo alternado *en n elementos, denotado por A_n, es el núcleo del homomorfismo* $\mathrm{sg} : S_n \to \mathbb{Z}^* = \{1, -1\}$. *Es decir, es el subgrupo de S_n formado por las permutaciones pares.*

Proposición 6.19 *A_n es un subgrupo normal de S_n, y para $n \geq 2$ se tiene:*

$$[S_n : A_n] = 2, \qquad |A_n| = \frac{n!}{2}, \qquad y \qquad \frac{S_n}{A_n} \simeq \{1, -1\} \simeq \mathbb{Z}_2.$$

Demostración. Al estar definido como el núcleo de un homomorfismo, A_n es normal en S_n. El resto es consecuencia del Primer Teorema de Isomorfía si vemos que, para $n \geq 2$, el homomorfismo sg es suprayectivo, para lo que basta notar que $\mathrm{sg}(1) = 1$ y $\mathrm{sg}(1\ 2) = -1$. ∎

Es elemental ver que A_2 es el grupo trivial y que A_3 es el subgrupo cíclico de S_3 generado por el 3-ciclo (1 2 3), y por tanto $A_3 \simeq C_3$. En el caso general, tenemos dos maneras sencillas de describir conjuntos de generadores de A_n.

Proposición 6.20 *Los siguientes son sistemas de generadores de A_n:*

(1) El conjunto de todos los productos de dos trasposiciones (disjuntas o no).

(2) El conjunto de todos los 3-ciclos.

Demostración. El apartado 1 es una consecuencia inmediata del apartado 4 de la Proposición 6.16. Por la misma proposición, todos los 3-ciclos están en A_n; por tanto, usando 1, para ver 2 sólo hay que probar que cada producto de dos trasposiciones distintas (disjuntas o no) se puede escribir como producto de 3-ciclos, lo que se sigue de las igualdades

$$(i\ j)(i\ k) = (i\ k\ j) \qquad \text{e} \qquad (i\ j)(k\ l) = (j\ l\ k)(i\ k\ j),$$

donde asumimos que i, j, k, l son distintos dos a dos. ∎

Obsérvese que, como el conjunto vacío genera el subgrupo trivial, la Proposición 6.20 es válida incluso cuando $n = 1$ ó $n = 2$.

A continuación describimos los subgrupos de A_4. Esto nos dará un ejemplo en el que no se verifica el recíproco del Teorema de Lagrange: A_4 tiene orden 12, pero no tiene subgrupos de orden 6.

Ejemplo 6.21 *Subgrupos de A_4.*

En virtud del Ejemplo 6.17, la siguiente es la lista completa de los elementos de A_4:

1	$\sigma = (1\ 2)(3\ 4)$	$\tau = (1\ 3)(2\ 4)$	$\eta = (1\ 4)(2\ 3)$
$\alpha = (1\ 2\ 3)$	$\beta = (1\ 2\ 4)$	$\gamma = (1\ 3\ 4)$	$\delta = (2\ 3\ 4)$
$\alpha^2 = (1\ 3\ 2)$	$\beta^2 = (1\ 4\ 2)$	$\gamma^2 = (1\ 4\ 3)$	$\delta^2 = (2\ 4\ 3)$

Por el Teorema de Lagrange, los subgrupos propios y no triviales de A_4 han de tener orden 2, 3, 4, ó 6. Los de orden 2 han de estar generados por elementos de orden 2, y por tanto son:

$$\langle\sigma\rangle = \{1, \sigma\} \qquad \langle\tau\rangle = \{1, \tau\} \qquad \langle\eta\rangle = \{1, \eta\}.$$

Como $\sigma^\alpha = \tau \notin \langle\sigma\rangle$, deducimos que $\langle\sigma\rangle$ no es normal en A_4, y del mismo modo se ve que no lo son $\langle\tau\rangle$ ni $\langle\eta\rangle$. Los subgrupos de orden 3 han de estar generados por elementos de orden 3, y por tanto son:

$$\langle\alpha\rangle = \langle\alpha^2\rangle = \{1, \alpha, \alpha^2\} \qquad \langle\beta\rangle = \langle\beta^2\rangle = \{1, \beta, \beta^2\}$$
$$\langle\gamma\rangle = \langle\gamma^2\rangle = \{1, \gamma, \gamma^2\} \qquad \langle\delta\rangle = \langle\delta^2\rangle = \{1, \delta, \delta^2\}.$$

Un subgrupo de orden 4 no puede contener a ninguno de los elementos de orden 3; como el resto de elementos forman un subgrupo

$$N = \{1, \sigma, \tau, \eta\},$$

éste es el único subgrupo de orden 4, que además es normal en S_n por el Teorema 6.9. Por último, veamos que no hay subgrupos de orden 6. Un tal subgrupo H sería normal en A_4 por tener índice 2, por lo que también $N \cap H$ sería normal en A_4. Además se tendría $NH = A_4$ (¿por qué?) y en consecuencia $|N \cap H| = 2$ (Teorema 5.9), en contra del hecho de que ninguno de los subgrupos de orden 2 de A_4 es normal.

6.3 El Teorema de Abel

Definición 6.22 *Un grupo no trivial G es* simple *si sus únicos subgrupos normales son $\{1\}$ y G.*

Como consecuencia inmediata de la Proposición 4.9 se tiene que un grupo abeliano es simple si y sólo si tiene orden primo. Obsérvese que $A_3 \simeq C_3$ es simple, pero A_4 no lo es, como muestra el Ejemplo 6.21.

Lema 6.23 *Si un subgrupo normal H de A_n ($n \geq 5$) contiene un 3-ciclo, entonces $H = A_n$.*

Demostración. Sea σ un 3-ciclo en H. Por la Proposición 6.20, basta ver que cualquier otro 3-ciclo σ' está en H. Sabemos por el Teorema 6.9 que existe $\alpha \in S_n$ tal que $\sigma' = \sigma^\alpha$, de modo que si $\alpha \in A_n$ entonces $\sigma' \in H$, por la normalidad de H en A_n; en consecuencia, podemos suponer que α es una permutación impar. Como σ sólo cambia 3 elementos y $n \geq 5$, existe una trasposición β disjunta con σ, por lo que $\sigma^\beta = \sigma$. Por tanto

$$\sigma^{\beta\alpha} = (\sigma^\beta)^\alpha = \sigma^\alpha = \sigma',$$

y como $\beta\alpha$ está en A_n por ser el producto de dos permutaciones impares, la normalidad de H en A_n implica que $\sigma' \in H$, como queríamos ver. ∎

Obsérvese que la hipótesis $n \geq 5$ en el Lema anterior es superflua, pues para $n \leq 3$ es obvio que se verifica el Lema y para $n = 4$ es consecuencia del Ejemplo 6.21.

Teorema 6.24 (Abel) *Si $n \geq 5$, entonces A_n es un grupo simple.*

Demostración. Supongamos que $H \neq \{1\}$ es un subgrupo normal de A_n y veamos que $H = A_n$. Por el Lema 6.23, bastará probar que H contiene un 3-ciclo.

Sea $1 \neq \sigma \in H$ tal que $r = |M(\sigma)|$ sea mínimo, es decir, $|M(\nu)| \leq r$ para todo $1 \neq \nu \in H$. Ahora veremos que debe tenerse $r = 3$, por lo que σ será un 3-ciclo en H y habremos terminado.

Desde luego, no puede ser $r = 1$ porque ninguna permutación cambia exactamente un elemento, ni tampoco $r = 2$ porque todas las permutaciones de H son pares. Supongamos pues, en busca de una contradicción, que $r > 3$. Se tienen entonces dos posibilidades:

(1) Que, en la factorización de σ en ciclos disjuntos, aparezca alguno de longitud ≥ 3.

(2) Que σ sea un producto de (al menos dos) trasposiciones disjuntas.

En el primer caso, σ debe cambiar al menos 5 elementos (si sólo cambiase 4, como en la factorización de σ aparece un ciclo de longitud ≥ 3, σ sería un 4-ciclo, lo que contradice el hecho de que $\sigma \in A_n$). Podemos suponer, sin pérdida de generalidad (¿por qué?), que $1, 2, 3, 4, 5 \in M(\sigma)$ y que alguno de los ciclos disjuntos que componen σ es de la forma $(1\ 2\ 3\ \dots)$ (con longitud al menos 3). Sea $\alpha = (3\ 4\ 5)$. Como $\alpha \in A_n$ y H es normal en A_n, deducimos que $\sigma^\alpha \in H$, y así $\beta = \sigma^{-1}\sigma^\alpha \in H$. Si $\sigma(i) = i$ entonces $i > 5$ y por tanto $\alpha(i) = i$, de donde se sigue que $\beta(i) = i$; por tanto $M(\beta) \subseteq M(\sigma)$, y la inclusión es estricta pues $\sigma(1) = 2$ mientras que $\beta(1) = 1$. En consecuencia, $\beta \in H$ cambia menos de r elementos, así que debe ser $\beta = 1$,

por la elección de r. Esto significa que $\sigma^\alpha = \sigma$, y por tanto $\alpha\sigma = \sigma\alpha$. Pero esto es falso, pues $\alpha\sigma(2) = 4$ y $\sigma\alpha(2) = 3$, de manera que la primera de las dos posibilidades consideradas nos lleva a una contradicción.

Pasamos al segundo caso. Reordenando los elementos de $\mathbb{N}_n$ podemos asumir que $\sigma = (1\ 2)(3\ 4)\cdots$ (puede haber más trasposiciones en el producto o no). Sea de nuevo $\alpha = (3\ 4\ 5)$. Como antes, tomamos $\beta = \sigma^{-1}\sigma^\alpha \in H$. Si $i \neq 5$ y $\sigma(i) = i$ entonces $i \neq 3, 4, 5$ y por tanto $\alpha(i) = i$, de donde se sigue que $\beta(i) = i$; por tanto $M(\beta) \subseteq M(\sigma) \cup \{5\}$. Pero el 1 y el 2 son fijados por β y cambiados por σ, de modo que β cambia menos de r elementos y así $\beta = 1$, o sea $\sigma\alpha = \alpha\sigma$. Pero se tiene $\sigma\alpha(3) = 3 \neq 5 = \alpha\sigma(3)$. En cualquier caso, pues, llegamos a la contradicción que buscábamos. ∎

6.4 Problemas

(1) Calcular σ^{1000}, donde $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 5 & 2 & 6 & 1 & 7 & 4 & 0 & 9 & 11 & 8 \end{pmatrix}$.

(2) Dada la permutación $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 9 & 8 & 2 & 3 & 4 & 6 & 7 \end{pmatrix}$, calcular el orden de σ^2.

(3) Sea $1 \neq \sigma \in S_n$. Demostrar que σ es un ciclo si y sólo si, para cualesquiera $j, k \in M(\sigma)$, existe un entero m tal que $\sigma^m(j) = k$.

(4) Probar que para toda permutación $\sigma \in S_n$ se cumple $\sigma(i_1 \cdots i_r)\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_r))$.

(5) Demostrar que una permutación tiene orden primo p si y sólo si se factoriza como un producto de ciclos disjuntos, cada uno de longitud p.

(6) Demostrar que para todo $1 \leq k < n$, S_n tiene al menos $\binom{n}{k}$ subgrupos isomorfos a $S_k \times S_{n-k}$ y que todos son conjugados; es decir, para dos de estos grupos H y K existe $\sigma \in G$ tal que $H^\sigma = K$.

(7) Dados dos números naturales n y k con $n \geq k \geq 2$, se pide:

   (a) Demostrar que, para cada subconjunto A de $\mathbb{N}_n$ de cardinal k, el número de k-ciclos σ de S_n con $M(\sigma) = A$ es $(k-1)!$.

   (b) Demostrar que el número de k-ciclos en S_n es $\binom{n}{k}(k-1)!$.

   (c) ¿Cuántos elementos de tipo $[2, 2]$ hay en S_5? ¿Cuántos de tipo $[2, 3]$?

   (d) ¿Cuántos elementos de tipo $[2, 2]$ hay en S_6? ¿Cuántos de tipo $[2, 3]$? ¿Y de tipo $[3, 3]$?

   (e) [*] Calcular en general el número de elementos de S_n de tipo $[k_1, \ldots, k_r]$.

(8) Sea G un grupo finito de orden n, y sea $g \in G$ de orden m. Se define $\phi_g : G \to G$ por $\phi_g(x) = gx$. Viendo a ϕ_g como un elemento de S_n, demostrar que:

   (a) ϕ_g es un producto de n/m ciclos de longitud m.

(b) La paridad de ϕ_g coincide con la paridad del entero $(m-1)\frac{n}{m}$.

(c) Si $(m-1)\frac{n}{m}$ es impar, entonces G tiene un subgrupo normal de índice 2.

(9) (Teorema de Cayley) Demostrar que todo grupo finito es isomorfo a un subgrupo de S_n para algún n.

(10) Demostrar que el centralizador de la permutación $\sigma = (1, 2, \ldots, n)$ en S_n es $\langle\sigma\rangle$.

(11) Demostrar que el grupo alternado A_n es un subgrupo característico del grupo simétrico S_n.

(12) Sea $n \geq 2$ y sea $f : S_n \to S_{n+2}$ la aplicación dada por $f(\sigma) = \sigma^*$, donde σ^* actúa igual que σ sobre los elementos $1, 2, \ldots, n$, y σ^* fija (respectivamente, intercambia) $n+1$ y $n+2$ cuando σ es par (respectivamente, impar). Demostrar que f es un homomorfismo inyectivo de grupos y que su imagen está contenida en A_{n+2}. Deducir que todo grupo finito es isomorfo a un subgrupo de un grupo alternado.

(13) Probar que si P es un subgrupo de orden 4 del grupo alternado A_5, entonces P es isomorfo al grupo de Klein $C_2 \times C_2$.

(14) Demostrar que D_n es isomorfo al subgrupo $\langle\rho, \sigma\rangle$ de S_n, donde $\rho = (1, 2, \ldots, n-1, n)$ y σ es el producto de las trasposiciones $(i, n+1-i)$, donde i varía desde 1 hasta la parte entera de $n/2$. ¿Para qué valores de n se tiene $\langle\rho, \sigma\rangle \subseteq A_n$?

(15) Dado $f \in \mathrm{Aut}(S_3)$, probar que f induce una permutación del conjunto $X = \{(1\,2), (1\,3), (2\,3)\} \subset S_3$. Deducir que la aplicación $\iota : S_3 \to \mathrm{Aut}(S_3)$ que lleva $\sigma \in S_3$ al automorfismo interno ι_σ es un isomorfismo de grupos.

(16) Demostrar que A_n está generado por los 3-ciclos de la forma $(1, 2, i)$ con $i = 3, \ldots, n$.

(17) Para $n \geq 5$, demostrar que S_n tiene exactamente tres subgrupos normales.

(18) Para $n \geq 2$, demostrar que A_n es el único subgrupo de índice dos de S_n.

(19) [*] Sea p un primo impar y sea H un subgrupo propio de S_p que contiene una trasposición. Demostrar que existen $i, j \in \mathbb{N}_p$ tales que $\sigma(i) \neq j$ para todo $\sigma \in H$. (Indicación: Considerar en $\mathbb{N}_p$ la relación de equivalencia en la que $i \sim j$ si $i = j$ ó si $(i, j) \in H$, y comparar el número de elementos de las clases de equivalencia.)

