ÁLGEBRA

Grupos, Anillos y Módulos

Jorge Alberto Guccione

y

Juan José Guccione

Índice general

Parte 1

Grupos

Capítulo 1

Teoría elemental

1. Monoides

Una *operación interna* definida en un conjunto S es una función $*\colon S \times S \to S$. Como es usual escribiremos $s_1 * s_2$ en lugar de $*(s_1, s_2)$. Decimos que la operación $*$ es *asociativa* si $s_1 * (s_2 * s_3) = (s_1 * s_2) * s_3$ para todo $s_1, s_2, s_3 \in S$, y que es *conmutativa* o *abeliana* si $s_1 * s_2 = s_2 * s_1$ para todo $s_1, s_2 \in S$. Un *magma* es un conjunto no vacío S provisto de una operación interna. Usualmente hablaremos de un magma S, mencionando sólo al conjunto subyacente. Esto es ambiguo, porque en un conjunto puede haber dos operaciones internas distintas. Por ejemplo en el conjunto de los números enteros tenemos la suma y el producto. Así que cuando sea necesario procuraremos ser claros. Un magma S es *asociativo* (respectivamente *conmutativo* o *abeliano*) si lo es su operación y es *finito* si lo es su conjunto subyacente. En ese caso llamamos *orden* de S al cardinal $|S|$ de S. Un *semigrupo* es un magma asociativo. Para cada magma S, podemos construir un nuevo magma con el mismo conjunto subyacente, llamado *magma opuesto de* S y denotado S^{op}, mediante el simple trámite de invertir el orden en que se realiza la operación. Más precisamente, si $*$ es la operación de S, la operación $*_{\mathrm{op}}$ de S^{op} está definida por $s_1 *_{\mathrm{op}} s_2 := s_2 * s_1$. Es evidente que S^{op} es un semigrupo si y sólo si S lo es, y que S es un magma conmutativo si y sólo si $S^{\mathrm{op}} = S$.

Para cada elemento s de un magma S, denotamos con $l_s\colon S \to S$ y $r_s\colon S \to S$ a las funciones definidas por $l_s(t) := s * t$ y $r_s(t) := t * s$, respectivamente. Es claro que las siguientes propiedades son equivalentes:

1. S es asociativo.
2. $l_{s_1} \circ r_{s_2} = r_{s_2} \circ l_{s_1}$ para todo $s_1, s_2 \in S$.
3. $l_{s_1} \circ l_{s_2} = l_{s_1 * s_2}$ para todo $s_1, s_2 \in S$.
4. $r_{s_1} \circ r_{s_2} = r_{s_2 * s_1}$ para todo $s_1, s_2 \in S$.

Todavía más claro es que S es conmutativo si y sólo si $l_s = r_s$ para todo $s \in S$.

Decimos que $s \in S$ es *cancelable a izquierda* si $s * t = s * t'$ implica $t = t'$, que es *cancelable a derecha* si $t * s = t' * s$ implica $t = t'$ y que es *cancelable* si lo es a izquierda y a derecha. Es

obvio que s es cancelable a izquierda si y sólo si l_s es inyectiva, y que lo es a derecha si y sólo si r_s es inyectiva. Notemos que s es cancelable a un lado en S si y sólo si lo es al otro en S^{op}. Si s_1 y s_2 son elementos cancelables a izquierda de un semigrupo S, entonces $s_1 * s_2$ también lo es y, obviamente, lo mismo pasa con la cancelatividad a derecha. En cambio, la hipótesis de que $s_1 * s_2$ es cancelable a izquierda sólo implica que s_2 lo es, y, similarmente, la de que $s_1 * s_2$ es cancelable a derecha, que s_1 lo es. Un magma es *cancelativo* si todos sus elementos son cancelables.

Un elemento $e \in S$ es *neutro a izquierda* si $e * s = s$ para todo $s \in S$, es *neutro a derecha* si $s * e = s$ para todo $s \in S$ y es *neutro* si lo es a izquierda y a derecha. Si un magma S tiene neutro a izquierda e y neutro a derecha e', entonces $e = e'$. En efecto, como e' es neutro a derecha, $e = e * e'$ y como e es neutro a izquierda, $e * e' = e'$. En particular S tiene a lo sumo un neutro. Diremos que un magma es *unitario* si tiene neutro. Evidentemente e es neutro a un lado en S si y sólo si lo es al otro en S^{op}.

Un *monoide* es un semigrupo unitario. Un elemento s de un monoide S es *inversible a izquierda* si existe $t \in S$ tal que $t * s = e$, y es *inversible a derecha* si existe $t \in S$ tal que $s * t = e$. En el primer caso decimos que t es una *inversa a izquierda* de s, y en el segundo, que es una *inversa a derecha*. Diremos que s es *inversible*, si lo es a ambos lados. Es claro que s es inversible a izquierda si y sólo si r_s es sobreyectiva, e inversible a derecha si y sólo si l_s es sobreyectiva. Si s tiene inversa a izquierda y a derecha, entonces estas son únicas y coinciden. En efecto, supongamos que t es una inversa a izquierda de s, y t' una inversa a derecha. Entonces

$$t = t * e = t * (s * t') = (t * s) * t' = e * t' = t'.$$

Esto nos autoriza a decir que t es la *inversa* de s.

Muchas propiedades predicables sobre elementos y subconjuntos de un magma S tienen una versión a izquierda y otra a derecha, de modo de que cada una de ellas en S es equivalente a la otra en S^{op}. A veces, cuando un predicado tenga una versión a izquierda y otra a derecha daremos sólo una de ellas, dejando al lector la tarea de enunciar la otra.

No es costumbre usar un símbolo especial como $*$ para denotar una operación asociativa diferente de la suma y la multiplicación usuales. Lo habitual es denotarla con $+$ y llamarla suma, o con la yuxtaposición y llamarla producto. En el primer caso 0 y $-s$ designan al neutro de la operación y al inverso de un elemento $s \in S$, respectivamente. En el segundo, estos papeles los cumplen los símbolos 1 y s^{-1}. La notación aditiva raramente se usa para designar operaciones que no son conmutativas, porque es muy desagradable encontrar expresiones tales como $s + t \neq t + s$. De ahora en más supondremos que S es un monoide no necesariamente conmutativo y usaremos la notación multiplicativa. También seguiremos esta convención para magmas arbitrarios y, más adelante, para grupos. Reservaremos la notación aditiva para usarla en algunos ejemplos y en unas pocas situaciones en las que haya involucradas estructuras abelianas.

Es evidente que 1 es inversible con $1^{-1} = 1$; que si r es inversible a izquierda con inversa a izquierda s, entonces s es inversible a derecha con inversa a derecha r; y que si s y t son inversibles a izquierda con inversas a izquierda s' y t' respectivamente, entonces st es inversible a izquierda con inversa a izquierda $t's'$. En particular, si s es inversible, s^{-1} también lo es y $(s^{-1})^{-1} = s$ y si s y t son inversibles, st también lo es y $(st)^{-1} = t^{-1}s^{-1}$. Es claro también que si r es un inverso a izquierda de st, entonces rs es un inverso a izquierda de t. Además se comprueba fácilmente que si s es inversible a izquierda, entonces es cancelable a izquierda

y, similarmente, que los elementos inversibles a derecha son cancelables a derecha (ponemos abajo un ejercicio que generaliza levemente este hecho). El siguiente resultado completa el panorama general.

PROPOSICIÓN 1.1. *Para cada elemento s de un monoide S son equivalentes:*

1. *s es inversible a izquierda y cancelable a derecha.*
2. *s es inversible a derecha y cancelable a izquierda.*
3. *s es inversible.*

DEMOSTRACIÓN. Es claro que 3) implica 1). Veamos que 1) implica 3). Por hipótesis existe $t \in S$ tal que $ts = 1$. Debemos mostrar que $st = 1$, pero esto se sigue de que

$$(st)s = s(ts) = s1 = s = 1s$$

y de que s es cancelable a derecha. La equivalencia entre 2) y 3) es similar. □

Como muestra la siguiente proposición para monoides finitos los conceptos de cancelatividad e inversibilidad coinciden.

PROPOSICIÓN 1.2. *Si S es finito, entonces para cada $s \in S$ son equivalentes:*

1. *s es inversible.*
2. *s es cancelable a izquierda.*
3. *s es cancelable a derecha.*

DEMOSTRACIÓN. Como S es finito,

$$\begin{aligned} s \text{ es cancelable a izquierda} &\Leftrightarrow l_s \text{ es inyectivo} \\ &\Leftrightarrow l_s \text{ es sobreyectivo} \\ &\Leftrightarrow s \text{ es inversible a derecha} \\ &\Rightarrow s \text{ es cancelable a derecha.} \end{aligned}$$

Por dualidad,

s es cancelable a derecha $\Leftrightarrow$ s es inversible a izquierda $\Rightarrow$ s es cancelable a izquierda.

El resultado es una consecuencia inmediata de estos dos hechos. □

EJERCICIO 1.3. *Consideremos un semigrupo S que tiene un neutro a izquierda e y tomemos $s \in S$. Pruebe que si existe $s' \in S$ tal que $s's = e$ entonces s es cancelable a izquierda.*

Para $n \geq 0$ definimos la n-ésima potencia s^n, de un elemento s de un monoide S, recursivamente por

- $s^0 := 1$,
- $s^{n+1} := s^n s$.

Si s es inversible, entonces $(s^{-1})^n = (s^n)^{-1}$ para todo $n > 0$ y definimos s^{-n} por

- $s^{-n} := (s^n)^{-1}$ para todo $n > 0$.

Dejamos como ejercicio probar que

$$s^{m+n} = s^m s^n \quad \text{y} \quad (s^m)^n = s^{mn}$$

para todo $m, n \geq 0$, y que cuando s es inversible estas igualdades valen para todo $m, n \in \mathbb{Z}$. Diremos que dos elementos s y t de S *conmutan* si $st = ts$. Si $s, t \in S$ conmutan, entonces s^m y t^n conmutan para todo $m, n \geq 0$ y $(st)^m = s^m t^m$, para todo $m \geq 0$. Nuevamente, cuando s y t son inversibles estas propiedades valen para todo $m, n \in \mathbb{Z}$.

Supongamos que $s \in S$ es inversible y que la aplicación $n \mapsto s^n$ no es inyectiva. Tomemos $m < n$ tales que $s^m = s^n$. Entonces

$$s^{n-m} = s^n s^{-m} = s^n (s^m)^{-1} = 1.$$

Al mínimo natural l tal que $s^l = 1$ se lo llama el *orden* de s y se lo denota $|s|$. Los elementos

$$s^0, \ldots, s^{|s|-1}$$

son todos distintos, ya que si existieran $0 \leq m < n < |s|$ tales que $s^m = s^n$, sería $s^{n-m} = 1$, contradiciendo la definición de $|s|$. Además, si $n \in \mathbb{Z}$ y $n = |s|q + r$ con $0 \leq r < |s|$, entonces

$$s^n = s^r (s^{|s|})^q = s^r.$$

Por lo tanto $|s|$ es la cantidad de elementos de $\{s^n : n \in \mathbb{N}\}$ y $s^n = 1$ si y sólo si n es múltiplo de $|s|$. Cuando no existe un tal l decimos que s tiene *orden infinito*.

EJEMPLO 1.4. *Los conjuntos* $\mathbb{N}$ *de los números naturales,* $\mathbb{N}_0$ *de los enteros no negativos,* $\mathbb{Z}$ *de los números enteros,* $\mathbb{Q}$ *de los números racionales,* $\mathbb{R}$ *de los números reales,* $\mathbb{C}$ *de los números complejos,* $\mathbb{Z}_n$ *de los enteros módulo* n *y* $k[X]$ *de los polinomios con coeficientes en un cuerpo* k*, son monoides abelianos vía el producto. Salvo* $\mathbb{N}$ *todos los demás también lo son vía la suma.*

EJEMPLO 1.5. *El conjunto* $\mathrm{Fun}(X, X)$*, de las funciones de un conjunto* X *en si mismo, es un monoide vía la composición, que sólo es abeliano cuando el cardinal de* X *es menor o igual que* 1*.*

EJEMPLO 1.6. *Para cada número natural* n*, el conjunto* $\mathrm{M_n}(k)$ *de las matrices de* $n \times n$ *con coeficientes en un cuerpo* k*, es un monoide cuyo neutro es la matriz identidad, vía el producto.*

EJEMPLO 1.7. *El conjunto* $\mathrm{End}_k(V)$*, de los endomorfismos de un* k*-espacio vectorial* V*, es un monoide cuyo neutro es la función identidad, vía la composición. Si* $\dim_k(V) \geq 2$*, entonces* $\mathrm{End}_k(V)$ *no es abeliano.*

2. Submonoides

Un subconjunto T de un monoide S es un *submonoide* de S si es cerrado para el producto y $1 \in T$. Es evidente que entonces T es un monoide. Los submonoides *triviales* de S son S y $\{1\}$. Por simplicidad, de ahora en más escribiremos 1 en lugar de $\{1\}$ para denotar al segundo. Un submonoide de S es *propio* si es distinto de S. Es claro que la intersección de una familia arbitraria de submonoides de S es un submonoide de S. Por ejemplo, dada una familia U de elementos de S, la intersección de los submonoides de S que incluyen a U es el mínimo submonoide $\langle U \rangle_{\mathrm{M}}$ de S que contiene a U, el cual es llamado el *submonoide*

de S generado por U. Si $S = \langle U\rangle_{\mathrm{M}}$, decimos que U *genera* a S. Siguiendo una práctica usual, escribiremos $\langle u_1, \ldots, u_{\mathrm{n}}\rangle_{\mathrm{M}}$ en lugar de $\langle\{u_1, \ldots, u_{\mathrm{n}}\}\rangle_{\mathrm{M}}$. Esto se debe simplemente a una cuestión de estética. Un monoide S es *finitamente generado* si tiene un subconjunto finito U que lo genera. Es obvio que si S es finito, entonces es finitamente generado. Por último decimos que S es *cíclico* si existe $s \in S$ tal que $S = \langle s\rangle_{\mathrm{M}}$. Dejamos a cargo del lector comprobar que, si adoptamos la convención de que el producto vacío da 1, entonces, para cada familia U de elementos de S,

$$\langle U\rangle_{\mathrm{M}} = \{u_1 \cdots u_n : n \geq 0 \text{ y } u_i \in U\}.$$

Para cada par de subconjuntos K y L de un monoide S, denotamos con KL al subconjunto de S formado por todos los productos kl con $k \in K$ y $l \in L$. Por supuesto, escribiremos sK y Ks en lugar de $\{s\}K$ y $K\{s\}$, respectivamente. En general $KL \subseteq \langle K \cup L\rangle_{\mathrm{M}}$, y si $1 \in K \cap L$, entonces $K \cup L \subseteq KL$. Asimismo, es evidente que $(KL)M = K(LM)$ para toda terna K, L y M de subconjuntos de S, por lo que es innecesario escribir los paréntesis.

Proposición 2.1. *Si K y L son submonoides de S, entonces KL es un submonoide de S si y sólo si $LK \subseteq KL$.*

Demostración. Supongamos que $LK \subseteq KL$. Como $1 \in KL$, para probar que KL es un submonoide de S, basta observar que

$$KLKL \subseteq KKLL = KL.$$

Recíprocamente, si KL es un submonoide de S, entonces $LK \subseteq KLKL = KL$. □

Dada una familia $\{S_i\}_{i\in I}$ de submonoides de S existe un mínimo submonoide $\bigvee_{i\in I} S_i$ de S que contiene a $\bigcup_{i\in I} S_i$, el cual es llamado el *supremo* de $\{S_i\}_{i\in I}$. Un cálculo sencillo muestra que

$$\bigvee_{i\in I} S_i = \left\langle \bigcup_{i\in I} S_i \right\rangle_{\mathrm{M}} = \{s_{i_1} \cdots s_{i_n} : n \geq 0,\ i_1, \ldots, i_n \in I,\ i_j \neq i_{j+1} \text{ y } s_{i_j} \in S_{i_j}\}.$$

Notemos que si $S_iS_j = S_jS_i$ para todo $i, j \in I$ e I es un conjunto provisto de un orden total, entonces

$$\bigvee_{i\in I} S_i = \{s_{i_1} \cdots s_{i_n} : n \geq 0,\ i_1 < \cdots < i_n \in I \text{ y } s_{i_j} \in S_{i_j}\}.$$

2.1. Ejemplos

Para cada monoide S, el subconjunto formado por los elementos de S que son cancelables a izquierda es un submonoide de S. Por supuesto que también lo son el subconjunto formado por los elementos que son cancelables a derecha, el formado por los elementos cancelables y el subconjunto $S^\times$ de las unidades de S.

3. Morfismos de monoides

Un *morfismo de monoides* $\varphi\colon S \to S'$ es una terna (S, φ, S'), formada por dos monoides S y S' y una función φ del conjunto subyacente de S en el de S', que satisface:

$$\varphi(1) = 1 \quad \text{y} \quad \varphi(st) = \varphi(s)\varphi(t) \text{ para todo } s, t \in S.$$

Los monoides S y S' son respectivamente el *dominio* y el *codominio* de φ. La razón para adoptar esta definición y no limitarnos simplemente a considerar la función φ, es que tomar la terna (S, φ, S') nos permite recuperar los monoides S y S' (y no sólo sus conjuntos subyacentes) en términos del morfismo, como el dominio y codominio del mismo. Si no hay peligro de confusión, a veces nos tomaremos la libertad de escribir frases como "φ es un morfismo de monoides", sin hacer referencia ni al dominio ni al codominio. El requisito de que $\varphi(1)$ sea igual a 1 puede debilitarse. Es suficiente pedir que $\varphi(1)$ sea cancelable a izquierda o a derecha. Para comprobarlo basta cancelar $\varphi(1)$ en la igualdad $\varphi(1) = \varphi(1)\varphi(1)$.

Si $\varphi\colon S \to S'$ es un morfismo y $s \in S$ tiene orden n, entonces el orden de $\varphi(s)$ divide a n, porque

$$\varphi(s)^n = \varphi(s^n) = 1.$$

Los ordenes de s y de $\varphi(s)$ son iguales cuando φ es inyectivo, debido a que si este es el caso,

$$\varphi(s^m) = \varphi(s)^m = 1 = \varphi(1) \Rightarrow s^m = 1.$$

De la definición de morfismo se sigue inmediatamente que si t es inversa a izquierda de s, entonces $\varphi(t)$ es inversa a izquierda de $\varphi(s)$. En particular, si s es inversible, entonces $\varphi(s)$ también lo es y $\varphi(s)^{-1} = \varphi(s^{-1})$.

Son ejemplos de morfismos de monoides

- la identidad $\mathrm{id}_S\colon S \to S$,
- la inclusión canónica $i\colon T \to S$, de un submonoide T de S en S,
- la composición $\psi \circ \varphi\colon S \to S''$, de morfismos de monoides $\varphi\colon S \to S'$ y $\psi\colon S' \to S''$,
- la aplicación $\varphi\colon S \to S'$, definida por $\varphi(s) := 1$ para todo $s \in S$, cualesquiera sean los monoides S y S'.

Es evidente que si $\varphi\colon S \to S'$ es un morfismo de monoides, entonces $\varphi(KL) = \varphi(K)\varphi(L)$ para todo par de subconjuntos K y L de S.

Un *endomorfismo* de S es un morfismo con dominio y codominio S. Un ejemplo es id_S. Un morfismo $\varphi\colon S \to S'$ es un *isomorfismo* si existe un morfismo $\varphi^{-1}\colon S' \to S$, necesariamente único, llamado la *inversa* de φ, tal que $\varphi^{-1} \circ \varphi = \mathrm{id}_S$ y $\varphi \circ \varphi^{-1} = \mathrm{id}_{S'}$. Es fácil ver que esto ocurre si y sólo si φ es biyectiva. Dos monoides S y S' son *isomorfos* si hay un isomorfismo de S en S'. En ese caso escribimos $S \simeq S'$. Un *automorfismo* de S es un endomorfismo de S que es un isomorfismo. Los símbolos $\mathrm{Hom_M}(S, S')$, $\mathrm{Iso_M}(S, S')$, $\mathrm{End_M}(S)$ y $\mathrm{Aut_M}(S)$ denotan respectivamente a los conjuntos de morfismos de S en S', isomorfismos de S en S', endomorfismos de S y automorfismos de S. Es obvio que $\mathrm{End_M}(S)$ es un monoide (cuyo elemento neutro es la función identidad) vía la composición. Decimos que un morfismo $\varphi\colon S \to S'$ es un *monomorfismo* si $\varphi \circ \psi = \varphi \circ \psi' \Rightarrow \psi = \psi'$ para todo par de morfismos de monoides $\psi, \psi'\colon S'' \to S$ con codominio S, un *epimorfismo* si $\psi \circ \varphi = \psi' \circ \varphi \Rightarrow \psi = \psi'$ para todo par de morfismos de monoides $\psi, \psi'\colon S' \to S''$ con dominio S', una *sección* si existe $\psi\colon S' \to S$ tal que $\psi \circ \varphi = \mathrm{id}_S$ y una *retracción* si existe $\zeta\colon S' \to S$ tal que $\varphi \circ \zeta = \mathrm{id}_{S'}$. Como el lector podrá comprobar sin dificultad, los monomorfismos, epimorfismos, secciones y retracciones son cerrados bajo la composición, toda retracción es sobreyectiva, toda sección es inyectiva, todo morfismo inyectivo es un monomorfismo y todo morfismo sobreyectivo es un epimorfismo. Además un morfismo $\varphi\colon S \to S'$ es un isomorfismo si y sólo si es una sección y un epimorfismo, y esto ocurre si y sólo si es una retracción y un monomorfismo (copie la prueba de la Proposición 1.1). Una propiedad apenas un poco más difícil de verificar es que todo

monomorfismo $\varphi\colon S \to S'$ es inyectivo. Para comprobar esto supongamos que $\varphi(r) = \varphi(s)$ y consideremos los morfismos de monoides $\psi, \psi'\colon \mathbb{N}_0 \to S$, definidos por

$$\psi(n) := r^n \quad \text{y} \quad \psi'(n) := s^n.$$

Como

$$(\varphi \circ \psi)(n) = \varphi(r^n) = \varphi(r)^n = \varphi(s)^n = \varphi(s^n) = (\varphi \circ \psi')(n),$$

y φ es un monomorfismo, obtenemos que $\psi = \psi'$ y, por lo tanto, $r = \psi(1) = \psi'(1) = s$. Por último, para cada par $\varphi\colon S \to S'$ y $\psi\colon S' \to S''$ de morfismos,

1. Si $\psi \circ \varphi$ es una sección o un monomorfismo, entonces también lo es φ.
2. Si $\psi \circ \varphi$ es una retracción, un epimorfismo o un morfismo sobreyectivo, entonces también lo es ψ.

EJEMPLO 3.1. *Supongamos que X es un subconjunto de Y. Definamos*

$$i_*\colon \operatorname{Fun}(X, X) \to \operatorname{Fun}(Y, Y)$$

por

$$i_*(\sigma)(x) := \begin{cases} \sigma(x) & \text{si } x \in X, \\ x & \text{si } x \notin X. \end{cases}$$

Es evidente que i es un morfismo inyectivo de monoides.

EJEMPLO 3.2. *Supongamos que $i\colon X \to Y$ es una biyección. Definamos*

$$i_*\colon \operatorname{Fun}(X, X) \to \operatorname{Fun}(Y, Y)$$

por $i_*(\sigma) := i \circ \sigma \circ i^{-1}$. Es evidente que i_* es un isomorfismo de monoides.

EJEMPLO 3.3. *Supongamos que $i\colon X \to Y$ es una función inyectiva. Definamos*

$$i_*\colon \operatorname{Fun}(X, X) \to \operatorname{Fun}(Y, Y)$$

por

$$i_*(\sigma)(y) := \begin{cases} i(\sigma(x)) & \text{si } y = i(x), \\ y & \text{si } y \notin i(X). \end{cases}$$

Es fácil ver que:

- *i_* es un morfismo inyectivo de monoides cuya imagen es el conjunto de las funciones de Y en si mismo que dejan fijos a los elementos que están fuera de $i(X)$.*
- *Si X es un subconjunto de Y e i es la inclusión canónica de X en Y recuperamos la definición dada en el Ejemplo 3.1, mientras que si i es una biyección recuperamos la dada en el Ejemplo 3.2.*
- *Si $j\colon Y \to Z$ es otra función inyectiva, entonces $(j \circ i)_* = j_* \circ i_*$.*

4. Grupos

Un *grupo* G es un monoide en el cual todos los elementos son inversibles. Claramente G es un grupo si y sólo si G^{op} lo es.

PROPOSICIÓN 4.1. *Un monoide G es un grupo si y sólo si para cada par g, h de elementos de G, las ecuaciones $gx = h$ y $xg = h$ tienen solución única en G.*

Demostración. Si G es un grupo, entonces $x = g^{-1}h$ es la única solución de $gx = h$ y $x = hg^{-1}$ es la única solución de $xg = h$. La recíproca se sigue inmediatamente de que G es un grupo si y sólo si las ecuaciones $gx = 1$ y $xg = 1$ tienen solución. □

Proposición 4.2. *Un semigrupo G es un grupo si y sólo si tiene un neutro a izquierda e, y para cada $g \in G$ hay un $g' \in G$ tal que $g'g = e$.*

Demostración. Es indiscutible que todo grupo satisface las condiciones requeridas en el enunciado. Recíprocamente, si estas se satisfacen, entonces

$$gg' = e(gg') = ((g')'g')(gg') = (g')'((g'g)g') = (g')'(eg') = (g')'g' = e$$

y

$$ge = g(g'g) = (gg')g = eg = g,$$

para todo $g \in G$. □

Nota 4.3. *Otra demostración es la siguiente: Tomemos $g \in G$ arbitrario. Entonces*

$$g'(ge) = (g'g)e = ee = e = g'g.$$

Cancelando g' (lo que puede hacerse por el Ejercicio 1.3) obtenemos que $ge = g$. En consecuencia e también es neutro a derecha de G. Para finalizar la prueba notemos ahora que como g y $(g')'$ son inversos a izquierda y derecha de g' respectivamente, necesariamente $(g')' = g$ y, por lo tanto, $gg' = 1$.

Si en la proposición anterior G es un semigrupo finito con un neutro a izquierda e, entonces para concluir que G es un grupo es suficiente pedir que cada elemento $g \in G$ sea cancelable a derecha. En efecto, si g cancelable a derecha, entonces r_g es inyectiva y, por lo tanto, como G es finito, sobreyectiva. En particular existe $g' \in G$ tal que $g'g = e$.