(20) [*] Sea $S_\infty = S(\mathbb{N})$ el grupo de permutaciones del conjunto numerable $\mathbb{N}$. El *grupo alternado infinito* es el subgrupo A_∞ de S_∞ generado por todos los 3-ciclos (donde un 3-ciclo se define del modo obvio). Demostrar que A_∞ es un grupo simple infinito.

Capítulo 7

Grupos Abelianos Finitos

7.1 Sumas directas

Un modo habitual de estudiar un objeto matemático consiste en descomponerlo en objetos más sencillos, estudiar éstos y recomponer entonces el objeto inicial. Lo que se entiende por objeto sencillo y la manera de descomponer y recomponer un objeto dependen de cada caso. En este capítulo el objeto estudiado será un grupo abeliano finitamente generado A, y los objetos sencillos serán los grupos cíclicos, que ya conocemos bien. En este contexto, el proyecto sugerido al principio del párrafo funciona porque existe un método muy efectivo para descomponer A de modo que es muy fácil conocer A a partir de sus componentes. Se trata de la suma directa de subgrupos, que analizamos en esta sección.

Proposición 7.1 *Sean $\{B_1, \ldots, B_n\}$ subgrupos de un grupo abeliano A. Entonces las condiciones siguientes son equivalentes:*

(1) El 0 se expresa de manera única como suma de elementos de los B_i. Es decir, si $b_1 + \cdots + b_n = 0$ con cada $b_i \in B_i$, entonces se tiene $b_i = 0$ para cada $i = 1, \ldots, n$.

(2) Cada elemento de $B_1 + \cdots + B_n$ se expresa de manera única como suma de elementos de los B_i. Es decir, si $b_1 + \cdots + b_n = b'_1 + \cdots + b'_n$ con cada $b_i \in B_i$ y cada $b'_i \in B_i$, entonces se tiene $b_i = b'_i$ para cada $i = 1, \ldots, n$.

(3) Para cada $j = 1, \ldots, n$ se verifica $B_j \cap (\sum_{i \neq j} B_i) = 0$.

Demostración. La equivalencia entre las dos primeras condiciones se deduce de un argumento típico que el lector conocerá del álgebra lineal, y se deja como ejercicio. Veamos pues que las condiciones 1 y 3 son equivalentes.

Si se verifica 1 y $x \in B_j \cap (\sum_{i \neq j} B_i)$, entonces $x \in B_j$ y existen $b_1, \ldots, b_{j-1}, b_{j+1}, \ldots, b_n$ tales que $x = b_1 + \cdots + b_{j-1} + b_{j+1} + \cdots + b_n$. Haciendo $b_j = -x$ se tiene $b_1 + \cdots + b_n = 0$, luego $b_j = 0$ y así $x = 0$. Recíprocamente, si se verifica 3 y se tiene $b_1 + \cdots + b_n = 0$ con cada $b_i \in B_i$ entonces, para cada índice j, se tiene $b_j = -(b_1 + \ldots + b_{j-1} + b_{j+1} + \ldots + b_n) \in B_j \cap (\sum_{i \neq j} B_i) = 0$, luego $b_j = 0$. ∎

La Proposición 7.1 se puede generalizar a una familia infinita de subgrupos. Explícitamente:

Ejemplo 7.2 *Sea $\{B_i : i \in I\}$ una familia de subgrupos de un grupo abeliano A. Entonces las condiciones siguientes son equivalentes:*

(1) El 0 se expresa de manera única como suma de elementos de los B_i. Es decir, si $\sum_{i\in I} b_i = 0$ con cada $b_i \in B_i$ y $b_i = 0$, para casi todo $i \in I$, entonces se tiene $b_i = 0$ para cada $i \in I$.

(2) Cada elemento de $\sum_{i\in I} B_i$ se expresa de manera única como suma de elementos de los B_i. Es decir, si $\sum_{i\in I} b_i = \sum_{i\in I} b'_i$ con cada $b_i, b'_i \in B_i$, $b_i = 0$ para casi todo $i \in I$ y $b'_i = 0$ para casi todo $i \in I$, entonces se tiene $b_i = b'_i$ para cada $i \in I$.

(3) Para cada $j \in I$ se verifica $B_j \cap (\sum_{i\neq j} B_i) = 0$.

Definición 7.3 *Si se verifican las condiciones equivalentes de la Proposición 7.1 (o del Ejercicio 7.2 en el caso infinito), se dice que la familia de subgrupos $\{B_1, \ldots, B_n\}$ es* independiente*, o que los subgrupos B_i son independientes. Su suma, $\sum_{i=1}^n B_i = B_1 + \cdots + B_n$, se llama entonces la* suma directa *de la familia $\{B_1, \ldots, B_n\}$, y se denota por $\oplus_{i=1}^n B_i = B_1 \oplus \cdots \oplus B_n$ (o por $\oplus_{i\in I} B_i$ en el caso infinito).*

La expresión "Sea $A = B_1 \oplus \cdots \oplus B_n$" quiere decir que los B_i son subgrupos independientes del grupo abeliano A y que su suma vale A.

Un subgrupo B de A es un sumando directo *de A si existe otro subgrupo C de A tal que $A = B \oplus C$; es decir, tal que $A = B + C$ y $B \cap C = 0$. En este caso se dice que C es un* complemento directo *de B.*

Ejemplos 7.4 *Subgrupos independientes y sumas directas.*

(1) En el grupo $A = \mathbb{Z}_6$ los subgrupos $B = \langle 2\rangle$ y $C = \langle 3\rangle$ son independientes y se tiene $A = B \oplus C$.

(2) En el grupo multiplicativo $\mathbb{R}^*$ se tiene $\mathbb{R}^* = \langle -1\rangle \oplus \mathbb{R}^+$.

(3) Si A y B son grupos abelianos, entonces el grupo producto $A \times B$ es la suma directa de los subgrupos $A \times 0$ y $0 \times B$.

(4) El complemento directo de un sumando directo no es, en general, único. Por ejemplo, para cualquier $a \in \mathbb{Z}$ se tiene $\mathbb{Z}\times\mathbb{Z} = \langle(1,0)\rangle \oplus \langle(a,1)\rangle$: la intersección es claramente nula, y un elemento arbitrario (x, y) de $\mathbb{Z}\times\mathbb{Z}$ se puede expresar como $(x, y) = y(a, 1)+(x-ya)(1, 0)$.

(5) En $\mathbb{Q}$ no hay dos subgrupos no triviales que sean independientes. En efecto, si A y B son subgrupos no nulos y elegimos elementos no nulos $\frac{a}{n} \in A$ y $\frac{b}{m} \in B$, entonces $0 = bn\frac{a}{n} - am\frac{b}{m}$ nos da una expresión no trivial del 0 como suma de elementos de A y B. En $\mathbb{Z}$ ocurre lo mismo, por un argumento similar.

Ejemplo 7.5 *Demostrar las siguientes afirmaciones sobre un grupo abeliano A.*

(1) Toda subfamilia de una familia independiente de subgrupos de A es independiente. Es decir, si $\{B_i : i \in I\}$ es una familia independiente de subgrupos de A y J es un subconjunto del conjunto de índices I, entonces la familia $\{B_i : i \in J\}$ es independiente.

(2) *Una familia de subgrupos es independiente precisamente si toda subfamilia finita suya lo es.*

(3) *Si la familia* $\{B_i : i \in I\}$ *de subgrupos de un grupo abeliano* A *es independiente y otro subgrupo* B_0 *de* A *verifica* $B_0 \cap (\oplus_{i\in I} B_i) = 0$*, entonces la familia* $\{B_0\} \cup \{B_i : i \in I\}$ *también es independiente.*

En particular, si a una familia independiente le añadimos el subgrupo trivial 0 (una o más veces), seguimos teniendo una familia independiente.

(4) *Si* $A = \oplus_{i\in I} B_i$ *entonces cada* B_j *es un sumando directo de* A *con complemento* $\oplus_{i\neq j} B_i$*.*

(5) *Si* $A = B \oplus C$ *y, a su vez,* $B = B_1 \oplus \cdots \oplus B_n$ *y* $C = C_1 \oplus \cdots \oplus C_m$*, entonces* $A = B_1 \oplus \cdots \oplus B_n \oplus C_1 \oplus \cdots \oplus C_m$*.*

(6) *Si* $A = B \oplus C$ *entonces la aplicación* $A \to C$ *dada por* $b + c \mapsto c$ *(donde* $b + c$ *es la expresión única de un elemento arbitrario de* A *con* $b \in B$ *y* $c \in C$*) es un homomorfismo suprayectivo de grupos con núcleo* B*. En particular,* $C \cong A/B$*.*

(7) *Si* B *es un sumando directo de* A*, cualquier complemento directo suyo es isomorfo a* A/B*. Por tanto, aunque un sumando directo puede tener distintos complementos directos, todos ellos son isomorfos entre sí.*

Cuando sólo consideramos familias finitas, existe una estrecha relación entre los conceptos de suma directa y producto directo de grupos, que describimos a continuación dejando los detalles a cargo del lector.

Supongamos primero que $A = B_1 \oplus \cdots \oplus B_n$. Entonces, viendo cada B_i como grupo y considerando su producto $B_1 \times \cdots \times B_n$, la aplicación $B_1 \times \cdots \times B_n \to A$ dada por $(b_1, \ldots, b_n) \mapsto b_1 + \cdots + b_n$ es un isomorfismo de grupos. Es decir, si A es la suma directa de los B_i, entonces A es isomorfo al producto directo de los B_i.

Recíprocamente, sean $B_1, \ldots, B_n$ grupos abelianos y sea A el grupo producto, $A = B_1 \times \cdots \times B_n$. Si denotamos por $\hat{B}_i$ al subgrupo de A formado por los elementos que llevan ceros en todas las coordenadas excepto tal vez en la i-ésima (o sea $\hat{B}_i = 0 \times \cdots \times 0 \times B_i \times 0 \times \cdots \times 0$), entonces es elemental ver que cada $\hat{B}_i$ es isomorfo a B_i y que $A = \hat{B}_1 \oplus \cdots \oplus \hat{B}_n$. Es decir, si A es el producto directo de los B_i, entonces A es la suma directa de los $\hat{B}_i$, que son isomorfos a los B_i.

En vista de esto, a partir de ahora identificaremos $B_1 \oplus \cdots \oplus B_n$ con $B_1 \times \cdots \times B_n$.

Ejemplo 7.6 *Extender la discusión anterior al caso de una familia infinita independiente de subgrupos, sustituyendo el producto directo por el grupo del último apartado de los Ejemplos 4.6.*

7.2 Grupos abelianos libres

Definición 7.7 *Sea* A *un grupo abeliano.*

Un subconjunto finito $\{a_1, \ldots, a_n\}$ *de* A *se dice que es* linealmente independiente *si la única solución, formada por números enteros* $x_1, \ldots, x_n$*, de la ecuación*

$$\sum_{i=1}^{n} x_i a_i = 0$$

es $x_1 = \cdots = x_n = 0$*. Un subconjunto de* A *se dice que es linealmente independiente si todo subconjunto finito suyo es linealmente independiente.*

Una base *de* A *es un sistema generador de* A *que es linealmente independiente. Diremos que* A *es un* grupo abeliano libre *si tiene una base.*

Ejemplo 7.8 *Demostrar que un subconjunto* X *de un grupo abeliano* A *es una base precisamente si cada elemento de* A *se puede expresar de forma única como combinación lineal con coeficientes enteros de los elementos de* X*. Es decir, si para cada* $a \in A$ *existe una única familia* $\{a_x : x \in X\}$ *de enteros, casi todos nulos, tal que* $a = \sum_{x \in X} a_x x$*.*

Ejemplos 7.9 *Grupos abelianos libres.*

(1) Sea n un número natural y sea $A = \mathbb{Z}^n$. Entonces el conjunto

$$e_1 = (1, 0, \ldots, 0), \quad e_2 = (0, 1, \ldots, 0), \quad \ldots \quad e_n = (0, 0, \ldots, 1)$$

es una base de A, llamada *base canónica*.

(2) En $A = \mathbb{Z}$, el conjunto $\{2, 3\}$ es un sistema generador minimal (en el sentido de que, si quitamos algún elemento, deja de ser sistema generador) que no es linealmente independiente. Por otra parte, el conjunto $\{2\}$ es un conjunto linealmente independiente maximal (en el sentido de que, en cuanto le añadamos un elemento, dejará de ser independiente) que no es generador.

Esto no ocurre con los espacios vectoriales: en un espacio vectorial, todo sistema generador minimal es una base (en el sentido de álgebra lineal) y todo conjunto linealmente independiente maximal es una base.

(3) Sea I un conjunto y consideremos el grupo $A = \mathbb{Z}^I = \{(a_i)_{i \in I} : a_i \in \mathbb{Z}\}$ con la suma componente a componente (a este grupo se le suele llamar el producto directo de $|I|$ copias de $\mathbb{Z}$). Para cada $i \in I$, sea $e_i = (\delta_{ij})_{j \in I}$, donde $\delta_{ij} = 0$ si $i \neq j$ y $\delta_{ii} = 1$ (este símbolo se conoce como *la delta de Kronecker*). Entonces $E = \{e_i : i \in I\}$ es un conjunto linealmente independiente de A. Sin embargo, E sólo es una base si I es finito. De hecho, el subgrupo generado por E es

$$\mathbb{Z}^{(I)} = \{(a_i)_{i \in I} \in \mathbb{Z}^I : a_i = 0 \text{ para casi todo } i \in I\}.$$

Luego $\mathbb{Z}^{(I)}$ es un grupo libre y E es una base suya llamada *base canónica*.

(4) Sea P el conjunto de los enteros primos positivos. Entonces la aplicación $f : \mathbb{Z}^{(P)} \to \mathbb{Q}^+$ dada por

$$f((n_p)_{p\in P}) = \prod_{p\in P} p^{n_p}$$

es un isomorfismo. Luego $\mathbb{Q}^+$ es libre con base P.

Ejemplo 7.10 *Demostrar que una familia $\{a_i : i \in I\}$ de elementos de un grupo A es linealmente independiente si y sólo si cada a_i tiene orden infinito y la familia $\{\langle a_i\rangle : i \in I\}$ de los subgrupos cíclicos generados por los a_i es independiente.*

En realidad, el apartado 3 del Ejemplo 7.9 agota, salvo isomorfismos, todos los posibles ejemplos de grupos libres, como muestra el siguiente ejercicio.

Ejemplo 7.11 *Sea X un subconjunto de un grupo abeliano A, y sea $f : \mathbb{Z}^{(X)} \to A$ la aplicación dada por $f((a_x)_{x\in X}) = \sum_{x\in X} a_x x$ (las sumas tienen sentido porque casi todos los sumandos son nulos). Demostrar:*

(1) f es un homomorfismo de grupos.

(2) f es inyectiva precisamente si X es linealmente independiente.

(3) f es suprayectiva precisamente si X es un conjunto generador de A.

(4) X es una base precisamente si f es un isomorfismo. En este caso $A \cong \mathbb{Z}^{(X)}$.

(5) A es libre precisamente si A es isomorfo a $\mathbb{Z}^{(I)}$ para cierto conjunto I.

Los conceptos de linealmente independiente, generador y base nos recuerdan a los correspondientes de álgebra lineal. En el siguiente ejercicio vemos algunas relaciones entre nuestro concepto y el de álgebra lineal.