Ejemplo 4.4. *El submonoide $S^\times$, de los elementos inversibles de un monoide S, es un grupo llamado el* grupo de unidades *de S. Por ejemplo, si S es un monoide, entonces $\mathrm{Aut}_{\mathrm{M}}(S)$ es el grupo de unidades de $\mathrm{End}_{\mathrm{M}}(S)$.*

Ejemplo 4.5. *Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$ y $k[X]$, donde k es un cuerpo, son grupos abelianos vía la suma. También lo son $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$, $\mathbb{Z}_n^\times$ y $k[X]^\times$ vía el producto.*

Ejemplo 4.6. *Consideremos un k-espacio vectorial V. El* grupo lineal general $\mathrm{GL}(V)$ *es el grupo de unidades del anillo de endomorfismos $\mathrm{End}_k(V)$. Este grupo es abeliano si y sólo si $\dim_k(V) = 1$.*

Ejemplo 4.7. *El grupo $\mathrm{GL}(n, k)$ es el grupo de unidades del anillo $\mathrm{M}_n(k)$, de matrices de $n \times n$ con coeficiente en un cuerpo k. Este grupo es abeliano si y sólo si $n = 1$.*

Ejemplo 4.8. *Una* permutación *de un conjunto no vacío X es una función biyectiva $\varphi\colon X \to X$. El conjunto S_X, de las permutaciones de X, es un grupo vía la operación dada por la composición de funciones. Notemos que S_X es el grupo de unidades de $\mathrm{Fun}(X, X)$. Cuando $|X| \geq 3$ este grupo no es conmutativo. Para comprobarlo es suficiente considerar $x_1, x_2, x_3 \in X$ y exhibir dos permutaciones σ y τ de X que se restringen a la identidad sobre $X \setminus \{x_1, x_2, x_3\}$ y no conmutan. Por ejemplo, podemos tomar*

$$\sigma(x_1) := x_2, \quad \sigma(x_2) := x_3, \quad \sigma(x_3) := x_1, \quad \tau(x_1) := x_2, \quad \tau(x_2) := x_1 \quad y \quad \tau(x_3) := x_3.$$

Cuando X es el conjunto $\{1, 2, \ldots, n\}$ de los primeros n números naturales, escribimos S_n en lugar de S_X. Es un ejercicio fácil de combinatoria probar que S_n tiene $n!$ elementos.

Decimos que un grupo G tiene *exponente finito* si existe $n \in \mathbb{N}$ tal que $g^n = 1$ para todo $g \in G$. En ese caso, al mínimo n que satisface esta condición lo llamamos el *exponente* de G. Se comprueba fácilmente que este número es el mínimo de los múltiplos comunes de los órdenes de los elementos de G. Cuando no existe un tal n, decimos que G tiene *exponente infinito*. Por supuesto que si esto ocurre G no puede ser finito.

EJERCICIO 4.9. *Pruebe que si un grupo G tiene exponente 2, entonces es abeliano.*

5. Subgrupos

Un submonoide de un grupo G es un *subgrupo* de G si es un grupo. Escribiremos $H \leq G$ para señalar que H es un subgrupo de G. Se comprueba sin dificultad que para cada subconjunto no vacío H de G las siguientes afirmaciones son equivalentes:

1. $H \leq G$.
2. $hl \in H$ y $h^{-1} \in H$ para todo $h, l \in H$.
3. $hl^{-1} \in H$ para todo $h, l \in H$.
4. $h^{-1}l \in H$ para todo $h, l \in H$.

Los *subgrupos triviales de G* son 1 y G. Un subgrupo de G es *propio* si es distinto de G. Como la intersección de cualquier familia de subgrupos de G es un subgrupo de G, para cada subconjunto T de G existe un mínimo subgrupo $\langle T \rangle$ de G que contiene a T, el cual es precisamente la intersección de los subgrupos de G que contienen a T. Evidentemente cualquier subgrupo de G que incluya a T debe incluir también a cada producto de una cantidad finita de elementos de T o T^{-1}, donde $T^{-1} := \{t^{-1} : t \in T\}$. Puesto que el conjunto de todos estos productos es un subgrupo de G,

$$\langle T \rangle = \{g_1 \cdots g_n : n \geq 0 \text{ y } g_i \in T \text{ o } g_i^{-1} \in T\}. \tag{1}$$

La principal ventaja de esta descripción respecto de la anterior es que es más concreta, debido a lo cual es más adecuada para hacer cálculos explícitos, e incluso a veces para obtener resultados teóricos. En general $\langle T \rangle_{\mathrm{M}}$ puede estar incluído propiamente en $\langle T \rangle$. Por ejemplo, si $G = \mathbb{Z}$, entonces $\langle \mathbb{N} \rangle_{\mathrm{M}} = \{0\} \cup \mathbb{N}$ y $\langle \mathbb{N} \rangle = \mathbb{Z}$. Sin embargo, si $g \in G$ tiene orden finito y $g \in \langle T \rangle_{\mathrm{M}}$, entonces g^{-1} pertenece a $\langle T \rangle_{\mathrm{M}}$, porque es una potencia de g. En consecuencia, si $T \neq \emptyset$ y todos sus elementos tienen orden finito, $\langle T \rangle_{\mathrm{M}} = \langle T \rangle$. Si $G = \langle T \rangle$, decimos que T *genera a G como grupo* o más simplemente que T *genera* a G. Tal como hicimos con monoides, escribiremos $\langle g_1, \ldots, g_n \rangle$ en lugar de $\langle \{g_1, \ldots, g_n\} \rangle$. Un grupo G es *finitamente generado* si existe un subconjunto finito T de G tal que $G = \langle T \rangle$, y es *cíclico* si existe $g \in G$ tal que $G = \langle g \rangle$. En ese caso, si g tiene orden infinito, entonces la asignación $n \mapsto g^n$ establece una correspondencia biyectiva entre $\mathbb{Z}$ y G, y si g tiene orden finito, entonces

$$G = \{g^0, \ldots, g^{|g|-1}\}$$

tiene $|g|$ elementos. Notemos por último que el supremo $\bigvee_{i \in I} G_i$ de una familia $\{G_i\}_{i \in I}$ de subgrupos de un grupo G (como fue definido para una familia de submonoides de un monoide) es un subgrupo de G.

EJERCICIO 5.1. *Un subgrupo G del grupo aditivo $\mathbb{R}$ es discreto si para cada $g \in G$ existe $\varepsilon > 0$ tal que $G \cap (g - \varepsilon, g + \varepsilon) = \{g\}$. Pruebe que todo grupo discreto es cíclico.*

EJERCICIO 5.2. *Pruebe que:*

1. *Si H y L son subgrupos propios de un grupo G, entonces $G \neq H \cup L$.*
2. *Si H es un subgrupo propio de un grupo G, entonces $G = \langle G \setminus H \rangle$.*

EJEMPLO 5.3. *Los conjuntos $\mathbb{Q}_{>0}$ y $\mathbb{R}_{>0}$ son subgrupos de $\mathbb{Q}^\times$ y $\mathbb{R}^\times$, respectivamente*

EJEMPLO 5.4. *El conjunto $\mathbb{Z}[X]$, de polinomios con coeficientes enteros, es un subgrupo de $\mathbb{Q}[X]$.*

EJEMPLO 5.5. *Consideremos un espacio euclideano E. El* grupo ortogonal de E *es el subgrupo $\mathrm{O}(E)$ de $\mathrm{GL}(E)$, formado por las transformaciones ortogonales de E. El* grupo lineal especial $\mathrm{SO}(E)$ *es el subgrupo de $\mathrm{O}(E)$ formado por las transformaciones ortogonales que tienen determinante 1.*

EJEMPLO 5.6. *El conjunto $\mathrm{SL}(n,k)$, de las matrices de $n \times n$ que tienen determinante 1 con coeficientes en un cuerpo k, es un subgrupo de $\mathrm{GL}(n,k)$.*

EJEMPLO 5.7. *Para cada $n \in \mathbb{N}$, el subconjunto G_n de $\mathbb{C}$, formado por las raíces n-ésimas de la unidad, es un subgrupo de $\mathbb{C}^\times$. También lo es $\mathrm{G}_\infty := \bigcup_{n\in\mathbb{N}} \mathrm{G}_n$.*

La función $\phi\colon \mathbb{N} \to \mathbb{N}$ *de Euler* asigna a cada número natural el cardinal del conjunto de los enteros no negativos menores que él y coprimos con él. En notación simbólica

$$\phi(n) := |\{m : 0 \leq m < n \text{ y } m \text{ es coprimo con } n\}|.$$

Por ejemplo, si p es un número primo, entonces $\phi(p^n) = p^{n-1}(p-1)$ para todo $n \in \mathbb{N}$, porque $\{0, \ldots, p^n - 1\}$ tiene p^n elementos, de los cuales p^{n-1} son múltiplos de p. En general, si $n = p_1^{r_1} \ldots p_s^{r_s}$ es la factorización de n como producto de primos positivos distintos, entonces $\phi(n) = (p_1 - 1)p_1^{r_1-1} \cdots (p_s - 1)p_s^{r_s-1}$.

EJEMPLO 5.8. *Consideremos el ángulo $\theta{:=}2\pi/n$, donde $n{\in}\mathbb{N}$ es mayor que 1. El subgrupo de $\mathrm{GL}(2,\mathbb{R})$ generado por*

$$x := \begin{pmatrix} \cos\theta & \operatorname{sen}\theta \\ -\operatorname{sen}\theta & \cos\theta \end{pmatrix} \qquad e \qquad y := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

es, por definición, el grupo diedral D_n. *Un cálculo directo muestra que*

$$x^i = \begin{pmatrix} \cos i\theta & \operatorname{sen} i\theta \\ -\operatorname{sen} i\theta & \cos i\theta \end{pmatrix}, \quad y^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad e \quad yx^i = \begin{pmatrix} \cos i\theta & \operatorname{sen} i\theta \\ \operatorname{sen} i\theta & -\cos i\theta \end{pmatrix} = x^{-i}y.$$

De esto se sigue fácilmente que x e y satisfacen las relaciones

$$x^n = 1, \quad y^2 = 1 \quad e \quad yxy^{-1} = x^{-1}$$

y que D_n consiste de los $2n$ elementos $1, x, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y$. Notemos además que:

- *Los elementos $x^i y$ tienen orden 2.*
- *Los elementos x^i tienen orden $n/(n:i)$, donde $(n:i)$ denota al máximo divisor común de n e i. Debido a esto, para cada divisor d de n hay $\phi(d)$ elementos de orden d de la forma x^i.*

En particular D_n tiene n elementos de orden 2 si n es impar y $n+1$ si n es par.

EJEMPLO 5.9. *Tomemos* $w := e^{i\pi/n}$ *donde* $n \in \mathbb{N}$ *es mayor que* 1. *Es claro que* $w \in \mathbb{C}$ *es una raíz de la unidad de orden* $2n$. *El subgrupo de* $\mathrm{GL}(2,\mathbb{C})$ *generado por*

$$x := \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix} \qquad e \qquad y := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

es el grupo cuaterniónico generalizado H_n. *Un cálculo directo muestra que*

$$x^i = \begin{pmatrix} w^i & 0 \\ 0 & w^{-i} \end{pmatrix}, \quad y^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = x^n \quad e \quad yx^i = \begin{pmatrix} 0 & w^{-i} \\ -w^i & 0 \end{pmatrix} = x^{-i}y. \tag{2}$$

Por consiguiente, x *e* y *satisfacen las relaciones*

$$x^n = y^2 \qquad e \qquad yxy^{-1} = x^{-1}. \tag{3}$$

Claramente por (2) *también vale* $x^{2n} = 1$. *Sin embargo queremos hacer notar que esto último es consecuencia de la igualdades de* (3), *ya que de ellas se sigue que*

$$x^n = yy^2y^{-1} = yx^ny^{-1} = x^{-n}.$$

Así, H_n *consiste de los* $4n$ *elementos* $1, x, \ldots, x^{2n-1}, y, xy, \ldots, x^{2n-1}y$. *Es útil observar que:*

- *Los elementos* x^iy *tienen orden* 4.
- *Los elementos* x^i *tienen orden* $2n/(2n:i)$. *En consecuencia, para cada divisor* d *de* $2n$ *hay* $\phi(d)$ *elementos de orden* d *de la forma* x^i.

En particular, H_n *tiene un solo elemento de orden* 2, *y tiene* $2n$ *elementos de orden* 4 *si* n *es impar, y* $2n+2$ *si* n *es par.*

5.1. Subgrupos de un grupo cíclico

Supongamos que $G = \langle g \rangle$ es cíclico infinito. Entonces la asignación $n \mapsto \langle g^n \rangle$ establece una correspondencia biyectiva entre $\mathbb{N}_0$ y el conjunto de los subgrupos de G. En efecto, es claro que esta asignación es inyectiva pues $\langle g^n \rangle \neq \langle g^m \rangle$ si $n \neq m$ y que $\langle g^0 \rangle = 1$. Veamos a continuación que también es sobreyectiva. Para ello debemos probar que si $H \neq 1$ es un subgrupo de G, entonces $H = \langle g^{n_0} \rangle$, donde n_0 el mínimo natural tal que $g^{n_0} \in H$. Supongamos, por lo tanto, que $g^m \in H$ y escribamos $m = n_0q + r$ con $0 \leq r < n_0$. Como

$$g^r = g^{m-n_0q} = g^m(g^{n_0})^{-q} \in H.$$

se sigue de la minimalidad de n_0 que $r = 0$ y, en consecuencia, $n_0 \mid m$.