Ejemplo 7.12 *Sea I un conjunto. Consideremos $A = \mathbb{Z}^{(I)}$ como un grupo abeliano libre y $V = \mathbb{Q}^{(I)}$ como un espacio vectorial sobre $\mathbb{Q}$. Demostrar las siguientes propiedades para un subconjunto S de A:*

(1) S es linealmente independiente como subconjunto del grupo A precisamente si S es linealmente independiente como subconjunto del espacio vectorial V.

(2) Si S es un sistema generador del grupo A, entonces S es un sistema generador del espacio vectorial V.

(3) Dar un ejemplo de un subconjunto de A que sea generador de V pero que no sea generador de A.

(4) Demostrar que todas las bases de A tienen el mismo cardinal, a saber $|I|$. Deducir que si J es otro conjunto, entonces $\mathbb{Z}^{(I)} \cong \mathbb{Z}^{(J)}$ precisamente si $|I| = |J|$.

Definición 7.13 *El cardinal de una base (cualquier base) de un grupo abeliano libre A se llama rango de A y se denota $r(A)$.*

De los Ejercicios 7.11 y 7.12 se deduce que el rango es un invariante que caracteriza los grupos abelianos libres salvo isomorfismos; es decir:

Proposición 7.14 *Si A y B son grupos abelianos libres, entonces $A \cong B$ si y sólo si $r(A) = r(B)$.*

Los grupos abelianos libres que más nos interesan son los finitamente generados. Obviamente, los grupos de la forma $\mathbb{Z}^n$ son grupos abelianos libres finitamente generados. De hecho no hay más, salvo isomorfismos, ya que si $\{a_1 = (a_{1i})_{i\in I}, \ldots, a_n = (a_{ni})_{i\in I}\}$ es un conjunto generador de $A = \mathbb{Z}^{(I)}$, entonces $F = \{i \in I : a_{ki} \neq 0 \text{ para algún } k = 1, \ldots, n\}$ es un subconjunto finito de I. Vamos a ver que $I = F$. Si $i \in I \setminus F$, entonces la coordenada i-ésima de todo elemento de la forma $\sum_{k=1}^{n} m_k a_k$ es 0. Como en $\mathbb{Z}^{(I)}$ hay elementos cuya coordenada i-ésima no es 0 (¡encuentra uno!), eso nos lleva a una contradicción, de donde deducimos que $I = F$ y, por tanto I es finito. Junto con la Proposición 7.14, esto demuestra que:

Corolario 7.15 *Todo grupo abeliano libre finitamente generado A es isomorfo a $\mathbb{Z}^n$, donde $n = r(A)$.*

Un grupo abeliano libre finitamente generado también se dice que es un grupo abeliano libre de *tipo finito* o de *rango finito*. Como consecuencia del Ejercicio 7.11 se deduce:

Proposición 7.16 *Sea A un grupo abeliano.*

(1) A es isomorfo a un cociente de un grupo abeliano libre.

(2) A es finitamente generado precisamente si es isomorfo a un cociente de un grupo abeliano libre de tipo finito.

(3) A es cíclico precisamente si es isomorfo a un cociente de $\mathbb{Z}$.

Demostración. Sea A un grupo abeliano, y sea I un conjunto generador de A (¿existe siempre?). Entonces la aplicación $f : \mathbb{Z}^{(I)} \to A$ del Ejercicio 7.11 es un epimorfismo. Por el Primer Teorema de Isomorfía se tiene $A \cong \mathbb{Z}^{(I)}/\text{Ker } f$, lo que demuestra la primera afirmación y la condición necesaria de las otras dos afirmaciones. Las condiciones suficientes son evidentes. ∎

Del isomorfismo evidente $\mathbb{Z}^n \times \mathbb{Z}^m \cong \mathbb{Z}^{n+m}$ se deduce:

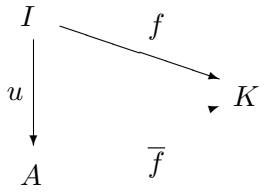
Proposición 7.17 *Si A y B son grupos abelianos libres de tipo finito entonces $A \times B$ es también libre, y se tiene $r(A \times B) = r(A) + r(B)$.*

El lector puede probar que el producto directo de un número finito de grupos libres (no necesariamente de tipo finito) es libre. No es cierto que el producto directo infinito de grupos libres sea libre. Por ejemplo, $\mathbb{Z}^{\mathbb{N}}$ no es libre, pero la demostración de este hecho excede los objetivos del curso.

Las bases de los grupos abelianos libres verifican una propiedad análoga a las bases de espacios vectoriales, en el sentido de que podemos describir homomorfismos que salgan de un grupo abeliano libre eligiendo arbitrariamente (en el grupo imagen) las imágenes de los elementos de la base. Explícitamente:

Proposición 7.18 (Propiedad Universal de las Bases) *Sea A un grupo abeliano libre y sea I una base de A. Si B es un grupo abeliano y $f : I \to B$ es una aplicación, entonces existe un único homomorfismo de grupos $\bar{f} : A \to B$ que extiende f (es decir, tal que $\bar{f}(i) = f(i)$ cuando $i \in I$).*

Obsérvese que, si $u : I \to A$ es la inclusión, entonces el homomorfismo $\bar{f}$ completa el siguiente diagrama



Demostración. Por el Ejercicio 7.11 existe un isomorfismo $g : A \to \mathbb{Z}^{(I)}$ tal que $g(i) = e_i$, donde $\{e_i : i \in I\}$ es la base canónica de $\mathbb{Z}^{(I)}$. Sea $\bar{f} : \mathbb{Z}^{(I)} \to B$ la aplicación dada por $\bar{f}((a_i)_{i\in I}) = \sum_{i\in I} a_i f(i)$. Por el Ejercicio 7.11, $\bar{f}$ es un homomorfismo de grupos y la composición $g \circ \bar{f} : A \to B$ satisface las condiciones requeridas. La unicidad es consecuencia del hecho obvio de que dos homomorfismos que toman los mismos valores en un conjunto generador son iguales. ∎

Lema 7.19 *Un subgrupo B de un grupo A es un sumando directo de A si y sólo si existe un homomorfismo $\rho : A \to B$ que es la identidad en B; es decir, tal que $\rho(b) = b$ para cada $b \in B$. Si tal ρ existe, entonces $A = B \oplus \operatorname{Ker} \rho$.*

Demostración. La condición necesaria es consecuencia del Ejercicio 7.5. Sea $\rho : A \to B$ un homomorfismo suprayectivo que es la identidad en B. Entonces $B \cap \operatorname{Ker} \rho = 0$ y, si $a \in A$, entonces $\rho(a - \rho(a)) = \rho(a) - \rho(a) = 0$ y

$$a = \rho(a) + a - \rho(a) \in B + \operatorname{Ker} \rho.$$

Luego $A = B \oplus \operatorname{Ker} \rho$. ∎

Corolario 7.20 *Sea $f : A \to L$ un homomorfismo suprayectivo de grupos abelianos. Si L es libre, entonces existe un subgrupo B de A isomorfo a L tal que $A = B \oplus \operatorname{Ker} f$.*

Demostración. Sea I una base de L y, para cada $i \in I$, sea $a_i \in A$ tal que $f(a_i) = i$. Por la Proposición 7.18, existe un único homomorfismo de grupos $g : L \to A$ tal que $g(i) = a_i$, para todo $i \in I$. Entonces $f \circ g = 1_L$ (¿por qué?); por tanto g es inyectiva y así $B = \text{Im } g \cong L$. Entonces, la composición $p = g \circ f : A \to B$ es la identidad sobre B, pues un elemento $b \in B$ es de la forma $b = g(x)$ con $x \in L$ y entonces

$$p(b) = p(g(x)) = g(f(g(x))) = g(1_L(x)) = g(x) = b.$$

Ahora el resultado es una consecuencia inmediata del Lema 7.19. ∎

Teorema 7.21 *Sea A un grupo abeliano libre de tipo finito y sea B un subgrupo de A. Entonces B es libre de tipo finito y $r(B) \leq r(A)$.*

Demostración. Sea $n = r(A)$. Por el Corolario 7.15, podemos suponer que $A = \mathbb{Z}^n$. Razonamos por inducción sobre n, con el caso $n = 1$ resuelto por el Corolario **??**. Supongamos pues que $n > 1$ y que se verifica el teorema para grupos abelianos libres de rango menor que n. Sea $e_1, \ldots, e_n$ la base canónica de A. Sean $A_1 = \langle e_1, \ldots, e_{n-1} \rangle$ y $B_1 = B \cap A_1$. Obviamente, A_1 es libre de rango $n-1$, y por la hipótesis de inducción B_1 es libre de rango $\leq n-1$. Sea $f : A \to \mathbb{Z}$ el homomorfismo dado por $f(x_1, \ldots, x_n) = x_n$, sea $C = f(B)$ y sea $g : B \to C$ la restricción de f a B. Entonces C es un grupo abeliano libre de rango ≤ 1 y Ker $g = B_1$. Del Corolario 7.20 se deduce que $B = B_1 \oplus C_1$, donde C_1 es un subgrupo de B isomorfo a C. Aplicando la Proposición 7.17 se deduce que B es libre de rango menor o igual que n. ∎

7.3 Grupos de torsión y libres de torsión

Definición 7.22 *Sea A un grupo abeliano.*

El subgrupo de torsión *de A es el conjunto $t(A)$ formado por los elementos de orden finito de A:*

$$t(A) = \{a \in A : \text{ existe } 0 \neq n \in \mathbb{Z} \text{ tal que } na = 0\}.$$

Se dice que A es un grupo de torsión *si $t(A) = A$. Es decir, si para cada $a \in A$ existe $0 \neq n \in \mathbb{Z}$ tal que $na = 0$.*

Se dice que A es un grupo libre de torsión *si $t(A) = 0$. Es decir, si para cada $0 \neq a \in A$, el único $n \in \mathbb{Z}$ tal que $na = 0$ es $n = 0$ (lo que equivale a que el conjunto $\{a\}$ sea linealmente independiente).*

Si un entero n verifica $na = 0$ para todo $a \in A$, escribiremos $nA = 0$. Si existe algún $n \geq 1$ con $nA = 0$, llamamos periodo *de A al menor entero positivo con esa propiedad. Si no existe tal entero positivo, decimos que A tiene periodo 0. Denotaremos con $p(A)$ al periodo de A.*

Dejamos que el lector compruebe algunas propiedades elementales de los conceptos recién definidos, y en particular las relaciones entre ellos.

Ejemplo 7.23 *Si A es un grupo abeliano, demostrar que:*

(1) El conjunto $t(A)$ es un subgrupo de A que es de torsión, y el grupo cociente $A/t(A)$ es libre de torsión.

(2) Si A es finito entonces $p(A) \neq 0$.

(3) Si $p(A) \neq 0$ entonces A es de torsión.

(4) Si A es libre entonces A es libre de torsión.

(5) Si A es libre de torsión y no trivial, entonces $p(A) = 0$.

(6) Si A es cíclico y $p(A) = n$ entonces $A \cong \mathbb{Z}_n$ (incluidos los casos $n = 0$ y $n = 1$).

(7) Si A es de torsión y B es un subgrupo de A entonces B y A/B también son de torsión.

(8) Si A es libre de torsión entonces cualquier subgrupo B es también libre de torsión; ¿lo es A/B?

(9) Si $A = B \oplus C$ entonces $t(A) = t(B) \oplus t(C)$.

(10) Si $p(A) = n \neq 0$ y $m \in \mathbb{Z}$ entonces $ma = 0$ para cada $a \in A$ si y sólo si $n \mid m$.

(11) Si $A = B_1 \oplus \cdots \oplus B_n$ entonces $p(A) = \operatorname{mcm}(p(B_1), \ldots, p(B_n))$.

(12) Si A es de torsión y $\{a_i : i \in I\}$ es un sistema generador entonces $p(A) = \operatorname{mcm}\{o(a_i) : i \in I\}$.

Ejemplos 7.24 *Torsiones y periodos.*

(1) El grupo $A = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$ (producto numerable de copias de $\mathbb{Z}_2$) tiene periodo 2. Esto nos da un contraejemplo para el recíproco del apartado 2.

(2) El grupo $\mathbb{Q}/\mathbb{Z}$ es de torsión, pues cada $\frac{a}{b} + \mathbb{Z}$ es anulado por $b \neq 0$. Además este grupo tiene periodo 0, pues dado $n \neq 0$ en $\mathbb{Z}$ se tiene $n(\frac{1}{p} + \mathbb{Z}) \neq 0$, donde p es cualquier primo que no divide a n. Esto nos da un contraejemplo para los recíprocos de los apartados 3 y 5.

(3) Existen grupos abelianos libres de torsión que no son libres; por ejemplo $\mathbb{Q}$ (cualquier subconjunto linealmente independiente tiene un solo elemento, y por tanto no es un sistema generador). Esto nos da un contraejemplo para el recíproco del apartado 4.

(4) Existen grupos abelianos que no son de torsión ni libres de torsión; por ejemplo, $\mathbb{Q}^*$, $\mathbb{R}^*$ ó $\mathbb{C}^*$.

(5) Si $A = \mathbb{Z} \times \mathbb{Z}_n$, con $n > 0$, entonces $t(A) = 0 \times \mathbb{Z}_n$.

(6) Si $A = \prod_p \mathbb{Z}_p$, donde p recorre el conjunto de los enteros positivos primos, entonces $t(A) = \oplus_p \mathbb{Z}_p$. Este subgrupo $t(A)$ es otro ejemplo de grupo de torsión con periodo 0.

(7) Sea $z \in \mathbb{C}^*$. Si $r = |z|$ entonces se tiene $z = re^{\alpha i} = r(\cos\alpha + i \operatorname{sen}\alpha)$, donde α es el argumento de z. Entonces $z^n = r^n e^{n\alpha i}$, con lo que $z^n = 1$ precisamente si $r = 1$ y $n\alpha = 2k\pi$ para algún $k \in \mathbb{Z}$. Por tanto

$$t(C^*) = \{e^{2\pi q i} : q \in \mathbb{Q},\ 0 \leq q < 1\}.$$

O sea, $t(C^*)$ está formado por los vértices de los polígonos regulares centrados en el origen con un vértice en el punto 1 (el lector puede representar gráficamente, por ejemplo, todos los elementos de orden ≤ 10.) Obsérvese que la aplicación $f : \mathbb{Q} \to \mathbb{C}^*$ dada por $f(q) = e^{2\pi q i}$ es un homomorfismo de grupos tal que $t(C^*) = \operatorname{Im} f$ y $\operatorname{Ker} f = \mathbb{Z}$, con lo que $t(C^*) \cong \mathbb{Q}/\mathbb{Z}$.

Los siguientes tres resultados nos dicen que, para grupos abelianos finitamente generados, todo lo relativo a la torsión se simplifica: Ser de torsión equivale a ser finito, ser libre de torsión equivale a ser libre y el subgrupo de torsión es un sumando directo[1].

Proposición 7.25 *Las condiciones siguientes son equivalentes para un grupo abeliano finitamente generado A:*

(1) A es finito.

(2) $p(A) \neq 0$.

(3) A es de torsión.