Supongamos ahora que $G = \langle g \rangle$ es cíclico finito. Entonces la asignación $n \mapsto \langle g^n \rangle$ define una correspondencia biyectiva entre el conjunto de los divisores positivos de $|g|$ y el de los subgrupos de G y, además, para todo divisor positivo n de $|g|$, el orden de $\langle g^n \rangle$ es $|g|/n$. En efecto, es evidente que si $n \mid |g|$, entonces el orden de $\langle g^n \rangle$ es $|g|/n$, lo que muestra además que la asignación que estamos considerando es inyectiva. Veamos a continuación que también es sobreyectiva. Para ello tomemos un subgrupo H de G y consideremos el mínimo número natural n_0 tal que $g^{n_0} \in H$. Si $g^m \in H$ y $m = n_0q + r$ con $0 \leq r < n_0$, entonces

$$g^r = g^{m-n_0q} = g^m(g^{n_0})^{-q} \in H,$$

por lo que $r = 0$ y $H = \langle g^{n_0} \rangle$. De paso, notemos que como $g^{|g|} = 1 \in H$, de la cuenta anterior se sigue que n_0 divide a $|g|$. Así la cantidad de subgrupos de un grupo cíclico finito $\langle g \rangle$, es igual a la cantidad de divisores positivos de $|g|$. Llamaremos a esta cantidad $\tau(|g|)$. Notemos por último que si g tiene orden finito, entonces para cada $n \in \mathbb{Z}$ arbitrario, $\langle g^n \rangle = \langle g^{(|g|:n)} \rangle$ y,

en particular, g^n es un generador de $\langle g\rangle$ si y sólo si n es coprimo con $|g|$. En efecto, dado que existen $r, s \in \mathbb{Z}$ tales que $(|g| : n) = r|g| + sn$,

$$g^{(|g|:n)} = (g^{|g|})^r (g^n)^s = (g^n)^s \in \langle g^n\rangle,$$

y, por lo tanto, $\langle g^{(|g|:n)}\rangle \subseteq \langle g^n\rangle$. Pero es obvio que también vale la inclusión recíproca.

NOTA 5.10. *La función $\tau\colon \mathbb{N} \to \mathbb{N}$ satisface la siguiente propiedad: Si $n = p_1^{r_1} \dots p_s^{r_s}$ es la factorización de n como producto de primos positivos distintos, entonces*

$$\tau(n) = (r_1 + 1) \dots (r_s + 1).$$

5.2. Subgrupos de los grupos diedrales y cuaterniónicos

A continuación calculamos los subgrupos de D_n y H_n. Usaremos libremente las notaciones introducidas en los Ejemplos 5.8 y 5.9. Consideremos primero un subgrupo H de D_n. Si $H \subseteq \langle x\rangle$, entonces $H = \langle x^i\rangle$, donde i es un divisor de n. Supongamos ahora que $H \nsubseteq \langle x\rangle$ y que j es el mínimo entero no negativo tal que $x^j y \in H$. Denotemos con i al único divisor positivo de n tal que $H \cap \langle x\rangle = \langle x^i\rangle$. Claramente

$$\bigcup_{0\le h<n/i} \{x^{hi}, x^{j+hi}y\} \subseteq H,$$

lo que muestra en particular que $0 \le j < i$. Es fácil ver que la unión que aparece a la izquierda de esta inclusión es igual a $\langle x^i, x^j y\rangle$. Afirmamos que este grupo coincide con H. En efecto si $x^{j'}y \in H$, entonces $x^{j'-j} = x^{j'}y(x^j y)^{-1} \in H \cap \langle x\rangle$ y, en concecuencia, $x^{j'-j} = x^{hi}$ para algún $0 \le h < n/i$, lo que implica que $x^{j'}y = x^{j+hi}y \in \langle x^i, x^j y\rangle$. Claramente la aplicación que a cada par (j, i), donde i es un divisor positivo de n y donde j es un entero no negativo menor que i, le asigna $\langle x^i, x^j y\rangle$, es inyectiva. Por lo tanto la cantidad de subgrupos de D_n que no están incluídos en $\langle x\rangle$, es igual a la suma de los divisores positivos de n. Llamaremos a esta suma $\sigma(n)$. En consecuencia, la cantidad de subgrupos de D_n es $\tau(n) + \sigma(n)$. Notemos finalmente que si m divide a n, entonces $D_m = \langle x^{n/m}, y\rangle$ es un subgrupo de D_n.

Tomemos ahora un subgrupo H de H_n. Si $H \subseteq \langle x\rangle$, entonces $H = \langle x^i\rangle$, donde i es un divisor de $2n$. Supongamos ahora que $H \nsubseteq \langle x\rangle$ y que j el mínimo entero no negativo tal que $x^j y \in H$. Denotemos con i al único divisor positivo de $2n$ tal que $H \cap \langle x\rangle = \langle x^i\rangle$. Dado que $x^n = y^2 = x^j y x^j y \in H \cap \langle x\rangle$, necesariamente $i \mid n$. Claramente

$$\bigcup_{0\le h<2n/i} \{x^{hi}, x^{j+hi}y\} \subset H,$$

lo que muestra en particular que $0 \le j < i$. Es fácil ver que la unión que aparece a la izquierda de esta inclusión es igual a $\langle x^i, x^j y\rangle$. Afirmamos que este grupo coincide con H. En efecto si $x^{j'}y \in H$, entonces $x^{j'-j} = x^{j'}y(x^j y)^{-1} \in H \cap \langle x\rangle$ y, en concecuencia, $x^{j'-j} = x^{hi}$ para algún $0 \le h < 2n/i$, lo que implica que $x^{j'}y = x^{j+hi}y \in \langle x^i, x^j y\rangle$. De la misma manera que para D_n, la aplicación que a cada par (j, i), donde i es un divisor positivo de n y donde j es un entero no negativo menor que i, le asigna $\langle x^i, x^j y\rangle$, es inyectiva. Por lo tanto la cantidad de subgrupos de H_n que no están incluídos en $\langle x\rangle$, es igual a $\sigma(n)$. En consecuencia, la cantidad de subgrupos de H_n es $\tau(2n) + \sigma(n)$. Notemos finalmente que si m divide a n, entonces $H_m = \langle x^{n/m}, y\rangle$ es un subgrupo de H_n.

NOTA 5.11. *La función $\sigma\colon \mathbb{N} \to \mathbb{N}$ satisface la siguiente propiedad: Si $n = p_1^{r_1} \dots p_s^{r_s}$ es la factorización de n como producto de primos positivos distintos, entonces*

$$\sigma(n) = \frac{p_1^{r_1+1} - 1}{p_1 - 1} \cdots \frac{p_s^{r_s+1} - 1}{p_s - 1}.$$

6. Coclases a izquierda y a derecha

Recordemos que para cada par de subconjuntos K y L de un monoide S, denotamos con KL al subconjunto de S formado por todos los productos kl con $k \in K$ y $l \in L$, y, que si S es un grupo, entonces para cada subconjunto K de S escribimos $K^{-1} := \{k^{-1} : k \in K\}$. Es obvio que $(K^{-1})^{-1} = K$ y que $(KL)^{-1} = L^{-1}K^{-1}$. Fijemos ahora un subgrupo H de un grupo G. Una *coclase a izquierda* de H en G es un subconjunto de G que tiene la forma gH para algún $g \in G$. Dos coclases a izquierda que no son disjuntas coinciden. En efecto, si $gh = g'h'$ con $h, h' \in H$, entonces $gH = ghH = g'h'H = g'H$. En consecuencia G es la unión disjunta de las coclases a izquierda de H en G. Asimismo, como la aplicación

$$\begin{array}{ccc} H & \longrightarrow & gH \\ h & \longmapsto & gh \end{array},$$

es biyectiva, todas las coclases a izquierda tienen el mismo cardinal. Estos argumentos prueban que vale el siguiente:

TEOREMA 6.1 (Lagrange). *Para cada $H \leq G$, los ordenes de H y G están relacionados por la igualdad*

$$|G| = |G : H||H|, \tag{4}$$

en la que el símbolo $|G : H|$, llamado el índice de H en G, *denota a la cantidad de coclases a izquierda de H en G.*

El mismo razonamiento, aplicado a las coclases a derecha de H en G (las cuales son los subconjuntos de G de la forma Hg para algún $g \in G$) prueba que estas parten G y satisfacen una fórmula similar a (4). Más aún, como la aplicación $gH \mapsto Hg^{-1}$ (que está bien definida pues de $g_1H = g_2H$ se sigue que $Hg_1^{-1} = H^{-1}g_1^{-1} = (g_1H)^{-1} = (g_2H)^{-1} = H^{-1}g_2^{-1} = Hg_2^{-1}$) es una función biyectiva del conjunto G/H de las coclases a izquierda de H en G, en el conjunto $G\backslash H$ de las coclases a derecha H en G, ambos tienen el mismo cardinal.

EJERCICIO 6.2. *Calcule las coclases a izquierda y a derecha de $\langle y \rangle$ en D_n y muestre que en general no coinciden.*

EJERCICIO 6.3. *Calcule las coclases a izquierda y a derecha de $\langle y \rangle$ en H_n y muestre que en general no coinciden.*

OBSERVACIÓN 6.4. *Del teorema de Lagrange se sigue inmediatamente que si H y L son subgrupos finitos de un grupo G, entonces $|H \cap L|$ divide a $(|H| : |L|)$. En particular si $|H|$ y $|L|$ son coprimos, entonces $H \cap L = 1$.*

COROLARIO 6.5. *Si G es finito, entonces el exponente de G divide al orden de G.*

DEMOSTRACIÓN. Tomemos $g \in G$ arbitrario. Como $|g| = |\langle g \rangle|$ se sigue del teorema de Lagrange que $|g|$ divide a $|G|$. En consecuencia el exponente de G también divide a $|G|$. □

COROLARIO 6.6. *Si un grupo G tiene orden primo, entonces es cíclico.*

DEMOSTRACIÓN. Tomemos $g \in G \setminus \{1\}$. Como $|g| > 1$ y $|G|$ es primo se sigue del teorema de Lagrange que $|g| = |G|$. En consecuencia G está generado por cada $g \in G \setminus \{1\}$. □

OBSERVACIÓN 6.7. *Debido al teorema de Lagrange si un grupo finito G tiene elementos de orden 2, entonces $|G|$ es par. En realidad también vale la recíproca. Para comprobarlo supongamos que $|G|$ es par y consideremos la partición*

$$G = \{1\} \cup \{g \in G : |g| = 2\} \cup \{g \in G : |g| > 2\}.$$

Como $|g| = 2$ si y sólo si $g \neq 1$ y $g^{-1} = g$, el conjunto $\{g \in G : |g| > 2\}$ tiene una cantidad par de elementos (estos se pueden agrupar de a pares, cada uno con su inverso). Por lo tanto $|\{g \in G : |g| = 2\}|$ es impar y, en particular, $\{g \in G : |g| = 2\} \neq \emptyset$. El resultado obtenido en la presente observación será generalizado más adelante.

El resultado que sigue generaliza la igualdad (4).

TEOREMA 6.8. *Si K y H son subgrupos de un grupo G y $K \subseteq H$, entonces*

$$|G : K| = |G : H||H : K|.$$

DEMOSTRACIÓN. Escribamos G y H como uniones disjuntas

$$G = \bigcup_i g_i H \quad \text{y} \quad H = \bigcup_j h_j K,$$

de coclases a izquierda de H en G y de K en H, respectivamente. Reemplazando H en la primera igualdad por la expresión en el lado derecho de la segunda, vemos que $G = \bigcup_{i,j} g_i h_j K$. Debemos probar que esta unión es disjunta. Supongamos que $g_i h_j K = g_{i'} h_{j'} K$. Multiplicando por H a la derecha obtenemos que $g_i H = g_{i'} H$ y, por lo tanto $i = i'$. Pero entonces $h_j K = h_{j'} K$ y así también $j = j'$. □

OBSERVACIÓN 6.9. *Del teorema anterior se sigue que si H, L y K son subgrupos de un grupo G, tales que $K \subseteq H \cap L$ y $|H : K|$ y $|L : K|$ son finitos, entonces*

$$|H \cap L : K| \text{ divide a } (|H : K| : |L : K|).$$

En particular si $|H : K|$ y $|L : K|$ son coprimos, entonces $H \cap L = K$.

OBSERVACIÓN 6.10. *Del teorema anterior se sigue también que si H y L son subgrupos de un grupo y $|G : H \cap L|$ es finito, entonces*

$$[|G : H| : |G : L|] \text{ divide a } |G : H \cap L|,$$

donde $[|G : H| : |G : L|]$ denota al mínimo múltiplo común de $|G : H|$ y $|G : L|$. Así, si $|G : H|$ y $|G : L|$ son coprimos, entonces $|G : H \cap L| = |G : H||G : L|$.