Demostración. Por el Ejercicio 7.23, basta ver que 3 implica 1. Supongamos pues que A es de torsión, con un sistema generador $\{a_1, \ldots, a_k\}$, y sea $n_i = o(a_i) < \infty$. Obviamente, la familia de los elementos de A de la forma $r_1a_1 + \cdots + r_ka_k$ con $0 \leq r_i < n_i$ para cada $i = 1, \ldots, k$, es finita (tal vez incluso se repitan elementos), y las condiciones implican que cada elemento de A es uno de esos, luego A es un conjunto finito. ∎

Teorema 7.26 *Un grupo abeliano finitamente generado es libre de torsión precisamente si es libre.*

Demostración. Todo grupo libre es libre de torsión, por el Ejercicio 7.23. Sea A un grupo abeliano finitamente generado y libre de torsión. Sea $X = \{a_1, \ldots, a_n\}$ un conjunto de generadores de A. Entre todos los subconjuntos de X que sean linealmente independientes elegimos uno maximal Y; podemos suponer, reordenando los a_i si es necesario, que $Y = \{a_1, \ldots, a_k\}$. Sea $L = \langle Y \rangle$, que claramente es libre.

Sea $i \in \{k+1, k+2, \ldots, n\}$. Por la maximalidad de Y, el conjunto $\{a_1, \ldots, a_k, a_i\}$ es linealmente dependiente, luego hay una relación

$$t_{i1}a_1 + \cdots + t_{ik}a_k + t_ia_i = 0$$

[1]Existen grupos abelianos A tales que $t(A)$ no es un sumando directo de A. Un ejemplo de esta situación es el grupo $\prod_p \mathbb{Z}_p$ del apartado 6 de los Ejemplos 7.24, pero no es sencillo comprobar esta propiedad.

donde los coeficientes son enteros, no todos nulos. Como Y es linealmente independiente, se tiene $t_i \neq 0$. Sea $t = t_{k+1} \cdots t_n$. Entonces cada $ta_i \in L$ y la aplicación $a \mapsto ta$ es un homomorfismo de grupos $f : A \to L$. Como A es libre de torsión y $t \neq 0$, la aplicación f es inyectiva y, por tanto A es isomorfo a un subgrupo de L. Del Teorema 7.21 se deduce que A es libre. ∎

Corolario 7.27 *Sea A un grupo abeliano finitamente generado. Entonces $A = t(A) \oplus L$ para un subgrupo abeliano libre L de A. Además $t(A)$ es finito y L es isomorfo a $A/t(A)$, y por tanto L es único salvo isomorfismos.*

Demostración. $A/t(A)$ es libre de torsión por el Ejercicio 7.23, y es finitamente generado por serlo A, luego es libre por el Teorema 7.26. Sea $\pi : A \to A/t(A)$ la proyección canónica. De la Proposición 7.20 se deduce que $A = t(A) \oplus L$, donde L es un subgrupo de A isomorfo a $A/t(A)$, luego L es un grupo abeliano libre. Además $t(A)$ es finitamente generado (es isomorfo al cociente A/L por el Ejercicio 7.5) y de torsión, luego es finito (Proposición 7.25). ∎

Ejemplos 7.28 *La torsión como sumando directo.*

(1) Si $A = \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}_6\times\mathbb{Z}_{36}$, entonces$t(A) = 0\times0\times\mathbb{Z}_6\times\mathbb{Z}_{36}$, y podemos tomar $L = \mathbb{Z}\times\mathbb{Z}\times0\times0$.

(2) Ya hemos visto que $\mathbb{R}^* = \langle -1\rangle \oplus \mathbb{R}^+$, y es claro que $\langle -1\rangle = t(\mathbb{R}^*)$.

(3) Sea G el subgrupo de $\mathbb{C}^*$ generado por $\{2, i\}$. Por los Ejemplos 7.24, si $z = 2^n i^m \in t(G)$ (con $n, m \in \mathbb{Z}$), entonces $1 = |z| = 2^n$, lo que implica que $n = 0$. O sea $t(G) = \langle i\rangle$. Como $\langle 2\rangle$ es libre de torsión, $G = \langle 2\rangle \oplus \langle i\rangle$ es la descomposición del Corolario 7.27.

(4) Sea R un anillo. En el anillo cociente $R[X]/(X^2)$, es claro que cada elemento tiene un único representante de la forma $r+sX$ con $r, s \in R$. Dados $r+sX+(X^2)$ y $r'+s'X+(X^2)$ en $R[X]/(X^2)$, se tiene

$$[r + sX + (X^2)] + [r' + s'X + (X^2)] = (r + r') + (s + s')X + (X^2)$$

y

$$[r + sX + (X^2)] \cdot [r' + s'X + (X^2)] = (rr') + (rs' + r's)X + (X^2).$$

Por tanto, podemos identificar $R[X]/(X^2)$ con el anillo cuyo grupo abeliano subyacente es $R \times R$ y en el que el producto viene dado por

$$(r, s) \cdot (r', s') = (rr', rs' + r's).$$

El elemento identidad de este anillo es $(1, 0)$.

Si (r, s) es invertible en este anillo, es claro que $r \in R^*$. Recíprocamente, si $r \in R^*$ entonces $(r^{-1}, -sr^{-2})$ es el inverso de (r, s) en este anillo. En consecuencia, el grupo multiplicativo de sus unidades, que denotaremos con $R^* \propto R$, es el conjunto $R^* \times R$ con el producto definido en el párrafo anterior.

Vamos a determinar el orden de un elemento $(r,s) \in R^* \propto R$. Si $n \in \mathbb{Z}^+$, es fácil ver (bien por inducción o bien considerando la fórmula del binomio de Newton en $R[X]/(X^2)$) que

$$(r,s)^n = (r^n, nr^{n-1}s).$$

Como r es invertible en R, se tiene $(r,s)^n = (1,0)$ precisamente si $r^n = 1$ y $ns = 0$. Por tanto, (r,s) tiene orden finito en $R^* \propto R$ precisamente si r tiene orden finito en $(R^*, \cdot)$ y s tiene orden finito en $(R, +)$. Es decir, $t(R^* \propto R) = t(R^*) \times t(R)$. Además, si $(r,s) \in t(R^* \propto R)$ entonces

$$o(r,s) = \text{mcm}(o_m(r), o_a(s)),$$

donde $o_m(r)$ es el orden de r en el grupo multiplicativo R^* y $o_a(s)$ es el orden de s en el grupo aditivo R.

Pasemos a un caso concreto: Sea $A = \mathbb{Z}^* \propto \mathbb{Z}$ (recuérdese que $\mathbb{Z}^* = \{1, -1\}$). Por el párrafo anterior se tiene $t(A) = \{(1,0), (-1,0)\}$. Por otra parte, $L = \langle (1,1) \rangle$ es un subgrupo libre de A, y el lector puede ahora comprobar que se tiene $A = t(A) \oplus L$.

Por el Teorema 7.21, todo subgrupo B de un grupo abeliano libre A es libre y $r(B) \leq r(A)$. Los resultados anteriores nos permiten determinar cuándo se da la igualdad entre los rangos.

Proposición 7.29 *Sea A un grupo abeliano libre finitamente generado y B un subgrupo de A. Entonces $r(A) = r(B)$ precisamente si A/B es un grupo finito.*

Demostración. Como A es finitamente generado, lo es también A/B, así que A/B es finito si y sólo si es de torsión (Proposición 7.25). Se trata pues de ver que A/B es de torsión si y sólo si $r(B) = r(A)$. Sean $n = r(A)$ (por lo que podemos asumir que $A = \mathbb{Z}^n$) y $k = r(B)$, y fijemos una base $b_1, \ldots, b_k$ de B. Es fácil ver que, para un elemento $a \in A$, el elemento $a + B \in A/B$ tiene orden infinito si y sólo si los elementos $b_1, \ldots, b_k, a$ son linealmente independientes en A. Podemos ya demostrar la equivalencia:

Si A/B no es de torsión, existe un elemento $a+B$ en A/B de orden infinito, luego $b_1, \ldots, b_k, a$ son linealmente independientes en A y así $k < k+1 \leq n$. Y si $k < n$ y vemos a $A = \mathbb{Z}^n$ dentro del espacio vectorial racional $V = \mathbb{Q}^n$, entonces existe $\alpha \in V$ tal que $b_1, \ldots, b_k, \alpha$ son linealmente independientes en V, y además existe un entero no nulo t tal que $a = t\alpha \in A$. Como $t \neq 0$, los elementos $b_1, \ldots, b_k, a$ son linealmente independientes en V y, por el Ejercicio 7.12, también lo son en A, por lo que $a + B$ tiene orden infinito y así A/B no es de torsión. ∎

7.4 Grupos indescomponibles y p-grupos

Como hemos comentado en la introducción del capítulo, nuestro objetivo es descomponer un grupo abeliano finitamente generado A como suma directa de subgrupos con algunas propiedades especiales. Con las herramientas desarrolladas en las secciones anteriores, en ésta veremos primero que A es suma directa de subgrupos que no pueden descomponerse más (indescomponibles), y a continuación demostraremos que estos subgrupos indescomponibles son cíclicos, de lo que deduciremos que A es suma directa de subgrupos cíclicos. Comenzamos definiendo con precisión los grupos indescomponibles.

Definición 7.30 *Un grupo abeliano no nulo se dice que es* indescomponible *si no es suma directa de dos subgrupos propios. Es decir A es indescomponible si $A = X \oplus Y$ implica $X = 0$ ó $Y = 0$ (y por tanto $X = A$ ó $Y = A$).*

Ejemplos 7.31 *Grupos Indescomponibles.*

(1) $\mathbb{Z}$ y $\mathbb{Q}$ son indescomponibles, por un argumento usado en los Ejemplos 7.4.

(2) Por el Corolario 7.15 y el Teorema 7.26, $\mathbb{Z}$ es, salvo isomorfismos, el único grupo abeliano libre de torsión y finitamente generado que es indescomponible.

(3) Si p es un número primo entonces $\mathbb{Z}_p$ es indescomponible, pues no tiene subgrupos propios no triviales. De hecho, $\mathbb{Z}_{p^n}$ es indescomponible para cada $n \geq 1$. En efecto, por el Teorema de la Correspondencia, los subgrupos de $\mathbb{Z}_{p^n}$ forman una cadena (Ejemplos 5.5), y es claro que cualquier grupo cuyos subgrupos estén linealmente ordenados es indescomponible.

(4) Sean $n, m \geq 2$ dos enteros coprimos; por el Teorema Chino de los Restos se tiene $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$, por lo que $\mathbb{Z}_{nm}$ no es indescomponible (recuérdese la relación entre entre suma directa y producto directo descrita al final de la Sección 7.1). En consecuencia, los grupos cíclicos finitos indescomponibles son exactamente aquellos cuyo orden es p^r para cierto primo p y cierto entero $r \geq 1$.

Como consecuencia inmediata del Corolario 7.27 se obtiene:

Corolario 7.32 *Un grupo abeliano finitamente generado indescomponible es de torsión (y por tanto finito) o libre de torsión.*

Proposición 7.33 *Todo grupo abeliano finitamente generado y no nulo A es una suma directa de subgrupos indescomponibles.*

Demostración. Por el Corolario 7.27, y teniendo en cuenta que los grupos abelianos libres de rango finito son sumas directas de copias de $\mathbb{Z}$ (Teorema 7.26) y que los grupos abelianos finitamente generados de torsión son finitos (Proposición 7.25), basta demostrar la afirmación para grupos abelianos finitos. Sea A un grupo abeliano finito. Razonamos por inducción en $|A|$, con el caso $|A| = 2$ trivial. Si A es indescomponible no hay nada que demostrar. En caso contrario $A = B \oplus C$ y los cardinales de B y C son estrictamente menores que el de A. Por hipótesis de inducción, B y C son sumas directas de grupos indescomponibles, y "pegando" las descomposiciones de B y C como en el Ejercicio 7.5 obtenemos una descomposición de A como suma directa de grupos indescomponibles. ∎

En los Ejemplos 7.31 han aparecido dos tipos de grupos finitamente generados e indescomponibles: $\mathbb{Z}$ y los cíclicos de orden p^n ($\mathbb{Q}$ no es finitamente generado por el Problema **??** del Capítulo 4). El resto de esta sección lo dedicaremos a ver que, salvo isomorfismos, no hay otros. Para ello, será importante considerar ciertos grupos que comparten una característica con $\mathbb{Z}_{p^n}$, y que definimos a continuación:

Lema 7.34 *Dados un grupo abeliano finito A y un entero positivo primo p, las siguientes condiciones son equivalentes:*

(1) El orden de A es una potencia de p.

(2) El orden de cada elemento de A es una potencia de p.

Demostración. Si $|A| = p^n$ entonces cada $a \in A$ tiene orden p^m con $m \leq n$ por el Teorema de Lagrange. Demostraremos el recíproco por inducción en el orden $|A|$, con el caso $|A| = 1$ trivial. Si $|A| > 1$ entonces existe $0 \neq b \in A$, y si ponemos $B = \langle b \rangle$ entonces tenemos $|B| = o(b) = p^m$ para cierto $m \geq 1$. El grupo cociente A/B tiene cardinal menor que $|A|$, y es elemental ver que el orden de todos sus elementos es una potencia de p. Por la hipótesis de inducción se tiene $|A/B| = p^n$ para cierto $n \geq 0$, y en consecuencia $|A| = |B| \cdot |A/B| = p^{m+n}$, como queríamos ver. ∎

Definición 7.35 *Un grupo abeliano finito que verifique las condiciones equivalentes del Lema 7.34 se llama un* p-grupo.

Esta definición la extenderemos a grupos no abelianos en la Definición **??**.

Como en la definición no se excluyen las potencias de exponente 0, el grupo trivial es un p-grupo para cualquier primo p. Un ejemplo más sofisticado es $\mathbb{Z}_{25} \times \mathbb{Z}_{625} \times \mathbb{Z}_{625}$, que es un 5-grupo.

Definición 7.36 *Dados un grupo abeliano A y un entero primo p, el* subgrupo de p-torsión *de A es*

$$t_p(A) = \{a \in A : \text{ existe } n \in \mathbb{N} \text{ tal que } p^n a = 0\} = \{a \in A : o(a) \text{ es una potencia de } p\}.$$

Dejamos que el lector compruebe que ambos conjuntos son iguales y que forman un subgrupo de A. De hecho, si A es finito, $t_p(A)$ es claramente el mayor *p-subgrupo* de A (es decir, el mayor subgrupo de A que es un p-grupo).

Proposición 7.37 *Sea A un grupo abeliano finito y sean $p_1, \ldots, p_k$ los divisores primos de $|A|$. Entonces*

$$A = t_{p_1}(A) \oplus \cdots \oplus t_{p_k}(A),$$

con cada $t_{p_i}(A) \neq 0$.

Demostración. Sea $a \in A$ y sea $o(a) = n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (¿por qué no pueden aparecer otros primos en la factorización de n?). Para cada $i = 1, \ldots, k$ sea $q_i = n/p_i^{\alpha_i}$. Es claro que ningún primo divide a la vez a todos los q_i, por lo que $\text{mcd}(q_1, \ldots, q_k) = 1$ y por tanto existen $m_1, \ldots, m_k \in \mathbb{Z}$ tales que $m_1 q_1 + \cdots + m_k q_k = 1$. Como $p_i^{\alpha_i} q_i a = 0$, se tiene $q_i a \in t_{p_i}(A)$, luego

$$a = m_1 q_1 a + \cdots + m_k q_k a \in t_{p_1}(A) + \cdots + t_{p_k}(A).$$

En consecuencia, $A = t_{p_1}(A) + \cdots + t_{p_k}(A)$.