OBSERVACIÓN 6.11. *Si la intersección de una familia $(g_i H_i)_{i \in I}$ de coclases a izquierda de un grupo G no es vacía, entonces es una coclase a izquierda de la intersección de los H_i's. En efecto, si $g \in \bigcap_{i \in I} g_i H_i$, entonces $g H_i = g_i H_i$ para todo $i \in I$ y, por lo tanto,*

$$\bigcap_{i \in I} g_i H_i = g \bigcap_{i \in I} H_i.$$

OBSERVACIÓN 6.12. *Consideremos dos subgrupos H y L de un grupo G. Dado que, para todo $h, h' \in H$,*

$$hL = h'L \Leftrightarrow h^{-1}h' \in L \Leftrightarrow h^{-1}h' \in H \cap L \Leftrightarrow h(H \cap L) = h'(H \cap L),$$

la aplicación

$$\begin{array}{c} H/(H \cap L) \xrightarrow{\varsigma} G/L \ , \\ h(H \cap L) \longmapsto hL \end{array}$$

es inyectiva. Dado que además

$$\operatorname{Im}\varsigma = \{hL : h \in H\} \qquad y \qquad |G : H \cap L| = |G : H||H : H \cap L|,$$

se sigue de esto que

$$|H : H \cap L| = |HL : L| \qquad y \qquad |G : H \cap L| = |G : H||HL : L|, \tag{5}$$

donde $|HL : L|$ denota al cardinal del conjunto de coclases a izquierda de L que están incluidas en HL. En consecuencia

$$|H : H \cap L| \leq |G : L| \qquad y \qquad |G : H \cap L| \leq |G : H||G : L|. \tag{6}$$

Notemos además que

$$|HL| = |HL : L||L| = |H : H \cap L||L|, \tag{7}$$

y que si HL es un subgrupo de G, entonces

$$|H : H \cap L||G : HL| = |G : L| \qquad y \qquad |G : H \cap L||G : HL| = |G : H||G : L|, \tag{8}$$

de manera que las desigualdades de (6) *se transforman en igualdades cuando $HL = G$. De la presente exposición se sigue que:*

- *$|G : H \cap L|$ es finito si y sólo si $|G : H|$ y $|G : L|$ lo son.*
- *Si $|G : L|$ es finito y $|H : H \cap L| = |G : L|$, entonces $HL = G$.*
- *Si $|G : H|$ es finito y $|G : H \cap L| = |G : H||G : L|$, entonces $|H : H \cap L| = |G : L|$.*

7. Una caracterización de los grupos cíclicos finitos

En la Sección 5.1 vimos que si G es un grupo cíclico de orden n, entonces G tiene $\phi(n)$ generadores y que si d divide a n, entonces G tiene exactamente un subgrupo de orden d (que además es cíclico). El principal objetivo de esta sección es mostrar que lo último caracteriza a los grupos cíclicos finitos.

Para cada grupo cíclico G vamos a denotar con $\operatorname{gen}(G)$ al conjunto de sus generadores.

LEMA 7.1. *Cada grupo G es la unión disjunta*

$$G = \bigcup \operatorname{gen}(C),$$

de los generadores de los subgrupos cíclicos C de G.

DEMOSTRACIÓN. Porque cada elemento de G genera un único subgrupo cíclico de G. □

PROPOSICIÓN 7.2. *La igualdad $n = \sum_{d/n} \phi(d)$ vale para cada $n \in \mathbb{N}$.*

Demostración. Como $\mathbb{Z}_n$ tiene exactamente un subgrupo cíclico de orden d, para cada divisor d de n, y dicho subgrupo tiene $\phi(d)$ generadores, se sigue del lema anterior que

$$n = |\mathbb{Z}_n| = \sum_{d/n} \phi(d),$$

como queríamos. □

Teorema 7.3. *Un grupo G de orden n es cíclico si y sólo si tiene a lo sumo un subgrupo de orden d, para cada divisor d de n.*

Demostración. Ya sabemos que si G es cíclico, entonces tiene exactamente un subgrupo de orden d para cada divisor d de n. Veamos que vale la recíproca. Supongamos que G es un grupo de orden n. Por el Lema 7.1 y la Proposición 7.2,

$$\sum_C |\operatorname{gen}(C)| = |G| = n = \sum_{d/n} \phi(d),$$

donde C recorre el conjunto de los subgrupos cíclicos de G. Por lo tanto, debido a que el orden de cada subgrupo cíclico C de G divide a n y a que $|\operatorname{gen}(C)| = \phi(|C|)$, si G tiene a lo sumo un subgrupo de orden d para cada divisor d de n, entonces debe tener efectivamente un subgrupo cíclico de orden d para cada divisor d de n. En particular G tiene un subgrupo cíclico de orden n y, en consecuencia, es cíclico. □

Teorema 7.4. *Si F es un cuerpo y G es un subgrupo finito de $F^\times$, entonces G es cíclico.—*

Demostración. Si $x \in G$ satisface $x^d = 1$, donde $d/|G|$, entonces x es una raíz del polinomio $X^d - 1 \in F[X]$. Dado que un polinomio de grado d con coeficientes en un cuerpo tiene a lo sumo d raíces, G no puede tener más que un subgrupo de orden d (dos subgrupos darían más de d raíces de $X^d - 1$). En consecuencia, por el teorema anterior, G es cíclico. □

Consideremos un primo p positivo. A continuación vamos a caracterizar el grupo de unidades del anillo de congruencias $\mathbb{Z}_{p^r}$. Para ello necesitaremos un par de lemas.

Lema 7.5. *Si $i \in \mathbb{N}$, $y, z \in \mathbb{Z}$ e $y \equiv z \pmod{p^i}$, entonces $y^p \equiv z^p \pmod{p^{i+1}}$.*

Demostración. Claramente

$$\sum_{j=0}^{p-1} y^i z^{p-i-1} \equiv p y^{p-1} \pmod{p^i}.$$

En consecuencia p^{2i} divide a

$$(y-z)\left(\sum_{j=0}^{p-1} y^i z^{p-i-1} - p y^{p-1}\right) = y^p - z^p - p(y-z)y^{p-1}.$$

Como $p^{i+1} \mid p(y-z)y^{p-1}$ se sigue de esto que $y^p \equiv z^p \pmod{p^{i+1}}$, como queremos. □

Lema 7.6. *Si $p = 2$ e $i > 1$ o si p es un primo impar e $i \geq 1$, entonces*

$$y \equiv 1 + p^i \pmod{p^{i+1}} \Longrightarrow y^p \equiv 1 + p^{i+1} \pmod{p^{i+2}}.$$

Demostración. Por el lema anterior se sigue de la hipótesis que

$$y^p \equiv (1 + p^i)^p \pmod{p^{i+2}}.$$

En consecuencia para terminar la demostración será suficiente comprobar que

$$(1+p^i)^p \equiv 1+p^{i+1} \pmod{p^{i+2}}. \tag{9}$$

Pero, como por la fórmula del binomio,

$$(1+p^i)^p = 1+p^{i+1}+\sum_{j=2}^{p}\binom{p}{j}p^{ij}$$

la congruencia (9) se sigue de que

$$\binom{p}{j}p^{ij} \equiv 0 \pmod{p^{i+2}},$$

para todo $2 < j \leq p$ y también para $j = 2$ si $p > 2$ o $i > 1$. □

Teorema 7.7. *Si p es un primo impar, entonces el grupo de unidades del anillo de congruencias $\mathbb{Z}_{p^r}$ es cíclico de orden $(p-1)p^{r-1}$, para todo $r \in \mathbb{N}$. En cambio, $\mathbb{Z}_{2^r}^\times$ es cíclico de orden 2^{r-1} si $r \leq 2$, e isomorfo a $\mathbb{Z}_{2^{r-2}} \oplus \mathbb{Z}_2$ si $r \geq 3$. Además, en este caso*

$$\mathbb{Z}_{2^r}^\times = \{\pm 5^i : 0 \leq i < 2^{r-2}\},$$

donde, por supuesto, las potencias de 5 son realizadas en $\mathbb{Z}_{2^r}$.

Demostración. Como $x \in \mathbb{Z}_{p^r}^\times$ si y sólo si p no divide a x, el grupo $\mathbb{Z}_{p^r}^\times$ tiene $(p-1)p^{r-1}$ elementos, tanto si $p = 2$ como si es impar. Cuando $r = 1$ el resultado se sigue de que el grupo de unidades de un cuerpo finito es cíclico. Podemos suponer entonces que $r > 1$. Afirmamos que si p es impar, entonces

$$(1+p)^{p^i} \equiv 1+p^{i+1} \pmod{p^{i+2}} \quad \text{para todo } i \geq 0.$$

Probaremos esto por inducción en i. El caso $i = 0$ es trivial. Supongamos que la afirmación vale para i. Entonces por los Lemas 7.5 y 7.6,

$$(1+p)^{p^{i+1}} \equiv (1+p^{i+1})^p \equiv 1+p^{i+2} \pmod{p^{i+3}},$$

como queremos. En particular, $1+p$ tiene orden p^{r-1} en $\mathbb{Z}_{p^r}^\times$. Debido a esto, para concluir la prueba de la primera afirmación será suficiente ver que existe $x \in \mathbb{Z}_{p^r}^\times$ de orden $p-1$, pues entonces $x(1+p)$ será un generador de $\mathbb{Z}_{p^r}^\times$. Pero si $z \in \mathbb{Z}_{p^r}$ es tal que $\pi(z)$ tiene orden $p-1$, donde $\pi\colon \mathbb{Z}_{p^r} \to \mathbb{Z}_p$ es la proyección canónica, entonces z es inversible (pues p no divide a z) y tiene orden $(p-1)p^i$ con $0 \leq i < r$, con lo cual $x := z^{p^i}$ tiene orden $p-1$, como queremos. Consideremos ahora el caso $p = 2$. Es obvio que el grupo de unidades de $\mathbb{Z}_{2^r}$ es cíclico si $r = 2$. Supongamos entonces que $r > 2$. Como $5 = 1+2^2$, se sigue de los Lemas 7.5 y 7.6 (razonando por inducción en i como arriba), que

$$5^{2^i} \equiv 1+2^{i+2} \pmod{2^{i+3}} \quad \text{para todo } i \geq 0.$$

Así, $\{5^i : 0 \leq i < 2^{r-2}\}$ es un subgrupo cíclico de orden 2^{r-2} de $\mathbb{Z}_{2^r}^\times$. Además

$$5^{2^{r-3}} \equiv 1+2^{r-1} \pmod{2^r}$$

y, en consecuencia, es distinto de -1 en $\mathbb{Z}_{2^r}^\times$. Como $5^{2^{r-3}}$ y -1 tienen ambos orden 2 en $\mathbb{Z}_{2^r}^\times$, el subgrupo $\{\pm 5^i : 0 \leq i < 2^{r-2}\}$ de $\mathbb{Z}_{2^r}^\times$ no es cíclico. Por lo tanto contiene propiamente al grupo $\{5^i : 0 \leq i < 2^{r-2}\}$ y coincide entonces con $\mathbb{Z}_{2^r}^\times$. Por último, es fácil ver que los grupos $\{\pm 5^i : 0 \leq i < 2^{r-2}\}$ y $\mathbb{Z}_{2^{r-2}} \oplus \mathbb{Z}_2$ son isomorfos. □

Las siguientes dos proposiciones dan una demostración alternativa del teorema anterior para el caso en que p es un primo impar. En realidad obtenemos una versión que es más útil a la hora de buscar un generador de $\mathbb{Z}_{p^r}^\times$.

Tomemos un número natural s tal que $0 < s < p$ tal que el orden de s en $\mathbb{Z}_p$ es $p-1$. Notemos que s es una unidad de $\mathbb{Z}_{p^2}$ ya que s es coprimo con p^2. Por lo tanto el orden de s divide al orden $p(p-1) = \phi(p^2)$ del grupo de unidades de $\mathbb{Z}_{p^2}$. Por otro lado, como s tiene orden $p-1$ en $\mathbb{Z}_p$, necesariamente $p-1$ divide al orden de s (pues $s^i \equiv 1 \pmod{p^2}$ implica $s^i \equiv 1 \pmod{p}$). Así que el orden de s en $\mathbb{Z}_{p^2}$ es $p-1$ o $(p-1)p$. Vale el siguiente resultado:

PROPOSICIÓN 7.8. *Si s tiene orden $p-1$ en $\mathbb{Z}_{p^2}^\times$, entonces $s+p$ tiene orden $(p-1)p$ en $\mathbb{Z}_{p^2}^\times$.*

DEMOSTRACIÓN. Para comenzar notemos que $s+p$ es coprimo con p^2 y, por lo tanto, $s+p$ está en el grupo de unidades de $\mathbb{Z}_{p^2}$. Dado que además el orden de s en $\mathbb{Z}_p^\times$ es $p-1$, necesariamente el orden de $s+p$ en $\mathbb{Z}_{p^2}^\times$ es $p-1$ o $(p-1)p$. Supongamos que $(s+p)^{p-1} \equiv 1 \pmod{p^2}$. Entonces por el teorema del binomio

$$\begin{aligned} 1 &= (s+p)^{p-1} \pmod{p^2} \\ &\equiv s^{p-1} + (p-1)ps^{p-2} \pmod{p^2} \\ &\equiv 1 + (p-1)ps^{p-2} \pmod{p^2}. \end{aligned}$$

Pero entonces $p \mid (p-1)s^{p-2}$, lo que es absurdo. Así el orden de $s+p$ en $\mathbb{Z}_{p^2}^\times$ es $(p-1)p$. □

PROPOSICIÓN 7.9. *Tomemos un número natural $s < p^2$, coprimo con p, tal que el orden de s en $\mathbb{Z}_{p^2}^\times$ es $(p-1)p$. Entonces para todo $r \geq 2$, el orden de s en $\mathbb{Z}_{p^r}^\times$ es $(p-1)p^{r-1}$.*

DEMOSTRACIÓN. Es suficiente probar por inducción en i que

$$p^i \nmid s^{(p-1)p^{i-2}} - 1 \qquad \text{para todo } i \geq 2 \tag{10}$$

El caso $i = 2$ vale porque el orden de s en $\mathbb{Z}_{p^2}^\times$ es $(p-1)p$. Supongamos ahora que $i \geq 2$ y que (10) vale para i. Por el teorema de Euler-Fermat sabemos que

$$p^{i-1} \mid s^{(p-1)p^{i-2}} - 1.$$

En consecuencia existe $k \in \mathbb{Z}$ tal que $s^{(p-1)p^{i-2}} = 1 + kp^{i-1}$. Así

$$s^{(p-1)p^{i-1}} = (1 + kp^{i-1})^p \equiv 1 + kp^i \pmod{p^{i+1}}. \tag{11}$$

Dado que, debido a (10) sabemos que $p \nmid k$, se sigue de (11), que

$$p^{i+1} \nmid s^{(p-1)p^{i-1}} - 1,$$

como queremos. □

8. Propiedades del producto de subgrupos de un grupo

En esta sección están probamos tres proposiciones acerca del producto de subgrupos de un grupo y una acerca del producto de subconjuntos. En la primera establecemos dos propiedades generales conocidas como ley modular y ley de Dedekind, respectivamente; en la segunda obtenemos una fórmula para calcular el cardinal de este producto; en la tercera damos una condición necesaria y suficiente para que dicho producto sea un subgrupo; y, en la

última, mostramos que si dos subconjuntos de un grupo finito son suficientemente grandes, entonces su producto es todo el grupo.

PROPOSICIÓN 8.1. *Si $K \leq H$ y L son subgrupos de un grupo G, entonces*

1. *$H \cap KL = K(H \cap L)$.*
2. *Si $K \cap L = H \cap L$ y $KL = HL$, entonces $K = H$.*

DEMOSTRACIÓN. 1) Evidentemente $K(H \cap L) \subseteq KL$ y también $K(H \cap L) \subseteq H$, porque $K \subseteq H$. En consecuencia, $K(H \cap L) \subseteq H \cap KL$. Veamos que vale la inclusión recíproca. Tomemos $g \in H \cap KL$ y escribamos $g = kl$ con $k \in K$ y $l \in L$. Entonces $l = k^{-1}g \in KH \subseteq H$ y, por lo tanto, $g = kl \in K(H \cap L)$.
2) Por el item 1) y las hipótesis,

$$H = H \cap HL = H \cap KL = K(H \cap L) = K(K \cap L) = K,$$

como queríamos. □

PROPOSICIÓN 8.2. *Si H y L son subgrupos de un grupo G, entonces*

$$|HL||H \cap L| = |H||L|.$$

DEMOSTRACIÓN. Como la función $\varsigma\colon H \times L \to HL$, definida por $\varsigma(h, l) := hl$, es sobreyectiva, para probar la proposición será suficiente ver que $|\varsigma^{-1}(g)| = |H \cap L|$ para todo $g \in HL$, lo que haremos verificando que si $g = hl$, entonces

$$\varsigma^{-1}(g) = \{(hy, y^{-1}l) : y \in H \cap L\}.$$

Es evidente que8 $\{(hy, y^{-1}l) : y \in H \cap L\} \subseteq \varsigma^{-1}(g)$. Recíprocamente, si $(h', l') \in \varsigma^{-1}(g)$, entonces $h^{-1}h' = ll'^{-1} \in H \cap L$ y, así, $h' = hy$ y $l' = y^{-1}l$, con $y \in H \cap L$. □

DEMOSTRACIÓN ALTERNATIVA DE LA PROPOSICIÓN 8.2. Por la igualdad (7) y el teorema de Lagrange,

$$|HL||H \cap L| = |H : H \cap L||H \cap L||L| = |H||L|,$$

como queremos.

PROPOSICIÓN 8.3. *Para cada par de subgrupos H y L de un grupo G son equivalentes:*

1. *$LH \subseteq HL$.*
2. *$HL \leq G$.*
3. *$LH = HL$.*
4. *$HL \subseteq LH$.*
5. *$LH \leq G$.*

DEMOSTRACIÓN. Es suficiente probar que 1) $\Rightarrow$ 2) y 2) $\Rightarrow$ 3). Si $LH \subseteq HL$, entonces

$$HL(HL)^{-1} = HLL^{-1}H^{-1} = HLH \subseteq HHL = HL$$

y, por lo tanto, $HL \leq G$. Por otra parte, si $HL \leq G$, entonces

$$LH = L^{-1}H^{-1} = (HL)^{-1} = HL,$$

como queremos. □

PROPOSICIÓN 8.4. *Consideremos un grupo finito G y dos subconjuntos K y L de G. Si $|K| + |L| > |G|$, entonces $G = KL$.*

Demostración. Tomemos $g \in G$ arbitrario. Como $|gL^{-1}| = |L|$,

$$|K| + |gL^{-1}| > |G|.$$

En consecuencia, $K \cap gL^{-1} \neq \emptyset$ y, por lo tanto, existen $k \in K$ y $l \in L$ tales que $gl^{-1} = k$, de manera que $g = kl \in KL$. □

La siguiente es una aplicación de este resultado.

Proposición 8.5. *Cada elemento de un cuerpo finito es suma de dos cuadrados.*

Demostración. Para cada cuerpo finito F, denotemos con $(F^\times)^2$ al conjunto de los cuadrados de $F^\times$. Como $a^2 = b^2 \Rightarrow a = b$ o $a = -b$, sabemos que $2|(F^\times)^2| \geq |F^\times|$. En consecuencia, por la Proposición 8.4,

$$F = \big((F^\times)^2 \cup \{0\}\big) + \big((F^\times)^2 \cup \{0\}\big).$$

El resultado se sigue inmediatamente de este hecho. □

9. Coclases dobles

Consideremos dos subgrupos (no necesariamente distintos) H y L de un grupo G. Una (H, L)-*coclase doble* es un subconjunto de G de la forma HgL. Como la relación definida por $g' \equiv g$ si y sólo si $g' \in HgL$, es de equivalencia, G se parte como una unión disjunta $G = \bigcup_{i\in I} Hg_iL$ de coclases dobles. Afirmamos que si G es finito, entonces

$$|G : L| = \sum_{i\in I} |H : H \cap g_iLg_i^{-1}|. \tag{12}$$

Como $|G| = \sum_{i\in I} |Hg_iL|$, para probar la afirmación bastará ver que

$$|Hg_iL| = \frac{|H||L|}{|H \cap g_iLg_i^{-1}|}.$$

Pero $|Hg_iL| = |Hg_iLg_i^{-1}|$ y, dado que H y $g_iLg_i^{-1}$ son subgrupos de G, de la Proposición 8.2 se sigue que

$$|Hg_iLg_i^{-1}| = \frac{|H||g_iLg_i^{-1}|}{|H \cap g_iLg_i^{-1}|} = \frac{|H||L|}{|H \cap g_iLg_i^{-1}|},$$

como necesitamos. Cuando $L = 1$, la fórmula (12) se reduce a la establecida en el teorema de Lagrange.

Ejemplo 9.1. *Escribamos* $\mathrm{S}_3 = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$, *donde*

$$\begin{array}{llll} \sigma_1(1) := 2, & \sigma_1(2) := 1 & y & \sigma_1(3) := 3, \\ \sigma_2(1) := 3, & \sigma_2(2) := 2 & y & \sigma_2(3) := 1, \\ \sigma_3(1) := 1, & \sigma_3(2) := 3 & y & \sigma_3(3) := 2, \\ \sigma_4(1) := 2, & \sigma_4(2) := 3 & y & \sigma_4(3) := 1, \\ \sigma_5(1) := 3, & \sigma_5(2) := 1 & y & \sigma_5(3) := 2. \end{array}$$

Si $H = \{\mathrm{id}, \sigma_1\}$ *y* $L = \{\mathrm{id}, \sigma_2\}$, *entonces*

$$H\,\mathrm{id}\,L = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_5\} \qquad y \qquad H\sigma_3L = \{\sigma_3, \sigma_4\}.$$

10. Subgrupos normales

Un subgrupo N de un grupo G es *normal* o *invariante* si $gNg^{-1} = N$ para todo $g \in G$. Escribiremos $N \triangleleft G$ para señalar que N es un subgrupo normal de G. Más adelante, en el Capítulo 4, también señalaremos este mismo hecho escribiendo $G \triangleright N$. Enseguida daremos varias caracterizaciones simples de los subgrupos normales. En particular, veremos que un subgrupo N de G es normal si y sólo si las coclases a izquierda y derecha de N coinciden (de todas las maneras en que sea razonable entender esto).

PROPOSICIÓN 10.1. *Para cada $N \leq G$ son equivalentes:*

1. *Para cada $g \in G$ existe $h \in G$ tal que $gN \subseteq Nh$.*
2. *Para cada $g \in G$ existe $h \in G$ tal que $gNh^{-1} \subseteq N$.*
3. *Para cada $g \in G$ existe $h \in G$ tal que $Ng \subseteq hN$.*
4. *Para cada $g \in G$ existe $h \in G$ tal que $h^{-1}Ng \subseteq N$.*
5. *$Ng = gN$ para todo $g \in G$*
6. *N es normal.*

DEMOSTRACIÓN. Por supuesto que 5) $\Rightarrow$ 1). Para probar que vale la recíproca, notemos primero que como $gN \subseteq Nh$,

$$Ng \subseteq NgN \subseteq NNh = Nh,$$

lo cual implica que $Ng = Nh$, porque las coclases a derecha de N parten G. En consecuencia, $gN \subseteq Nh = Ng$. Similarmente, $g^{-1}N \subseteq Ng^{-1}$ y, por lo tanto,

$$Ng = gg^{-1}Ng \subseteq gNg^{-1}g = gN.$$

Los items 1) y 2) son equivalentes porque

$$gN \subseteq Nh \Leftrightarrow gNh^{-1} \subseteq Nhh^{-1} \Leftrightarrow gNh^{-1} \subseteq N.$$

El mismo argumento prueba que 5) es equivalente a 6). Por último, 3) $\Leftrightarrow$ 4) $\Leftrightarrow$ 5) por dualidad. □

EJEMPLO 10.2. *Recordemos que el grupo diedral D_n es el subgrupo de $\mathrm{GL}(2,\mathbb{R})$ generado por las matrices*

$$x := \begin{pmatrix} \cos\theta & \operatorname{sen}\theta \\ -\operatorname{sen}\theta & \cos\theta \end{pmatrix} \qquad e \qquad y := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

donde $\theta := 2\pi/n$ con $n > 1$. Es fácil ver que todos los subgrupos de D_n que están incluídos en $\langle x \rangle$ son normales. En efecto, debido a que x e y generan D_n, para comprobarlo basta verificar que

$$x\langle x^r\rangle x^{-1} \subseteq \langle x^r\rangle \qquad e \qquad y\langle x^r\rangle y^{-1} \subseteq \langle x^r\rangle.$$

Lo primero es obvio y lo segundo se sigue de que

$$yx^{ri}y^{-1} = (yxy^{-1})^{ri} = (x^{-1})^{ri} = x^{-ri}.$$

Supongamos ahora que N es un subgrupo normal de D_n que contiene a $x^j y$ para algún j. Como $x^i x^j y x^{-i} = x^{j+2i}y$, entonces $x^{j+2i}y$ y también $x^{2i} = x^{j+2i}y(x^j y)^{-1}$ pertenecen a H para todo i. En consecuencia

$$\bigcup_{0 \leq i < n/2} \{x^{2i}, x^{2i}y\} \subseteq N \qquad o \qquad \bigcup_{0 \leq i < n/2} \{x^{2i}, x^{2i+1}y\} \subseteq N$$

y, por lo tanto,

$$N = \langle x^2, y\rangle, \qquad N = \langle x^2, xy\rangle \qquad o \qquad N = D_n$$

si n es par, mientras que necesariamente $N = D_n$ si n es impar.

EJEMPLO 10.3. *Recordemos que el grupo cuaterniónico generalizado H_n es el subgrupo de* $\mathrm{GL}(2,\mathbb{C})$ *generado por las matrices*

$$x := \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix} \qquad e \qquad y := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

donde $w := e^{i\pi/n}$ con $n > 1$. Es evidente que todos los subgrupos de H_n que están incluídos en $\langle x\rangle$ son normales y que el cálculo hecho en el ejemplo anterior muestra que si N es un subgrupo normal de H_n que contiene a $x^j y$ para algún j, entonces

$$N = \langle x^2, y\rangle, \qquad N = \langle x^2, xy\rangle \qquad o \qquad N = H_n$$

si n es par, mientras que necesariamente $N = H_n$ si n es impar.

EJERCICIO 10.4. *Pruebe que un subgrupo N de G es invariante si y sólo si $hg \in N$ siempre que $gh \in N$.*

OBSERVACIÓN 10.5. *Si $N \subseteq L$ son subgrupos de un grupo G y $N \lhd G$, entonces $N \lhd L$.*

OBSERVACIÓN 10.6. *Si $N \lhd G$, entonces $NL = LN$ para todo subconjunto L de G. Si además $L \leq G$, entonces $NL \leq G$. Por último, si $L \lhd G$, entonces $NL \lhd G$.*

El siguiente resultado será mejorado más adelante.