Para ver que la suma es directa, supongamos que $a_1 + \cdots + a_k = 0$ con cada $a_i \in t_{p_i}(A)$. Por tanto, para cada $i = 1, \ldots, k$, existe β_i tal que $p_i^{\beta_i} a_i = 0$. Sea $m = p_1^{\beta_1} \cdots p_k^{\beta_k}$. Para cada índice i ponemos $t_i = m/p_i^{\beta_i}$, de modo que $t_i a_j = 0$ cuando $i \neq j$, y así

$$t_i a_i = -t_i \sum_{j \neq i} a_j = 0.$$

Entonces $o(a_i)$ divide a t_i y a $p_i^{\beta_i}$, y como éstos son coprimos, se tiene $o(a_i) = 1$ y por tanto $a_i = 0$. Esto prueba que la familia es independiente.

Por último, de la igualdad $A = t_{p_1}(A) \oplus \cdots \oplus t_{p_k}(A)$ se deduce que $|A| = |t_{p_1}(A)| \cdots |t_{p_k}(A)|$. Como el orden de cada $t_{p_i}(A)$ es una potencia de p_i (Lema 7.34) y cada p_i divide a $|A|$, deducimos que ese orden es mayor que 1 y por tanto $t_{p_i}(A) \neq 0$. ∎

El siguiente corolario es inmediato:

Corolario 7.38 *Un grupo finito e indescomponible es un p-grupo para cierto primo p.*

Ejemplos 7.39 *Descomposición en suma directa de p-grupos*

(1) Sea $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ una factorización prima irredundante del entero n. Por el Teorema Chino de los Restos, $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$ y claramente los factores de esta descomposición van a corresponder con los factores $t_p(\mathbb{Z}_n)$ de la descomposición de la Proposición 7.37. Más concretamente, si $q_i = n/p_i^{\alpha_i}$ para cada $i = 1, \ldots, k$, entonces $\overline{q_i} = q_i + n\mathbb{Z}$ genera un grupo de orden $p_i^{\alpha_i}$, y por tanto $t_{p_i}(\mathbb{Z}_n) = \langle \overline{q_i} \rangle$.

(2) Sea $A = \mathbb{Z}_{12}^* \propto \mathbb{Z}_{12}$ (véanse los Ejemplos 7.28 para la definición de este grupo). Como $|\mathbb{Z}_{12}^*| = 4$ y $|\mathbb{Z}_{12}| = 12$, se tiene $|A| = 48 = 2^4 \cdot 3$. Usando la descripción del orden de cada elemento que se dio en los Ejemplos 7.28, se tiene

$$t_3(A) = \{(1, b) : b = 0, 4, 8\} \qquad \text{y} \qquad t_2(A) = \{(a, b) : b = 0, 3, 6, 9\}$$

(donde identificamos cada entero con su clase módulo 12).

Sea B un subgrupo del grupo abeliano A, y sea $a \in A$. Si $na = 0$ (con $n \in \mathbb{N}$), entonces, en A/B, se tiene $n(a + B) = 0$. Eso implica que el orden de $a + B$ divide al orden de a. En general estos órdenes no coinciden; por ejemplo, no lo hacen si a es un elemento no nulo de B. Se dice entonces que a "baja de orden" en el cociente A/B. El siguiente lema muestra que, en algunas clases laterales, podemos elegir un representante que no baja el orden.

Lema 7.40 *Sean A un p-grupo finito. Entonces:*

(1) Existe $a \in A$ tal que $o(a) = p(A)$.

(2) Si $B = \langle a \rangle$ (donde a es el del apartado anterior) entonces todo elemento del cociente A/B tiene un representante que no baja de orden. Es decir, para todo $\gamma \in A/B$ existe $x \in A$ tal que $x + B = \gamma$ y $o(x) = o(\gamma)$.

Demostración. El primer apartado se tiene porque el periodo de un grupo abeliano es el mínimo común múltiplo de los ordenes de sus elementos (Ejercicio 7.23).

Para el segundo, comenzaremos eligiendo un representante cualquiera de γ, y veremos que podemos sustituirlo por otro con la propiedad requerida. Sea pues $y \in A$ tal que $y + B = \gamma$. Supongamos que $o(a) = p(A) = p^m$, $o(y) = p^s$ y $o(\gamma) = p^k$. Por el párrafo anterior al lema, se tiene $k \leq s \leq m$. Si $k = s$, tomamos $x = y$ y hemos terminado. Supongamos pues que $k < s$. Como $p^k(y + B) = p^k\gamma = 0$, se tiene que $p^k y \in B = \langle a \rangle$; es decir, $p^k y = qa$, para algún $q \in \mathbb{Z}$. Dividiendo q por la mayor potencia posible de p, podemos poner $q = rp^t$ con $\mathrm{mcd}(p, r) = 1$. Entonces

$$p^{m+k-t}y = p^{m-t}p^k y = p^{m-t}qa = rp^m a = 0$$

y, por tanto, $s \leq m + k - t$. Por otro lado,

$$p^{m+k-t-1}y = p^{m-t-1}qa = rp^{m-1}a \neq 0,$$

de donde se deduce que $s = m+k-t$. Sea ahora $x = y - rp^{m-s}a$; entonces $x + B = y + B = \gamma$, y por tanto $o(\gamma) = p^k$ divide a $o(x)$. Pero además, $p^k x = p^k y - rp^{m+k-s}a = p^k y - rp^t a = 0$, de donde se deduce que $o(x) = p^k = o(\gamma)$, como queríamos ver. ∎

Ahora podemos caracterizar los grupos abelianos finitamente generados que son indescomponibles.

Proposición 7.41 *Las siguientes condiciones son equivalentes para un grupo abeliano finitamente generado A:*

(1) A es indescomponible.

(2) A es isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}_{p^n}$ con p primo y $n \in \mathbb{Z}^+$.

Demostración. Ya hemos observado (Ejemplos 7.31) que los grupos del apartado 2 son indescomponibles. Supongamos pues que A es indescomponible y veamos que es isomorfo a uno de ellos.

Por el Corolario 7.32, A es libre de torsión o de torsión. En el primer caso A es isomorfo a $\mathbb{Z}$ por el Teorema 7.26 y el Corolario 7.15. Supongamos pues que A es de torsión, por lo que debe ser un p-grupo finito (Proposición 7.25 y Corolario 7.38) y en consecuencia $|A| = p^n$ para cierto $n \geq 1$. Sólo falta demostrar que A es cíclico, cosa que vamos a hacer por inducción sobre n.

El caso $n = 1$ lo resuelve el Teorema **??**. En el caso general, por el Lema 7.40, A contiene un elemento a cuyo orden coincide con el periodo de A. Sean $B = \langle a \rangle$ y $C = A/B$. Por la Proposición 7.33 se tiene $C = C_1 \oplus \cdots \oplus C_k$ para ciertos $C_1, \ldots, C_k$ indescomponibles. Por hipótesis de inducción, cada C_i es cíclico. Es decir, existen $x_1, \ldots, x_k \in A$ tales que $C_i = \langle x_i + B \rangle$ para cada i, y por el Lema 7.40 podemos suponer que $o(x_i) = o(x_i + B)$ para cada i. Claramente $A = B + \langle x_1 \rangle + \langle x_2 \rangle + \cdots + \langle x_k \rangle$. Vamos a ver que esta suma es directa. Sean $b \in B$ y $m_1, \ldots, m_k \in \mathbb{Z}$ tales que $b + m_1 x_1 + \cdots + m_k x_k = 0$. Entonces $0 = m_1(x_1 + B) + \cdots + m_k(x_k + B)$ y, por tanto, cada $m_i(x_i + B) = 0$. De aquí se deduce que m_i es múltiplo de $o(x_i + B) = o(x_i)$ y por tanto $m_i x_i = 0$ y $b = 0$. Como A es indescomponible y $B \neq 0$, deducimos que $A = B = \langle a \rangle$ es cíclico. ∎

Combinando las Proposiciones 7.33 y 7.41 se obtiene:

Corolario 7.42 *Todo grupo abeliano finitamente generado es suma directa de subgrupos cíclicos (y los que sean finitos se pueden tomar de manera que su orden sea potencia de primo).*

7.5 Descomposiciones primarias e invariantes

El Corolario 7.42 va a ser fundamental para clasificar los grupos abelianos finitamente generados salvo isomorfismos. La idea es que cada clase de isomorfía de grupos abelianos finitamente generados estará dada por una lista de números que van a representar los cardinales de los factores que aparecen en una descomposición de cualquiera de los elementos de la clase como suma directa de grupos cíclicos. Vamos a elegir dos tipos de listas de números: En la primera los números que admitimos son potencias de primos y 0; en la segunda los números van a ser números naturales arbitrarios pero con la exigencia de que cada uno de ellos divida a los anteriores.

Definición 7.43 *Sea A un grupo abeliano finitamente generado. Una* descomposición primaria *o* indescomponible *de A es una expresión de A como suma directa de subgrupos indescomponibles. Como cada uno de estos sumandos es isomorfo a $\mathbb{Z}$ ó a $\mathbb{Z}_{p^n}$, con p primo y $n \geq 1$, siempre podemos reordenarlos de modo que se tenga*

$$\begin{aligned} A &= (\oplus_{j=1}^{n} A_j) \oplus (\oplus_{j=1}^{m_1} A_{1j}) \oplus \cdots \oplus (\oplus_{j=1}^{m_k} A_{kj}) \\ &= A_1 \oplus A_2 \oplus \cdots \oplus A_n \oplus \\ &\quad A_{11} \oplus A_{12} \oplus \cdots \oplus A_{1m_1} \oplus \\ &\quad \cdots \\ &\quad A_{k1} \oplus A_{k2} \oplus \cdots \oplus A_{km_k} \end{aligned}$$

con $p(A_i) = 0$ (es decir, A_i es cíclico infinito) y $p(A_{ij}) = p_i^{\alpha_{ij}}$ para ciertos enteros primos positivos $p_1 < p_2 < \cdots < p_k$ y ciertos enteros positivos α_{ij} con $\alpha_{i1} \geq \alpha_{i2} \geq \cdots \geq \alpha_{im_i} \geq 1$ para cada $i = 1, \ldots, k$.

Con esta terminología, la Proposición 7.33 se reenuncia como:

Teorema 7.44 *Todo grupo abeliano finitamente generado tiene una descomposición primaria.*

Para obtener una descomposición primaria de un grupo abeliano finitamente generado seguimos los pasos indicados en la sección anterior; es decir, dado un grupo abeliano finitamente generado A:

(1) Se calcula $T = t(A)$ y un subgrupo libre de torsión L de A tal que $A = T \oplus L$ (Proposición 7.27).

(2) Se busca una base $b_1, \ldots, b_n$ de L y por tanto se tiene $L = \langle b_1 \rangle \oplus \cdots \oplus \langle b_n \rangle \cong \mathbb{Z}^n$. Esta es la "primera fila" en la ordenación de los sumandos que se propone en la Definición 7.43.

(3) Se calcula $t_p(T)$ para cada divisor primo de $|T|$; entonces $T = t_{p_1}(T) \oplus \cdots \oplus t_{p_k}(T)$ (Proposición 7.37).

(4) Para cada divisor primo p de $|T|$ se calcula $a \in t_p(T)$ tal que $o(a)$ coincida con el periodo de $t_p(T)$ (Proposición 7.40) y pasamos a estudiar $t_p(T)/\langle a\rangle$, que tiene orden menor que el de $t_p(T)$. Por recurrencia vamos pasando a grupos de orden cada vez más pequeño hasta obtener un grupo cíclico. Volvemos para atrás siguiendo la demostración de la Proposición 7.41 y así obtendremos una descomposición primaria de $t_p(T)$, que ocupará una fila en la ordenación de los sumandos según la Definición 7.43.

Ejemplos 7.45 *Descomposiciones primarias.*

(1) Sea $A = \langle 2, i\rangle$ el grupo del Ejemplo 7.28. Ya vimos que $t(A) = \langle i\rangle$ y $A = \langle i\rangle \oplus \langle 2\rangle$. Como $\langle i\rangle$ es cíclico de orden 4, hemos obtenido una descomposición primaria de A.

(2) Sea $A = \mathbb{Z}^* \propto \mathbb{Z}$. Vimos que $t(A) = \langle(-1, 0)\rangle$ y $A = \langle(-1, 0)\rangle \oplus \langle(1, 1)\rangle$. Como $\langle(-1, 0)\rangle$ es cíclico de orden 2, la anterior es una descomposición primaria de A.

(3) Sea $A = \mathbb{Z}_{12}^* \propto \mathbb{Z}_{12}$. Como este grupo es finito, no hay que dar los dos primeros pasos, y el tercero lo habíamos dado en el Ejemplo 7.39. Claramente $t_3(A) = \{(1, b) : b = 0, 4, 8\}$ es cíclico de orden 3, generado por $(1, 4)$. Sin embargo $t_2(A) = \{(a, b) : b = 0, 3, 6, 9\}$ no es cíclico ya que su cardinal es 16 y su periodo 4. Un elemento de orden 4 es $(1, 3)$. Pongamos

$$B = \langle(1, 3)\rangle = \{(1, 0), (1, 3), (1, 6), (1, 9)\}$$

y $C = A/B$, que tiene orden 4. Obsérvese que $x^2 \in B$ para todo $x \in t_2(A)$. Por tanto $C \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, de donde se deduce que si C_1 y C_2 son dos subgrupos C de orden 2 y distintos, entonces $C = C_1 \oplus C_2$ es una descomposición primaria de C. Uno de estos subgrupos puede ser $\langle(-1, 3)B\rangle$ (notación multiplicativa), pero como $(-1, 3)$ no tiene orden 2 en A, es necesario cambiarlo, como hicimos en la demostración del Lema 7.40, por otro elemento de la misma clase módulo B que no baje el orden, por ejemplo $(-1, 3)(1, 3) = (-1, 0)$ está en $(-1, 3)B$ y tiene orden 2. El otro subgrupo puede ser $\langle(5, 0)B\rangle$, de donde se obtiene que $C = \langle(-1, 0)B\rangle \oplus \langle(5, 0)B\rangle$ y, por tanto,

$$t_2(A) = \langle(1, 3)\rangle \oplus \langle(-1, 0)\rangle \oplus \langle(5, 0)\rangle.$$

Uniendo toda la información obtenemos

$$A = \langle(1, 3)\rangle \oplus \langle(-1, 0)\rangle \oplus \langle(5, 0)\rangle \oplus \langle(1, 4)\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Definición 7.46 *Sea A un grupo abeliano finitamente generado. Una* descomposición invariante *de A es una expresión del tipo*

$$A = \oplus_{i=1}^{n} A_i,$$

donde cada A_i es un grupo cíclico no trivial y se verifica $p(A_i) \mid p(A_{i-1})$ para cada $i = 2, \ldots, n$.