PROPOSICIÓN 10.7. *Todo subgrupo N de índice 2 de un grupo G es normal.*

DEMOSTRACIÓN. Si $g \in N$, entonces $gN = N = Ng$. Tomemos $g \in G \setminus N$. Como N tiene índice 2,

$$G = N \cup gN = N \cup Ng,$$

con ambas uniones disjuntas. Así que también en este caso $gN = Ng$. □

Claramente la intersección de una familia de subgrupos normales de G es un subgrupo normal de G. En consecuencia, para cada subconjunto S de G existe un mínimo subgrupo normal $\overline{\langle S\rangle}$ de G que contiene a S, el cual es precisamente la intersección de todos los subgrupos normales de G que contienen a S. Como $\overline{\langle S\rangle}$ es normal e incluye a S, debe incluir también al subgrupo de G generado por $\bigcup_{g\in G} gSg^{-1}$. Pero usando la caracterización de subgrupos generados por un conjunto dada en (1), se comprueba inmediatamente que el último es normal, por lo que

$$\overline{\langle S\rangle} = \left\langle \bigcup_{g\in G} gSg^{-1} \right\rangle.$$

En general $\langle S\rangle$ está incluído estrictamente en $\overline{\langle S\rangle}$.

PROPOSICIÓN 10.8. *Si $\{G_i\}_{i\in I}$ es una familia de subgrupos normales de un grupo G, entonces $\bigvee_{i\in I} G_i$ es normal. Además, si I está provisto de un orden total, entonces*

$$\bigvee_{i\in I} G_i = \{g_{i_1} \cdots g_{i_n} : n \geq 0,\ i_1 < \cdots < i_n \in I \text{ y } g_{i_j} \in G_{i_j}\}.$$

DEMOSTRACIÓN. Tomemos $g_{i_1} \cdots g_{i_n} \in \bigvee_{i\in I} G_i$. Como

$$g(g_{i_1} \cdots g_{i_n})g^{-1} = (gg_{i_1}g^{-1})(gg_{i_2}g^{-1}) \cdots (gg_{i_n}g^{-1}) \in \bigvee_{i\in I} G_i \quad \text{para cada } g \in G,$$

el subgrupo $\bigvee_{i\in I} G_i$ de G es normal. La segunda afirmación se sigue de que, por la Observación 10.6, sabemos que $G_iG_j = G_jG_i$ para todo $i, j \in I$. □

11. Morfismos de grupos

Un *morfismo* $\varphi\colon G \to G'$, de un grupo G en otro G', es por definición un morfismo de monoides de G en G'. Es fácil ver que $\varphi\colon G \to G'$ es un morfismo de grupos si y sólo si $\varphi(xy) = \varphi(x)\varphi(y)$ para todo $x, y \in G$. Dicho de otra forma, no es necesario pedir que $\varphi(1) = 1$. En realidad, esto es una consecuencia inmediata de una observación hecha al principio de la Sección 3.

La identidad $\mathrm{id}_G\colon G \to G$, y más generalmente, la inclusión canónica $i\colon H \to G$ de un subgrupo H de G en G, es un morfismo de grupos. También lo es la composición $\psi \circ \varphi\colon G \to G''$ de dos morfismos de grupos $\varphi\colon G \to G'$ y $\psi\colon G' \to G''$.

Muchas de las propiedades básicas de los morfismos de grupos son análogas a las establecidas para los de monoides. Las definiciones de endomorfismo, isomorfismo, grupos isomorfos, automorfismo, monomorfismo, epimorfismo, sección y retracción son las mismas. Mantenemos la notación $G \simeq G'$ para señalar que los grupos G y G' son isomorfos. Se comprueba fácilmente que un morfismo es un isomorfismo si y sólo si es biyectivo. Nuevamente los monomorfismos, epimorfismos, secciones y retracciones son cerrados bajo la composición, toda retracción es sobreyectiva, toda sección es inyectiva, todo morfismo sobreyectivo es un epimorfismo, y un morfismo es inyectivo si y sólo si es un monomorfismo (la parte no trivial de la última afirmación es la suficiencia, la cual puede probarse copiando la demostración dada para monoides, con $\mathbb{Z}$ jugando el papel de $\mathbb{N}_0$). En consecuencia todo monomorfismo de grupos lo es de monoides. También para grupos un morfismo $\varphi\colon G \to G'$ es un isomorfismo si y sólo si es una sección y un epimorfismo, y esto ocurre si y sólo si es una retracción y un monomorfismo. Por último, también es cierto que todo epimorfismo es sobreyectivo, pero esto es mucho más difícil de probar, y lo dejamos para después.

EJEMPLO 11.1. *Hay monomorfismos que no son secciones y epimorfismos que no son retracciones. En efecto:*

1. *El monomorfismo $j\colon \mathbb{Z}_2 \to \mathbb{Z}_4$, definido por $j(0) := 0$ y $j(1) := 2$, no es una sección.*
2. *El epimorfismo $\pi\colon \mathbb{Z}_4 \to \mathbb{Z}_2$, definido por $\pi(0) := \pi(2) := 0$ y $\pi(1) := \pi(3) := 1$, no es una retracción.*

Igual que en el caso de los monoides, para cada par $\varphi\colon G \to G'$ y $\psi\colon G' \to G''$ de morfismos vale lo siguiente:

1. Si $\psi \circ \varphi$ es una sección, o un morfismo inyectivo, entonces también lo es φ.
2. Si $\psi \circ \varphi$ es una retracción, un epimorfismo, o un morfismo sobreyectivo, entonces también lo es ψ.

Al tratar con grupos utilizaremos los símbolos $\mathrm{Hom}(G, G')$, $\mathrm{Iso}(G, G')$, $\mathrm{End}(G)$ y $\mathrm{Aut}(G)$ para denotar respectivamente a los conjuntos de morfismos de G en G', isomorfismos de G en G', endomorfismos de G y automorfismos de G. De la definición se sigue inmediatamente que

$\mathrm{End}(G)$ es un monoide (cuyo elemento neutro es la función identidad) vía la composición y que $\mathrm{Aut}(G)$ es su grupo de unidades.

Una propiedad completamente nueva es que si $\varphi\colon G \to G'$ es un morfismo de grupos, entonces $\varphi(K^{-1}) = \varphi(K)^{-1}$, para cada subconjunto K de G.

EJERCICIO 11.2. *Consideremos un morfismo $\varphi\colon G \to G'$ y subconjuntos K y L de G'.*

1. *Pruebe que $\varphi^{-1}(K^{-1}) = \varphi^{-1}(K)^{-1}$.*
2. *Pruebe que si φ es sobreyectivo, entonces $\varphi^{-1}(KL) = \varphi^{-1}(K)\varphi^{-1}(L)$.*

EJEMPLO 11.3. *Para cada par de grupos G y G', el morfismo nulo $1_{GG'}\colon G \to G'$ es la función que manda todos elementos x de G a 1 (cuando usemos la notación aditiva, lo que nunca sucederá si G' no es abeliano, designaremos a este morfismo con el símbolo $0_{GG'}$).*

EJEMPLO 11.4. *Para cada grupo G, la* aplicación antipodal

$$\begin{aligned} G &\longrightarrow G^{\mathrm{op}} \\ g &\longmapsto g^{-1} \end{aligned}$$

es un isomorfismo de grupos.

EJEMPLO 11.5. *El determinante* $\det\colon \mathrm{GL}(n,k) \to k^\times$ *es un morfismo sobreyectivo de grupos.*

EJEMPLO 11.6. *La exponencial $x \mapsto e^x$ es un isomorfismo del grupo aditivo $\mathbb{R}$ en el grupo multiplicativo $\mathbb{R}_{>0}$, formado por los números reales positivos. Su inversa es el logaritmo natural.*

EJEMPLO 11.7. *La exponencial $x \mapsto e^{ix}$ es un morfismo del grupo aditivo $\mathbb{R}$ en el grupo multiplicativo $\mathbb{C}^\times$. Su imagen es el círculo unidad S^1.*

EJEMPLO 11.8. *La aplicación $\varsigma\colon \mathbb{C}^\times \to \mathbb{R}_{>0}$, definida por $\varsigma(x) := |x|$, es un morfismo sobreyectivo.*

EJEMPLO 11.9. *La aplicación $\varsigma\colon \mathbb{Z}[X] \to \mathbb{Q}_{>0}$, definida por*

$$\varsigma\left(\sum_{i\geq 0} n_i X^i\right) := \prod_{i\geq 0} p_i^{n_i},$$

donde $p_0 < p_1 < p_2 < \ldots$ es la sucesión de los números primos positivos, es un isomorfismo.

EJEMPLO 11.10. *Fijemos una raíz $w \in \mathbb{C}$ de orden n de la unidad (por ejemplo, podemos tomar $w := \cos(2\pi/n) + i\,\mathrm{sen}(2\pi/n)$). La aplicación $\varphi\colon \mathbb{Z}_n \to \mathrm{G}_n$, definida por $\varphi(n) = w^n$, es un isomorfismo de grupos.*

EJEMPLO 11.11. *Para cada $n > 1$, consideremos el subgrupo $\widetilde{D}_n$ de $\mathrm{GL}(2,\mathbb{C})$ generado por las matrices*

$$a = \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix} \qquad y \qquad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

donde $w \in \mathbb{C}$ es una raiz n-ésima primitiva de la unidad. Un cálculo directo muestra que

$$a^i = \begin{pmatrix} w^i & 0 \\ 0 & w^{-i} \end{pmatrix}, \quad b^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad y \quad ba^i = \begin{pmatrix} 0 & w^{-i} \\ w^i & 0 \end{pmatrix} = a^{-i}b.$$

Por lo tanto a y b satisfacen las relaciones

$$a^n = 1, \quad b^2 = 1 \quad y \quad bab^{-1} = a^{-1}$$

y los $2n$ elementos $1, a \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b$ son todos distintos. Así la función

$$\begin{aligned} D_n &\longrightarrow \widetilde{D}_n \ , \\ x^i y^j &\longmapsto a^i b^j \end{aligned}$$

donde x e y son como en el Ejemplo 5.8, es un isomorfismo.

Observación 11.12. *Si bien $|H_n| = |D_{2n}|$, estos dos grupos nunca son isomorfos, pues el primero tiene sólo un elemento de orden 2, mientras que el segundo tiene $2n+1$.*

Ejemplo 11.13. *Supongamos que X es un subconjunto de Y. Definamos*

$$i_*\colon \mathrm{S}_X \to \mathrm{S}_Y$$

por

$$i_*(\sigma)(y) := \begin{cases} \sigma(y) & \text{si } y \in X, \\ y & \text{si } y \notin X. \end{cases}$$

Es evidente que i_* es un morfismo inyectivo de grupos cuya imagen es el conjunto de las permutaciones de Y que dejan fijos a los elementos que están fuera de X. Llamamos a i_* la inclusión canónica de S_X en S_Y e identificamos a S_X con $i_*(\mathrm{S}_X)$. En particular consideramos a S_n como el subgrupo de $\mathrm{S}_{\mathbb{N}}$ formado por las permutaciones que dejan fijos a los números mayores que n, lo cual permite definir $\mathrm{S}_\infty := \bigcup_{n\in\mathbb{N}} S_n$. Es obvio que S_∞ es el subgrupo de $\mathrm{S}_{\mathbb{N}}$ que consiste de las permutaciones que sólo mueven a una cantidad finita de números y que S_∞ es un grupo infinito cuyos elementos tienen orden finito.

Ejemplo 11.14. *Supongamos que $i\colon X \to Y$ es una biyección. Definamos*

$$i_*\colon \mathrm{S}_X \to \mathrm{S}_Y$$

por $i_*(\sigma) := i \circ \sigma \circ i^{-1}$. Es evidente que i_* es un isomorfismo de grupos.

Ejemplo 11.15. *Supongamos que $i\colon X \to Y$ es una función inyectiva. Definamos*

$$i_*\colon \mathrm{S}_X \to \mathrm{S}_Y$$

por

$$i_*(\sigma)(y) := \begin{cases} i(\sigma(x)) & \text{si } y = i(x), \\ y & \text{si } y \notin i(X). \end{cases}$$

Es fácil ver que:

- *i_* es un morfismo inyectivo de grupos cuya imagen es el conjunto de las permutaciones de Y que dejan fijos a los elementos que están fuera de $i(X)$.*
- *Si X es un subconjunto de Y e i es la inclusión canónica de X en Y recuperamos la definición dada en el Ejemplo 11.13, mientras que si i es una biyección recuperamos la dada en el Ejemplo 11.14—.*
- *Si $g\colon Y \to Z$ es otra función, entonces $(j \circ i)_* = j_* \circ i_*$.*

11.1. Estructuras en el conjunto de los morfismos de un grupo en otro

En general $\mathrm{Hom}(G, G')$ no tiene ninguna estructura algebraica interesante, sólo es un conjunto con un punto distinguido (el morfismo nulo). Esto cambia cuando G' es abeliano. En esta subsección utilizaremos la notación aditiva.