Ejemplo 7.47 *Demostrar que, si $A = \oplus_{i=1}^{n} C_i$ es una descomposición invariante A y el subíndice k es tal que $p(C_k) = 0 \neq p(C_{k+1})$, entonces el subgrupo de torsión de A es $t(A) = \oplus_{i=k+1}^{n} C_i$.*

Utilizando el Teorema 7.44 podemos obtener también:

Teorema 7.48 *Todo grupo abeliano finitamente generado tiene una descomposición invariante.*

Demostración. Sea A un grupo abeliano finitamente generado. Añadiendo sumandos triviales a una descomposición primaria suya, tenemos

$$\begin{aligned} A &= A_1 \oplus A_2 \oplus \cdots \oplus A_n \oplus \\ &\quad A_{11} \oplus A_{12} \oplus \cdots \oplus A_{1m} \oplus \\ &\quad \cdots \\ &\quad A_{k1} \oplus A_{k2} \oplus \cdots \oplus A_{km}, \end{aligned}$$

donde cada sumando es cíclico y se tiene $p(A_i) = 0$ y $p(A_{ij}) = p_i^{\alpha_{ij}}$, para ciertos primos positivos distintos $p_1, p_2, \ldots, p_k$ y ciertos enteros α_{ij} tales que, para cada i,

$$\alpha_{11} \geq \alpha_{12} \geq \ldots \geq \alpha_{1m} \geq 0. \tag{7.1}$$

Los α_{ij} que valen cero se corresponden con los sumandos triviales que hemos añadido para que, en cada fila de la descomposición de A, a partir de la segunda, haya el mismo número de sumandos.

Para obtener la descomposición primaria basta con "agrupar los sumandos por columnas", a partir de la segunda fila. Explícitamente, para cada $j = 1, \ldots, m$, sea

$$B_j = A_{1j} \oplus A_{2j} \oplus \cdots \oplus A_{kj}.$$

Entonces

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_n \oplus B_1 \oplus B_2 \oplus \cdots \oplus B_m$$

y, por el Teorema Chino de los Restos, cada B_j es cíclico de orden $d_j = p^{\alpha_{1j}} p^{\alpha_{2j}} \cdots p^{\alpha_{mj}}$. Como consecuencia de las desigualdades (7.1) se tiene que $d_j \mid d_{j-1}$ para todo $j = 2, \ldots, n$. ∎

La demostración del Teorema 7.48 nos dice cómo se obtiene una descomposición invariante a partir de una descomposición primaria.

Ejemplos 7.49 *Descomposiciones invariantes a partir de descomposiciones primarias.*

(1) Supongamos dada una descomposición primaria de A, digamos

$$A = (A_1 \oplus A_2) \oplus (A_{21} \oplus A_{22} \oplus A_{23} \oplus A_{24}) \oplus (A_{31} \oplus A_{32}) \oplus (A_{71} \oplus A_{72} \oplus A_{73}),$$

donde $A_{ij} = \langle a_{ij} \rangle$ y los ordenes de los respectivos sumandos son (por este orden) 0,0,16, 4, 2, 2, 27, 3, 7, 7, 7. Entonces:

- $B_1 = A_{21} \oplus A_{31} \oplus A_{71} = \langle a_{21} + a_{31} + a_{71} \rangle$ es cíclico de orden $16 \cdot 27 \cdot 7 = 3.024$;
- $B_2 = A_{22} \oplus A_{32} \oplus A_{72} = \langle a_{22} + a_{32} + a_{72} \rangle$ es cíclico de orden $4 \cdot 3 \cdot 7 = 84$;
- $B_3 = A_{23} \oplus A_{73} = \langle a_{23} + a_{73} \rangle$ es cíclico de orden $2 \cdot 7 = 14$ y

- $B_4 = A_{24}$ es cíclico de orden 2.

Entonces

$$A = A_1 \oplus A_2 \oplus B_1 \oplus B_2 \oplus B_3 \oplus B_4 \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_{3.024} \times \mathbb{Z}_{84} \times \mathbb{Z}_{14} \times \mathbb{Z}_2$$

es una descomposición invariante de A.

(2) Sea $A = \mathbb{Z}_{12}^* \propto \mathbb{Z}_{12}$. En los Ejemplos 7.45 vimos que

$$A = \langle(1,3)\rangle \oplus \langle(-1,0)\rangle \oplus \langle(5,0)\rangle \oplus \langle(1,4)\rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$$

es una descomposición primaria de A. Por tanto

$$A = \langle(1,7)\rangle \oplus \langle(-1,0)\rangle \oplus \langle(5,0)\rangle \cong \mathbb{Z}_{12} \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

es una descomposición invariante de A.

También es fácil sacar consecuencias de la demostración del Teorema 7.48 para obtener descomposiciones primarias a partir de descomposiciones invariantes.

Ejemplo 7.50 *Descomposiciones primarias a partir de descomposiciones invariantes.*
Sea

$$A = \langle a_1\rangle \oplus \langle a_2\rangle \oplus \langle a_3\rangle \oplus \langle a_4\rangle \cong \mathbb{Z}_{2.025} \times \mathbb{Z}_{135} \times \mathbb{Z}_9$$

(donde el isomorfismo es componente a componente). Observando que $2.025 = 3^4 \cdot 5^2$ y $135 = 3^3 \cdot 5$, definimos

$$\begin{array}{ll} B_{31} = \langle 25a_1\rangle \cong \mathbb{Z}_{81}, & B_{51} = \langle 81a_1\rangle \cong \mathbb{Z}_{25} \\ B_{32} = \langle 5a_2\rangle \cong \mathbb{Z}_{27}, & B_{52} = \langle 27a_2\rangle \cong \mathbb{Z}_5 \\ B_{33} = \langle a_4\rangle \cong \mathbb{Z}_9. & \end{array}$$

Entonces $A = B_{31} \oplus B_{32} \oplus B_{33} \oplus B_{51} \oplus B_{52}$ es una descomposición primaria de A.

Por supuesto, es posible descomponer un grupo abeliano finito como suma directa de subgrupos cíclicos sin ajustarse a ninguno de los "formatos" de las descomposiciones primarias o invariantes. Por ejemplo, si $A = \mathbb{Z}_6 \times \mathbb{Z}_3 \times \mathbb{Z}_2$ entonces la descomposición

$$A = \langle(1,0,0)\rangle \oplus \langle(0,1,0)\rangle \oplus \langle(0,0,1)\rangle$$

no es de ninguno de esos dos tipos, aunque no es difícil obtener una descomposición primaria

$$A = \langle(2,0,0)\rangle \oplus \langle(3,0,0)\rangle \oplus \langle(0,1,0)\rangle \oplus \langle(0,0,1)\rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2$$

y una invariante

$$A = \langle(1,0,0)\rangle \oplus \langle(0,1,1)\rangle \cong \mathbb{Z}_6 \times \mathbb{Z}_6.$$

Lo importante de estas descomposiciones es que presentan buenas condiciones de unicidad. En efecto, como vamos a ver, cualesquiera dos descomposiciones primarias de un grupo A

(abeliano y finitamente generado) son "esencialmente iguales", lo que nos permite asignarle a un tal grupo una lista de números enteros (los periodos de los sumandos que aparecen en una de esas descomposiciones). Otro tanto podrá decirse de las descomposiciones invariantes. Además, estas listas de números determinan salvo isomorfismos al grupo A, en el mismo sentido en el que la dimensión determina salvo isomorfismos a un espacio vectorial de dimensión finita. Aunque el caso que nos ocupa es más sofisticado, en ambos somos capaces de asociar a un objeto (grupo o espacio vectorial) una lista de números (uno sólo, la dimensión, en el caso vectorial) de tal modo que dos objetos son isomorfos si y sólo si tienen la misma lista.

Definición 7.51 *Sean A y B dos grupos abelianos finitamente generados.*

Dos descomposiciones primarias de A y B son semejantes *si los sumandos que intervienen son isomorfos dos a dos. Si ordenamos las descomposiciones como se ha indicado en la Definición 7.43, digamos*

$$A = (\oplus_{j=1}^{n} A_j) \oplus (\oplus_{j=1}^{m_1} A_{1j}) \oplus \cdots \oplus (\oplus_{j=1}^{m_k} A_{kj})$$

y

$$B = (\oplus_{j=1}^{n'} B_j) \oplus (\oplus_{j=1}^{m'_1} B_{1j}) \oplus \cdots \oplus (\oplus_{j=1}^{m'_{k'}} B_{k'j}),$$

es claro que éstas son semejantes si y sólo si $n = n'$, $k = k'$, cada $m_i = m'_i$ y $p(A_{ij}) = p(B_{ij})$ para cada posible par de índices.

Dos descomposiciones invariantes $A = \oplus_{i=1}^{n} A_i$ y $B = \oplus_{i=1}^{n'} B_i$ son semejantes *si los sumandos que intervienen son isomorfos dos a dos, lo que claramente equivale a que tengan el mismo número de sumandos ($n = n'$) y las mismas listas de periodos ($p(A_i) = p(B_i)$ para todo $i = 1, \ldots, n$).*

Es fácil ver que, si A y B tienen descomposiciones primarias (o invariantes) semejantes, entonces A y B son isomorfos. El siguiente teorema nos dice, esencialmente, que se verifica el recíproco:

Teorema 7.52 *Sea A un grupo abeliano finitamente generado. Entonces:*

(1) Todas las descomposiciones primarias de A son semejantes.

(2) Todas las descomposiciones invariantes de A son semejantes.

Demostración. En vista de que se puede pasar de una descomposición primaria a una invariante y viceversa, bastará con demostrar una de las dos afirmaciones. Demostraremos la primera.

Sea

$$A = (\oplus_{j=1}^{n} A_j) \oplus (\oplus_{j=1}^{m_1} A_{1j}) \oplus \cdots \oplus (\oplus_{j=1}^{m_k} A_{kj})$$

una descomposición primaria de A con $p(A_i) = 0$ y $p(A_{ij}) = p_i^{\alpha_{ij}}$ para ciertos enteros primos positivos $p_1 < p_2 < \cdots < p_k$ y ciertos enteros positivos α_{ij} con $\alpha_{i1} \geq \alpha_{i2} \geq \cdots \geq \alpha_{im_i} \geq 1$ para cada $i = 1, \ldots, k$. Obsérvese que $\oplus_{j=1}^{n} A_j \cong A/t(A)$, por lo que n es el rango del grupo

libre $A/t(A)$ y por tanto está determinado por A (no depende de la descomposición particular elegida). Por otro lado, es claro que, para cada $i = 1, \ldots, k$, se tiene

$$\oplus_{j=1}^{m_i} A_{ij} = t_{p_i}(A),$$

por lo que estos subgrupos también están determinados por A. En consecuencia, podemos limitarnos a demostrar la unicidad asumiendo que A es un p-grupo finito.

En esta situación, dos descomposiciones primarias de A serán de la forma

$$A = A_1 \oplus \cdots \oplus A_n = B_1 \oplus \cdots \oplus B_m,$$

donde cada sumando es cíclico y, si ponemos $p(A_i) = p^{\alpha_i}$ y $p(B_i) = p^{\beta_i}$, se tiene $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$ y $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_m$. Vamos a ver, por inducción en i, que $\alpha_i = \beta_i$ para cada i.

Obsérvese que $p^{\alpha_1} = p(A) = p^{\beta_1}$, lo que resuelve el caso $i = 1$. Supongamos pues que $\alpha_j = \beta_j$ para cada $j = 1, \ldots, i-1$, y veamos que $\alpha_i = \beta_i$. Podemos suponer sin pérdida de generalidad que $\alpha_i \leq \beta_i$.

Observemos lo siguiente: Sea C un grupo cíclico de orden p^r y sea $s \in \mathbb{N}$. Se tiene $p^s C = 0$ si y sólo si $s \geq r$. Por otra parte, si $s \leq r$, entonces $p^s C$ es cíclico de orden p^{r-s} por la Proposición **??**. En consecuencia, si ponemos $q = p^{\alpha_i}$, se tiene

$$\begin{array}{rcl} qA & \cong & qA_1 \oplus \cdots \oplus qA_{i-1} \\ & \cong & (qB_1 \oplus \cdots \oplus qB_{i-1}) \oplus (qB_i \oplus \cdots \oplus qB_m). \end{array}$$

Como $qA_1 \oplus \cdots \oplus qA_{i-1}$ y $qB_1 \oplus \cdots \oplus qB_{i-1}$ tienen el mismo cardinal, deducimos que $qB_i \oplus \cdots \oplus qB_m = 0$. En particular $0 = qB_i = p^{\alpha_i} B_i$, de modo que $\alpha_i \geq \beta_i$, y por tanto $\alpha_i = \beta_i$, como queríamos ver. ∎

Definición 7.53 *Sea A un grupo abeliano finitamente generado. Sea*

$$A = \oplus_{i=1}^{n} A_i \tag{7.2}$$

una descomposición primaria ordenada como en la Definición 7.43. Entonces la lista $(p(A_1), \ldots, p(A_n))$ (que no depende de la descomposición primaria elegida, por el Teorema 7.52) se conoce como la lista de los divisores elementales *de A.*

Análogamente, si (7.2) es una descomposición invariante, entonces la lista $(p(A_1), \ldots, p(A_n))$ (que tampoco depende de la descomposición invariante elegida) se conoce como la lista de los factores invariantes *de A.*

En ambas listas, cada sumando cíclico infinito aporta un 0 al principio de la lista. A menudo se simplifica la notación escribiendo $(m; p(A_{m+1}), \ldots, p(A_n))$, donde m es el número de ceros en la lista original.

Ejemplos 7.54 *Listas de divisores elementales y factores invariantes.*

(1) Si A es el grupo del primer apartado de los Ejemplos 7.49, la lista de sus divisores elementales es $(2; 16, 4, 2, 2, 27, 3, 7, 7, 7)$, y la de sus factores invariantes es $(2; 3.024, 84, 14)$.

(2) Para el grupo $\mathbb{Z}^* \propto \mathbb{Z}$, las listas de divisores elementales y de factores invariantes coinciden, y son $(0, 2)$. ¿Para qué tipo de grupos coinciden ambas listas?

(3) Los divisores elementales de $\mathbb{Z}_{12}^* \propto \mathbb{Z}_{12}$ son $(4, 2, 2, 3)$, y sus factores invariantes son $(12, 2, 2)$.

Todo lo visto en esta sección se resume en el siguiente Teorema:

Teorema 7.55 (Teorema de Estructura de Grupos Abelianos Finitamente Generados)

(1) Todo grupo abeliano finitamente generado tiene una descomposición primaria y una descomposición invariante.

(2) Las siguientes condiciones son equivalentes para dos grupos abelianos:

(a) Son isomorfos.
(b) Tienen descomposiciones primarias semejantes.
(c) Tienen descomposiciones invariantes semejantes.
(d) Tienen la misma lista de divisores elementales.
(e) Tienen la misma lista de factores invariantes.

Ejemplo 7.56

(1) Demostrar que, si $n \in \mathbb{Z}^+$ es libre de cuadrados, entonces todo grupo abeliano finito de orden n es cíclico (y por tanto isomorfo a $\mathbb{Z}_n$).

(2) Si p es un primo positivo, demostrar que, salvo isomorfismos, los únicos grupos abelianos de orden p^2 son $\mathbb{Z}_{p^2}$ y $\mathbb{Z}_p \times \mathbb{Z}_p$. Además se puede borrar "abelianos".

(3) Describir, salvo isomorfismos, todos los grupos abelianos de órdenes 8, 12, 16, 20 y 24.

Ejemplo 7.57 *Demostrar el recíproco del Teorema de Lagrange para grupos abelianos finitos. Es decir, demostrar que un grupo abeliano de orden n tiene un subgrupo de orden m para cada divisor m de n.*

Ejemplos 7.58 *Algunas decomposiciones invariantes y primarias.*

(1) Los grupos multiplicativos $\mathbb{Z}_5^*$, $\mathbb{Z}_{10}^*$ y $\mathbb{Z}_{12}^*$ tienen 4 elementos (pues $\phi(5) = \phi(10) = \phi(12) = 4$). Los dos primeros son cíclicos (busca un generador), y por tanto isomorfos entre sí. El tercero no es cíclico (tiene periodo 2), y por el ejercicio anterior debe ser isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ (da un isomorfismo explícito).

(2) Los grupos multiplicativos $\mathbb{Z}_{15}^*$, $\mathbb{Z}_{16}^*$, $\mathbb{Z}_{20}^*$, $\mathbb{Z}_{24}^*$ y $\mathbb{Z}_{30}^*$ tienen 8 elementos, por lo que han de ser isomorfos a uno de estos tres: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ ó $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Considerando los órdenes de los elementos se deduce que ninguno es cíclico, que $\mathbb{Z}_{24}^*$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ y que los otros cuatro son isomorfos a $\mathbb{Z}_4 \times \mathbb{Z}_2$.

(3) Vamos a calcular todos los grupos abelianos de orden 420 salvo isomorfismos y sus descomposiciones invariantes y primarias. Como $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, las posibles listas de divisores elementales son $(4, 3, 5, 7)$ ó $(2, 2, 3, 5, 7)$. Por tanto, salvo isomorfismos, los grupos abelianos de orden 420 son

$$A = \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \quad \text{y} \quad B = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7.$$

Éstas son sus descomposiciones primarias. Sus descomposiciones invariantes serán

$$A = \mathbb{Z}_{420} \quad \text{y} \quad B = \mathbb{Z}_{210} \times \mathbb{Z}_2.$$

Por el Teorema de Estructura 7.55, todo grupo abeliano finitamente generado es suma directa de cíclicos. Esto no es cierto para grupos abelianos en general, considérese $\mathbb{Q}$; ni siquiera para grupos abelianos de torsión, como muestra el siguiente ejemplo.

Ejemplo 7.59 *Un grupo abeliano de torsión que no es suma directa de grupos cíclicos.*
Sea p un número primo. El conjunto X_p de los números racionales de la forma $\frac{m}{p^n}$, donde $m \in \mathbb{Z}$ y n es un entero no negativo, es un subgrupo de $\mathbb{Q}$. Además $\mathbb{Z}$ es un subgrupo de X_p. Se define $\mathbb{Z}_{p^\infty} = X_p/\mathbb{Z}$. Para cada entero no negativo n, sea A_n el subgrupo de $\mathbb{Z}_{p^\infty}$ generado por $a_n = \frac{1}{p^n} + \mathbb{Z}$. Como a_n tiene orden p^n, entonces A_n es isomorfo a $\mathbb{Z}_{p^n}$. Además $0 = A_0 \subset A_1 \subset A_2 \subset \cdots$ y $\cup_{n\in\mathbb{N}} A_n = \mathbb{Z}_{p^\infty}$.

Vamos a ver que todo subgrupo propio H de $\mathbb{Z}_{p^\infty}$ es igual a A_n para algún $n \in \mathbb{N}$. El conjunto de los números naturales n tales que $a_n \in H$ está acotado (¿por qué?). Sea n el máximo de dicho conjunto. Entonces $A_n \subseteq H$. Si $\frac{m}{p^t} + \mathbb{Z} \in H$, con $\text{mcd}(m, p) = 1$, entonces existen $x, y \in \mathbb{Z}$ tales que $xm + yp^t = 1$. Luego $a_t = \frac{1}{p^t} + \mathbb{Z} = x\frac{m}{p^t} + y + \mathbb{Z} = x(\frac{m}{p^t} + \mathbb{Z}) \in H$, y por tanto $t \leq n$, de donde se concluye que $\frac{m}{p^t} + \mathbb{Z} = mp^{n-t}a_n \in A_n$. Deducimos que $H = A_n$, como queríamos.

La conclusión final es que $\mathbb{Z}_{p^\infty}$ es indescomponible y, como no es cíclico, tampoco es suma directa de grupos cíclicos.

7.6 Presentaciones por generadores y relaciones

Sea L un grupo abeliano libre con base $\{a_1, \ldots, a_n\}$ y sea S un subgrupo de L. Sabemos que S ha de estar generado por un conjunto finito $\{r_1, \ldots, r_m\}$ de elementos de L; es decir, cada r_i será una combinación lineal con coeficientes enteros de los a_j, digamos

$$r_i = k_{i1}a_1 + \cdots + k_{in}a_n \qquad (k_{ij} \in \mathbb{Z}).$$

Consideremos ahora el grupo cociente L/S. Abusando de la notación, escribiremos $a_j = a_j + S$. Entonces $\{a_1, \ldots, a_n\}$ es un conjunto generador de L/S, y para cada $i = 1, \ldots, m$ se tiene

$$k_{i1}a_1 + \cdots + k_{in}a_n = 0 \qquad (\text{en } L/S).$$

Estas igualdades se llaman "relaciones" entre los generadores $a_1, \ldots, a_n$ del grupo L/S. Es decir, los a_i son generadores "libres" (linealmente independientes, sin relaciones no triviales) cuando los vemos en L, pero satisfacen ciertas relaciones en el cociente L/S.

Por la Proposición 7.16, todo grupo abeliano finitamente generado A es isomorfo a uno de la forma recién descrita, y de hecho es usual encontrar grupos abelianos dados de esa manera. Dados L y S en la situación anterior y tales que $A \cong L/S$, escribiremos

$$A = \langle a_1, \ldots, a_n \mid r_1, \ldots, r_m \rangle,$$

y diremos que ésta es una *presentación de A por generadores y relaciones.*

Un resultado básico para el manejo de las presentaciones por generadores y relaciones es el siguiente:

Ejemplo 7.60 *Sea A un grupo abeliano que es suma directa de subgrupos: $A = A_1 \oplus \cdots \oplus A_n$. Para cada $i = 1, \ldots, n$, sea B_i un subgrupo de A_i. Entonces la familia $B_1, \ldots, B_n$ es independiente y, si $B = B_1 \oplus \cdots \oplus B_n$, se verifica*

$$\frac{A}{B} \cong \frac{A_1}{B_1} \times \cdots \times \frac{A_n}{B_n}$$

donde, si algún B_i coincide con A_i, el correspondiente factor es trivial y se puede eliminar del producto. (Indicación: Usar el Primer Teorema de Isomorfía.)

Como consecuencia, las presentaciones en las que cada relación es un múltiplo entero de un generador nos permiten ver al grupo en cuestión como suma directa de cíclicos de modo inmediato. Explícitamente, el hecho de que A tenga una presentación del tipo

$$A = \langle a_1, \ldots, a_r \mid d_1 a_1, \ldots, d_s a_s \rangle$$

(con $s \leq r$ y cada $d_i \in \mathbb{Z}^+$) equivale a decir que

$$A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

con $r - s$ factores iguales a $\mathbb{Z}$, y podemos eliminar los factores con $d_i = 1$. Por ejemplo, las siguientes son varias expresiones por generadores y relaciones de grupos abelianos finitamente generados:

$$\mathbb{Z}^n = \langle a_1, \ldots, a_n \rangle, \qquad \mathbb{Z}_n = \langle a \mid na \rangle, \qquad \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle a, b, c \mid 2b, 3c \rangle.$$

Un grupo puede tener diversas presentaciones. Por ejemplo, $\mathbb{Z} = \langle a \rangle = \langle a, b \mid b \rangle$ o, utilizando el Teorema Chino de los Restos, $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle a, b \mid 2a, 3b \rangle = \langle c \mid 6c \rangle$. En esta sección veremos cómo conseguir, a partir de una presentación por generadores y relaciones de un grupo abeliano finitamente generado A, otras presentaciones más manejables, con el objetivo último de obtener una presentación del tipo $\langle a_1, \ldots, a_r \mid d_1 a_1, \ldots, d_s a_s \rangle$ con $d_1 \mid d_2 \mid \cdots \mid d_s$, lo que nos dará la descomposición invariante de A.

La segunda herramienta básica para la manipulación de las presentaciones es:

Ejemplo 7.61 *Sean $a_1, a_2, \ldots, a_n$ elementos de un grupo abeliano A. Si, o bien $a_1' = a_1 + ta_2$, donde $t \in \mathbb{Z}$, o bien $a_1' = -a_1$, entonces:*

(1) $\langle a_1, a_2, \ldots, a_n \rangle = \langle a_1', a_2, \ldots, a_n \rangle$.

(2) El conjunto $\{a_1, a_2, \ldots, a_n\}$ es linealmente independiente si y sólo si lo es $\{a_1', a_2, \ldots, a_n\}$.

En otras palabras, si en un conjunto sumamos a un elemento un múltiplo entero de otro, o si cambiamos de signo un elemento, no cambian ni el subgrupo generado ni la dependencia o independencia lineal. Aplicando reiteradamente el Ejercicio 7.61, vemos que la afirmación sigue valiendo si sumamos a un elemento una combinación lineal (con coeficientes enteros) del resto de elementos.

Veamos con un ejemplo cómo pueden usarse estos resultados para simplificar las presentaciones:

Ejemplo 7.62 *Simplificación de una presentación por generadores y relaciones.*
Sea $A = \langle a, b, c \mid 2a+b+6c,\ 2a+2b+2c\rangle$. Esto significa que $A \cong L/S$, donde $\{a, b, c\}$ es base de L y $S = \langle 2a+b+6c, 2a+2b+2c\rangle$. Si hacemos $b' = 2a+b+6c$, entonces $\{a, b', c\}$ sigue siendo base de L y se tiene $2a+2b+2c = -2a+2b'-10c$, luego $S = \langle b', -2a+2b'-10c\rangle$; restando al segundo generador el doble del primero, y cambiando luego el signo del resultado, obtenemos $S = \langle b', 2a+10c\rangle$. Por tanto, $A = \langle b', a, c \mid b', 2a+10c\rangle$. Podemos simplificar más, haciendo $a' = a+5c$. Entonces $\{b', a', c\}$ sigue siendo base de L y además $S = \langle b', 2a'\rangle$, de modo que $A = \langle b', a', c \mid b', 2a'\rangle = \langle a', c' \mid 2a'\rangle$. Por tanto $A \cong \mathbb{Z}_2 \times \mathbb{Z}$.

En lo que sigue vemos cómo las ideas usadas en el Ejemplo 7.62 son suficientes para simplificar cualquier presentación. Lo primero que haremos será adoptar una notación matricial para las presentaciones que las hace más manejables. Supongamos que partimos de una expresión de un grupo por generadores y relaciones $A = \langle a_1, \ldots, a_n \mid r_1, \ldots, r_m\rangle$, donde las relaciones vienen dadas por las combinaciones lineales

$$r_i = k_{i1}a_1 + \cdots + k_{in}a_n \qquad (k_{ij} \in \mathbb{Z}). \tag{7.3}$$

Representamos este conjunto de relaciones por una matriz $K = (k_{ij})$. Recíprocamente, a cada matriz K de números enteros con m filas y n columnas, le asociaremos el grupo cuya presentación por generadores y relaciones es $\langle a_1, \ldots, a_n \mid r_1, \ldots, r_m\rangle$, donde cada r_i viene dado por la igualdad (7.3). En particular, una matriz $m \times n$ de la forma

$$\begin{pmatrix} d_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & d_m & 0 & \cdots & 0 \end{pmatrix} \tag{7.4}$$

se corresponde con el grupo abeliano $A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$, con $n-m$ factores iguales a $\mathbb{Z}$.

Comenzaremos notando que ciertas transformaciones en una matriz no alteran el grupo que define, y después veremos cómo combinar esas transformaciones para alcanzar una matriz del tipo (7.4).

Lema 7.63 *Si K es una matriz de números enteros y K' es una matriz obtenida a partir de K mediante una de las operaciones que siguen, entonces los grupos asociados a K y K' son isomorfos.*

F0: Eliminar una fila formada por ceros.

F1: Reordenar las filas.

F2: Cambiar el signo a todos los elementos de una fila.

F3: Sumar a una fila un múltiplo entero de otra.
(Si a la fila i-ésima le sumamos la j-ésima multiplicada por t, escribiremos $F_i + tF_j$).

C1: Reordenar las columnas.

C2: Cambiar el signo a todos los elementos de una columna.

C3: Sumar a una columna un múltiplo entero de otra.
(Si a la columna i-ésima le sumamos la j-ésima multiplicada por t, escribiremos $C_i + tC_j$).

Demostración. Con la notación L/S que venimos usando, las operaciones en las filas se traducen en manipulaciones de los generadores de S (o sea, de las relaciones en L/S) que no afectan al subgrupo: quitar un generador nulo, reordenar los generadores, sustituir uno por su opuesto, o sumarle a uno un múltiplo de otro.

Vemos ahora que la operación C3 no afecta a L ni a S, y dejamos que el lector analice por qué son también admisibles las operaciones de los tipos C1 y C2. Supongamos, para simplificar, que la operación es $C_1 + tC_2$. Si $\{a_1, \ldots, a_n\}$ es la base de L y ponemos $a'_2 = a_2 - ta_1$, entonces $\{a_1, a'_2, \ldots, a_n\}$ también es base de L. Si la matriz de partida es (k_{ij}) entonces el generador r_i es

$$\begin{aligned} r_i &= k_{i1}a_1 + k_{i2}a_2 + k_{i3}a_3 + \cdots + k_{in}a_n \\ &= k_{i1}a_1 + k_{i2}(a'_2 + ta_1) + k_{i3}a_3 + \cdots + k_{in}a_n \\ &= (k_{i1} + tk_{i2})a_1 + k_{i2}a'_2 + k_{i3}a_3 + \cdots + k_{in}a_n, \end{aligned}$$

por lo que la matriz obtenida al aplicar C3 representa a los mismos generadores de S, aunque expresados en una base distinta. En conclusión, la operación C3 no supone ningún cambio en L ni en S. ∎

A continuación describimos un método para pasar, mediante operaciones de los tipos anteriores, de una matriz cualquiera con coeficientes enteros a una matriz del tipo (7.4) en la que $d_1 \mid d_2 \mid \cdots \mid d_m$. Cada vez que hablemos de "la matriz K" nos estaremos refiriendo a la última matriz obtenida a partir de la inicial mediante las operaciones que se hayan descrito.

Comencemos notando el siguiente hecho: Sea a una entrada no nula de K con el menor valor absoluto (podemos suponer que $a > 0$, cambiando si hace falta el signo de su fila), y supongamos que a no divide a todas las entradas de K. Entonces podemos transformar K hasta hacer aparecer una entrada r con $0 < r < a$. Para ello, comenzamos haciendo operaciones F1 y C1 para poner a en la entrada $(1, 1)$; este paso lo damos sólo por comodidad en la notación. Supongamos que a no divide a cierta entrada de la primera fila, digamos k_{1j} (con $j \neq 1$). Dividiendo con resto, encontramos $q, r \in \mathbb{Z}$ con $0 < r < a$ y $k_{1j} = aq + r$. Entonces la operación $C_j - qC_1$ nos da una matriz con r en la entrada $(1, j)$, como queríamos. Si a no divide a una entrada de la primera columna procedemos de modo análogo, operando esta vez

por filas. Podemos pues suponer que a divide a todas las entradas de la primera fila y a todas las de la primera columna, pero no divide a cierto k_{ij} con $i, j \neq 1$. Por hipótesis, existen enteros b y c tales que $k_{1j} = ba$ y $k_{i1} = ca$. Haciendo primero la operación $F_i - cF_1$ (para poner un 0 en la entrada $(i, 1)$) y después la operación $F_1 - F_i$, obtenemos una matriz con a en la entrada $(1, 1)$ y $ba + bca - k_{ij}$ en la entrada $(1, j)$. Como a no divide a esta entrada de la primera fila, procedemos como al principio de este párrafo para obtener una entrada r con $0 < r < a$.

Como el valor absoluto no puede bajar indefinidamente, repitiendo el proceso anterior llegará un momento en el que K tendrá una entrada $a > 0$ que dividirá al resto de entradas de K, y podemos llevar a hasta el lugar $(1, 1)$. Ponemos entonces ceros en el resto de los lugares $(i, 1)$ de la primera columna: Tomamos $q \in \mathbb{Z}$ tal que $k_{i1} = qa$ y hacemos la operación $F_i - qF_1$. Hecho esto, podemos cambiar todas las entradas de la primera fila, excepto la $(1, 1)$, por ceros (¿por qué?).

Hemos llegado pues a una matriz de la forma

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

en la que a es positivo y divide a cada b_{ij}. A partir de ahora no haremos operaciones con la primera fila ni con la primera columna, por lo que ni a ni los ceros de esos lugares van a variar. De hecho, podemos eliminar esa fila y esa columna de la matriz y "apuntar" el valor de a (incluso olvidarlo, si $a = 1$). Además, las operaciones que podemos hacer no van a cambiar el hecho de que todas las entradas que se obtengan sean múltiplos de a (¿por qué?). Pues bien, procediendo con la submatriz (b_{ij}) como se acaba de describir, podremos llegar a una matriz del tipo

$$\begin{pmatrix} a & 0 & 0 & \cdots & 0 \\ 0 & b & 0 & \cdots & 0 \\ 0 & 0 & c_{33} & \cdots & c_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & c_{m3} & \cdots & c_{mn} \end{pmatrix}$$

en la que a divide a b y b divide a los c_{ij}. Continuando de este modo, y eliminando las filas de ceros que puedan aparecer, conseguiremos la matriz que buscamos. Por supuesto, el proceso se puede simplificar por procedimientos heurísticos.

Ejemplos 7.64 *Transformaciones en la matriz de generadores y relaciones.*

(1) Sea A el grupo abeliano con generadores a, b, c, d, e, f y relaciones:

$$\begin{array}{rcrcrcrcrcrcr} 4a & + & 13b & & & & & + & 3e & + & f & = & 0 \\ 5a & - & 7b & + & 6c & & & + & & - & f & = & 0 \\ 3a & + & 3b & & & + & 3d & + & & & & = & 0 \\ 3a & + & 6b & & & & & + & 3e & & & = & 0 \\ a & + & 7b & & & & & & & + & f & = & 0 \end{array}$$

La matriz asociada a dicho grupo es

$$\begin{pmatrix} 4 & 13 & 0 & 0 & 3 & 1 \\ 5 & -7 & 6 & 0 & 0 & -1 \\ 3 & 3 & 0 & 3 & 0 & 0 \\ 3 & 6 & 0 & 0 & 3 & 0 \\ 1 & 7 & 0 & 0 & 0 & 1 \end{pmatrix}$$

En este ejemplo veremos que no es necesario seguir estrictamente los pasos descritos anteriormente. Por ejemplo, el papel que antes ha representado la entrada de arriba a la izquierda lo asumirá ahora la entrada de abajo a la derecha. Observamos que la primera fila es combinación lineal de las dos últimas. Luego, restando a la primera la suma de las dos últimas (lo que representaremos por $F_1 - F_4 - F_5$) obtenemos:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & -7 & 6 & 0 & 0 & -1 \\ 3 & 3 & 0 & 3 & 0 & 0 \\ 3 & 6 & 0 & 0 & 3 & 0 \\ 1 & 7 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Eliminando la primera fila, y haciendo sucesivamente $F_1 + F_4$ (con la nueva numeración), $C_1 - C_6$ y $C_2 - 7C_6$, obtenemos

$$\begin{pmatrix} 6 & 0 & 6 & 0 & 0 & 0 \\ 3 & 3 & 0 & 3 & 0 & 0 \\ 3 & 6 & 0 & 0 & 3 & 0 \\ 1 & 7 & 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 6 & 0 & 6 & 0 & 0 & 0 \\ 3 & 3 & 0 & 3 & 0 & 0 \\ 3 & 6 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Podemos eliminar la última fila y última columna, y haciendo entonces (con la nueva numeración) $C_1 - C_3 - C_4 - C_5$ y $C_2 - C_4 - 2C_5$, obtenemos por fin la matriz

$$\begin{pmatrix} 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix},$$

de la que se deduce que $A \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_6 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ es la descomposición invariante de A. A partir de ésta podemos obtener la descomposición indescomponible $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

(2) Sea A un grupo abeliano con matriz de generadores y relaciones dada por

$$\begin{pmatrix} 0 & 12 & 24 & 0 \\ 4 & 10 & 12 & 6 \\ 4 & 8 & 0 & 4 \end{pmatrix}$$

Es claro que, por más que operemos, las entradas van a ser siempre pares. Por otra parte, no es difícil conseguir que una sea 2, por ejemplo, haciendo $F_2 - F_3$ (escriba el lector las

matrices que se van obteniendo). De los dos "2" que aparecen, el más cómodo es de la última columna. Podemos poner ceros en el resto de esa columna haciendo $F_3 - 2F_2$, siguiendo el método descrito, pero es más fácil hacer $C_4 - C_1$. Ahora podemos poner ceros en la segunda fila, haciendo $C_2 - C_4$ y $C_3 - 6C_4$. Pasando entonces la primera fila al último lugar, y pasando después la última columna al primer lugar, habremos puesto el 2 en la entrada $(1,1)$. Haciendo entonces, sucesivamente, $C_3 - 2C_2$ y $C_4 - 2C_3$, se obtiene por fin

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 12 & 0 \end{pmatrix},$$

por lo que $A \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}$.

(1) Sea $f : A \to B$ un isomorfismo entre dos grupos abelianos. Demostrar (hasta aburrirse) que:

   (a) La familia $\{A_i\}_{i\in I}$ de subgrupos de A es independiente si y sólo si la familia $\{f(A_i)\}_{i\in I}$ de subgrupos de B es independiente.

   (b) Un subgrupo C de A es un sumando directo de A si y sólo si el subgrupo $f(C)$ es un sumando directo de B.

   (c) A es indescomponible si y sólo si B es indescomponible.

   (d) La familia $\{a_i\}_{i\in I}$ de elementos de A es linealmente independiente si y sólo si la familia $\{f(a_i)\}_{i\in I}$ de elementos de B es linealmente independiente.

   (e) A es libre si y sólo si B es libre.

   (f) Si T es el subgrupo de torsión de A entonces $f(T)$ es el subgrupo de torsión de B.

   (g) A es de torsión si y sólo si B es de torsión.

   (h) A es libre de torsión si y sólo si B es libre de torsión.

(2) Sea A un grupo abeliano libre de rango n. Decidir sobre la verdad o falsedad de las siguientes afirmaciones:

   (a) Todo subconjunto linealmente independiente de A tiene a lo sumo n elementos.

   (b) Todo subconjunto generador de A tiene al menos n elementos.

   (c) Todo subconjunto linealmente independiente de A con n elementos es una base de A.

   (d) Todo subconjunto generador de A con n elementos es una base de A.

(3) Sean L, M, N grupos abelianos finitamente generados con $L \oplus N \cong M \oplus N$. Demostrar que $L \cong M$.

(4) Determinar el subgrupo de torsión de los siguientes grupos aditivos: $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Z} \oplus \mathbb{Z}_n$, $\mathbb{Q}/\mathbb{Z}$, $\mathbb{R}/\mathbb{Z}$.

(5) Determinar el subgrupo de torsión del grupo de las unidades de los anillos $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[i]$ y $\mathbb{Z}[\sqrt{2}]$.

(6) Sea P un polinomio mónico de $\mathbb{Z}[X]$ de grado n. Demostrar que el grupo aditivo de $\mathbb{Z}[X]/(P)$ es libre de rango n. ¿Puede fallar el resultado si P no es mónico?

(7) Probar que si A es un grupo abeliano libre y $n \in \mathbb{N}$, entonces A tiene un subgrupo de índice n.

(8) Encontrar un subgrupo B de $A = \mathbb{Z}_{16}^*$ tal que $A/B \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(9) Sea A el subconjunto de $\mathbb{Z} \times \mathbb{Z}$ formado por las parejas de números enteros (a, b) tales que $a \equiv b \bmod 10$. Demostrar que A es un subgrupo de $\mathbb{Z} \times \mathbb{Z}$ y determinar una base de A.

(10) Para un grupo abeliano arbitrario A, demostrar que la familia $\{t_p(A)\}$, donde p recorre el conjunto de todos los enteros primos positivos, es independiente, y que su suma directa es $t(A)$.

(11) Demostrar que $t_p(\mathbb{Q}/\mathbb{Z})$ es el subgrupo $\mathbb{Z}_{p^\infty}$ del Ejemplo 7.59, y que $\mathbb{Q}/\mathbb{Z} = \oplus_p \mathbb{Z}_{p^\infty}$, donde p recorre el conjunto de todos los enteros primos positivos.

(12) Demostrar que el grupo aditivo $(A, +)$ de un anillo A es de torsión precisamente si la característica de A es diferente de 0. Si A es un dominio, demostrar que las condiciones son equivalentes a que $(A, +)$ no sea libre de torsión. El anillo $\mathbb{Z}[X]/(2X)$ muestra que, en la segunda parte, la hipótesis de que A sea un dominio no es superflua, ¿por qué?

(13) Encontrar bases para los siguientes subgrupos de grupos abelianos libres:

(a) $\langle 3a, 4b, 6a + 2b \rangle$, siendo a, b generadores de un grupo abeliano libre de rango 2.

(b) $\langle x+2y+4z, 3x+6y+12z, -12x-24y-48z, -2x+y+7z \rangle$, siendo x, y, z generadores de un grupo libre de rango 3.

(14) Demostrar que el grupo aditivo de los números racionales es indescomponible.

(15) Calcular las descomposiciones primaria e invariante de los siguientes grupos abelianos:

(a) $\mathbb{Z}_{20} \oplus \mathbb{Z}_{40} \oplus \mathbb{Z}_{108}$

(b) $\mathbb{Z}_{21}^*$.

(c) $\langle a, b \mid 3a + 6b = 9a + 24b = 0 \rangle$.

(d) $\langle a, b, c \mid 2a + b = 3a + c = 0 \rangle$.

(e) $\langle a, b, c \mid -4a + 2b + 6c = -6a + 2b + 6c = 7a + 4b + 15c = 0 \rangle$.

(f) $\langle a, b, c \mid a + 2b + 4c = 3a + 6b + 12c = -2a + b + 7c = 0 \rangle$.

(16) Clasificar el grupo abeliano presentado por los generadores y relaciones dados:

(a) Generadores a, b, c y relaciones

$$\begin{array}{rcrcrcl} 7a & + & 8b & + & 9c & = & 0 \\ 4a & + & 5b & + & 6c & = & 0 \\ a & + & 2b & + & 3c & = & 0 \end{array}$$

(b) Generadores a, b, c, d, e y relaciones

$$\begin{array}{rcrcrcrcrcr} a & - & 7b & - & 21c & + & 14d & & & = & 0 \\ 5a & - & 7b & - & 2c & + & 10d & - & 15e & = & 0 \\ 3a & - & 3b & - & 2c & + & 6d & - & 9e & = & 0 \\ a & - & b & & & + & 2d & - & 3e & = & 0 \end{array}$$

(17) Encontrar todos los grupos abelianos, salvo isomorfismos, de órdenes 30, 60, 72, 90, 180, 360, 720 y 1830, calculando para cada uno de ellos las descomposiciones primaria e invariante.

(18) Determinar salvo isomorfismos todos los grupos abelianos de orden ≤ 30 y dar la lista de sus divisores elementales y factores invariantes.

(19) Demostrar que la lista de factores invariantes de $\mathbb{Z}_n \oplus \mathbb{Z}_m$ es (nm) ó $(\text{mcm}(n,m), \text{mcd}(n,m))$.

(20) Demostrar que si A es un p-grupo abeliano que es la suma directa de n grupos cíclicos no nulos, entonces la ecuación $px = 0$ tiene exactamente p^n soluciones.

(21) Sea G un p-grupo abeliano finito en el que la ecuación $px = 0$ tiene a lo sumo p soluciones. Demostrar que G es cíclico. Demostrar que también es cíclico un grupo abeliano finito (no necesariamente un p-grupo) en el que la ecuación $px = 0$ tenga a lo sumo p soluciones para todo primo p.

(22) Resolver el Problema 32 del Capítulo 4 usando los resultados de este capítulo.

(23) Del Ejercicio 7.57 se deduce que, si G es un grupo abeliano finito y p es un divisor primo de $|G|$, entonces G contiene un elemento de orden p. Demostrar que este resultado sigue siendo válido si G no es abeliano. Éste es el Teorema de Cauchy que demostraremos en el capítulo siguiente con otros métodos. (Indicación: Usar el Ejercicio 7.57, la Ecuación de Clases e inducción en $|G|$.)

(24) Sea p primo. Demostrar que si G es un grupo abeliano finito en el que todo elemento no nulo tiene orden p, entonces $G \cong \mathbb{Z}_p^n$ para algún n.

(25) Demostrar que todo grupo abeliano finito no cíclico contiene un subgrupo isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$ para algún primo p.

(26) Sea B un subgrupo de un grupo abeliano finito A. Demostrar que A contiene un subgrupo isomorfo a A/B. ¿Es cierto el resultado si A es infinito?

(27) Sea A un grupo abeliano finito y sea a un elemento de A orden máximo. Demostrar que $\langle a \rangle$ es un sumando directo de A.

(28) Se pide:

(a) Encontrar un número natural n tal que existan exactamente 5 grupos abelianos de orden n salvo isomorfismos.

(b) [*] Encontrar todos los números naturales n tales que, salvo isomorfismos, existen exactamente 6 grupos abelianos de orden n.

(c) [*] Demostrar que para ningún número natural n hay exactamente 13 grupos abelianos de orden n salvo isomorfismos.

(29) [*] Un subgrupo propio H de un grupo G que no está contenido en ningún otro subgrupo propio de G se dice que es *maximal* (en G). Para un grupo abeliano finito A, demostrar:

(a) Los subgrupos maximales son precisamente los de índice primo.

(b) A tiene exactamente 2 subgrupos maximales si y sólo si A es cíclico y $|A|$ tiene exactamente dos divisores primos.

(30) Sea G el grupo abeliano definido por los generadores $g_1, \ldots, g_n$ y las relaciones $\sum_{j=1}^{n} a_{ij} g_i = 0$ $(i = 1, \ldots, n)$, con $a_{ij} \in \mathbb{Z}$. Demostrar que G es finito precisamente si el determinante de la matriz (a_{ij}) es diferente de 0 y que, en tal caso, el orden de G coincide con el valor absoluto de dicho determinante.

Index