PROPOSICIÓN 11.16. *Si G' es abeliano, entonces $\mathrm{Hom}(G, G')$ es un grupo abeliano vía la operación $(\varphi + \psi)(g) := \varphi(g) + \psi(g)$. El neutro de este grupo es el morfismo nulo $0_{GG'}$ y la inversa de un morfismo φ es la función $-\varphi$ definida por $(-\varphi)(g) := -\varphi(g)$.*

DEMOSTRACIÓN. Primero debemos ver que $+$ es una operación interna en $\mathrm{Hom}(G, G')$. En otras palabras, que si $\varphi, \psi\colon G \to G'$ son morfismos de grupos, entonces $\varphi + \psi$ también lo es. Pero esto es cierto porque, como G' es abeliano,

$$\begin{aligned}(\varphi + \psi)(gh) &= \varphi(gh) + \psi(gh)\\ &= \varphi(g) + \varphi(h) + \psi(g) + \psi(h)\\ &= \varphi(g) + \psi(g) + \varphi(h) + \psi(h)\\ &= (\varphi + \psi)(g) + (\varphi + \psi)(h).\end{aligned}$$

Ahora es evidente que

$$\varphi + (\psi + \zeta) = (\varphi + \psi) + \zeta \quad \text{y} \quad \varphi + \psi = \psi + \varphi \quad \text{para todo } \varphi, \psi, \zeta \in \mathrm{Hom}(G, G').$$

Por último, también es evidente que $0_{GG'}$ es neutro de la suma de morfismos, que si $\varphi\colon G \to G'$ es un morfismo de grupos, entonces $-\varphi$ también lo es, y que $\varphi + (-\varphi) = 0_{GG'}$. □

OBSERVACIÓN 11.17. *De la misma manera puede probarse que si M y M' son monoides y M' es abeliano, entonces $\mathrm{Hom}(M, M')$ es un monoide abeliano.*

OBSERVACIÓN 11.18. *Si $\varphi\colon H \to G$ es un morfismo de grupos y $\psi\colon G' \to H'$ es un morfismo de grupos abelianos, entonces las aplicaciones*

$$\varphi^*\colon \mathrm{Hom}(G, G') \to \mathrm{Hom}(H, G') \quad y \quad \psi_*\colon \mathrm{Hom}(G, G') \to \mathrm{Hom}(G, H'),$$

definidas por $\varphi^*(\alpha) := \alpha \circ \varphi$ y $\psi_*(\alpha) := \psi \circ \alpha$ respectivamente, son morfismos de grupos abelianos.

12. Núcleo e imagen

El *núcleo* $\ker\varphi$ de un morfismo de grupos $\varphi\colon G \to G'$ es la preimagen de 1 por φ. Es evidente que $\ker\varphi \lhd G$ e $\mathrm{Im}\,\varphi \leq G'$. Más aún, no es nada difícil comprobar que la imagen de un subgrupo H de G es un subgrupo de G', que es normal si H lo es y φ es sobreyectivo, y que la preimagen de un subgrupo H' de G' es un subgrupo de G, que es normal si H' lo es.

Es claro que la inclusión canónica $\iota\colon \ker\varphi \to G$ tiene las siguientes propiedades, la segunda de la cuales es llamada la *propiedad universal del núcleo*:

- $\varphi \circ \iota = 1_{\ker\varphi, G'}$,

- Para cada morfismo de grupos $\psi\colon H \to G$ que satisface $\varphi \circ \psi = 1_{HG'}$, existe un único morfismo de grupos $\psi'\colon H \to \ker\varphi$ tal que el diagrama

$$\begin{array}{ccccc} H & \xrightarrow{\psi} & G & \xrightarrow{\varphi} & G' \\ \downarrow{\scriptstyle \psi'} & \nearrow{\scriptstyle \iota} & & & \\ \ker\varphi & & & & \end{array}$$

conmuta.

Observación 12.1. *Una manera equivalente de formular la propiedad universal del núcleo es decir que para todo grupo H la correspondencia*

$$\begin{array}{ccc} \mathrm{Hom}(H, \ker\varphi) & \longrightarrow & \mathrm{Hom}(H, G) \\ \psi' & \longmapsto & \iota \circ \psi' \end{array}$$

es inyectiva y su imagen es $\{\psi \in \mathrm{Hom}(H, G) : \varphi \circ \psi = 1_{HG'}\}$.

A lo largo de este apunte aparecerán muchas más propiedades universales, todas en el estilo usado al establecer la del núcleo. Cada una de ellas tiene una versión equivalente, similar a la dada recién. No siempre mencionaremos la segunda, pero recomendamos al lector tomarse el trabajo de formularla.

Proposición 12.2. *Si $\varphi\colon G \to G'$ es un morfismo de grupos, entonces dos elementos g y h de G tienen la misma imagen bajo φ si y sólo si $g\ker\varphi = h\ker\varphi$.*

Demostración. En efecto,

$$\varphi(g) = \varphi(h) \Leftrightarrow g^{-1}h \in \ker\varphi \Leftrightarrow g\ker\varphi = h\ker\varphi,$$

como afirmamos. □

Corolario 12.3. *Un morfismo de grupos $\varphi\colon G \to G'$ es inyectivo si y sólo si $\ker\varphi = 1$.*

Ejemplo 12.4. *El núcleo de* $\det\colon \mathrm{GL}(n, k) \to k^\times$ *es el* grupo lineal especial $\mathrm{SL}(n, k)$.

Ejemplo 12.5. *El núcleo de la función exponencial*

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{C} \\ x & \longmapsto & e^{ix} \end{array},$$

es el grupo aditivo $\{2\pi n : n \in \mathbb{Z}\}$.

Ejemplo 12.6. *El núcleo del morfismo $\varsigma\colon \mathbb{C}^\times \to \mathbb{R}_{>0}$, definido por $\varsigma(x) = |x|$, es el círculo unidad.*

13. Cociente de grupos

Consideremos una relación de equivalencia $\simeq$ definida en el conjunto subyacente de un monoide S y denotemos con $\pi\colon S \to S/\simeq$ a la aplicación canónica. Para cada $s \in S$ denotemos con $[s]$ a la clase de equivalencia de s en el conjunto cociente $S/\simeq$. Por definición

$$[s] := \{s' \in S : s' \simeq s\} \qquad \text{y} \qquad \pi(s) := [s]$$

para cada $s \in S$. Supongamos que $S/\simeq$ tiene una estructura de monoide tal que la aplicación canónica $\pi\colon S \to S/\simeq$ es un morfismo. Entonces

$$[1] = \pi(1) = 1 \qquad \text{y} \qquad [s][s'] = \pi(s)\pi(s') = \pi(ss') = [ss'],$$

para todo $s, s' \in S$. Por lo tanto

$$s \simeq t \text{ y } s' \simeq t' \Leftrightarrow [s] = [t] \text{ y } [s'] = [t'] \Rightarrow [ss'] = [s][s'] = [t][t'] = [tt'] \Rightarrow ss' \simeq tt'.$$

Llamaremos *compatibles* a las relaciones de equivalencia que satisfaces esta propiedad. Supongamos recíprocamente, que $\simeq$ es una relación de equivalencia compatible definida en un monoide S. Definimos en el cociente $S/\simeq$ un producto por $[s][s'] := [ss']$ para todo $s, s' \in S$. Esta definición es correcta porque

$$[s] = [t] \text{ y } [s'] = [t'] \Leftrightarrow s \simeq t \text{ y } s' \simeq t' \Rightarrow ss' \simeq tt' \Leftrightarrow [ss'] = [tt'].$$

Con esta operación $S/\simeq$ es un monoide con neutro $[1]$, pues

$$([s][s'])[s''] = [ss'][s''] = [(ss')s''] = [s(s's'')] = [s][s's''] = [s]([s'][s''])$$

para todo $s, s', s'' \in S$ y

$$[s][1] = [s1] = [s] = [1s] = [1][s],$$

para todo $s \in S$. El mismo argumento prueba que $S/\simeq$ es conmutativo si S lo es. Además, la aplicación canónica $\pi\colon S \to S/\simeq$ es un morfismo de monoides. En particular, si S es un grupo, entonces también lo es $S/\simeq$, y $\pi\colon S \to S/\simeq$ es un morfismo de grupos. Notemos por último que para cada $s, s' \in S$ el producto $[ss']$ de s y t, definido aquí contiene al producto

$$[s][t] = \{s' \in S : s' \simeq s\}\{t' \in S : t' \simeq t\} = \{s't' : s' \simeq s \text{ y } t' \simeq t\}$$

definido al comienzo de la Sección 2.

Se pueden decir muchas cosas más acerca de los cocientes de monoides por relaciones de equivalencia compatibles, pero casi todas son de caracter formal. Así que a partir de ahora vamos a concentrarnos en el caso de grupos, donde los resultados son más elegantes. Supongamos entonces que $\simeq$ es una relación de equivalencia compatible definida en un grupo G. Escribamos $N := \ker \pi$. Ya sabemos que $N \lhd G$, y es trivial que

$$g \in hN \Leftrightarrow h^{-1}g \in N \Leftrightarrow h^{-1}g \simeq 1 \Leftrightarrow h \simeq g \Leftrightarrow hg^{-1} \simeq 1 \Leftrightarrow hg^{-1} \in N \Leftrightarrow h \in Ng,$$

de modo que $\simeq$ queda determinada por N y, además,

$$\{h \in G : h \simeq g\} = gN = Ng \quad \text{para todo } g \in N.$$

Recíprocamente, si N es un subgrupo normal de G, entonces por la Proposición 10.1 las relaciones de equivalencia

$$h \simeq g \Leftrightarrow hg^{-1} \in N \Leftrightarrow h \in Ng \Leftrightarrow Nh{=}Ng \quad \text{y} \quad h \simeq' g \Leftrightarrow g^{-1}h \in N \Leftrightarrow h \in gN \Leftrightarrow hN{=}gN$$

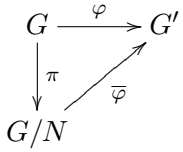
coinciden y son compatibles con la operación de G, porque

$$gNg'N = gg'NN = gg'N.$$

lo que muestra además que, para grupos, el productos de clases definido en esta sección coincide es un caso particular del producto de subconjuntos definido al comienzo de la Sección 2.

De ahora en más, para cada subgrupo normal N de G, denotaremos con G/N al grupo cociente $G/\simeq$ de G por la relación de equivalencia $\simeq$ definida arriba, y lo llamaremos *grupo cociente de G por N*. Es evidente que el núcleo del morfismo canónico $\pi\colon G \to G/N$ es N. Este morfismo es inicial entre aquellos con dominio G, cuyos núcleos incluyen a N. En otras palabras, π tiene la siguiente propiedad universal:

- Si $\varphi\colon G \to G'$ es un morfismo de grupos tal que $N \subseteq \ker\varphi$, entonces existe un único morfismo de grupos $\overline{\varphi}\colon G/N \to G'$ tal que el triángulo



conmuta.

Para comprobarlo, notemos que

$$g \simeq h \Rightarrow gh^{-1} \in N \subseteq \operatorname{Ker}\varphi \Rightarrow \varphi(g) = \varphi(h),$$

lo que permite definir $\overline{\varphi}([g]) := \varphi(g)$. Como $\pi(g) = [g]$, el triángulo conmuta. Adicionalmente, $\overline{\varphi}$ es un morfismo de grupos porque

$$\overline{\varphi}([g][h]) = \overline{\varphi}([gh]) = \varphi(gh) = \varphi(g)\varphi(h) = \overline{\varphi}([g])\overline{\varphi}([h]),$$

para todo $g, h \in G$.

Observación 13.1. *Una manera equivalente de formular la propiedad universal del cociente es decir que para todo grupo G' la correspondencia*

$$\begin{aligned} \operatorname{Hom}(G/N, G') &\longrightarrow \operatorname{Hom}(G, G') \\ \overline{\varphi} &\longmapsto \overline{\varphi} \circ \pi \end{aligned}$$

es inyectiva y su imagen es $\{\varphi \in \operatorname{Hom}(G, G') : \varphi(N) = 1\}$.

Una manera equivalente de formular la propiedad universal del cociente es decir que para todo grupo G' la correspondencia

$$\begin{aligned} \operatorname{Hom}(G/N, G') &\longrightarrow \operatorname{Hom}(G, G') \\ \overline{\varphi} &\longmapsto \overline{\varphi} \circ \pi \end{aligned}$$

es inyectiva y su imagen es $\{\varphi \in \operatorname{Hom}(G, G') : \varphi(N) = 1\}$.

Observación 13.2. *El núcleo de $\overline{\varphi}$ es $\ker\varphi/N$ y su imagen es la imagen de φ. En particular, $\overline{\varphi}$ es inyectiva si y sólo si $\ker\varphi = N$ y sobreyectiva si y sólo si lo es φ. En efecto, la segunda afirmación es clara. Para probar la primera notemos que, como $\overline{\varphi} \circ \pi = \varphi$, la clase en G/N de un elemento g de G pertenece a $\ker\overline{\varphi}$ si y sólo si $g \in \ker\varphi$ y, por consiguiente,*

$$\ker\overline{\varphi} = \{gN : g \in \ker\varphi\} = \frac{\ker\varphi}{N},$$

como queríamos.

El resto de la sección estará dedicado a establecer algunos resultados que son consecuencias más o menos directa de la propiedad universal del cociente. Entre ellos se encuentran los teoremas de isomorfismo de Noether.

Teorema 13.3 (Primer teorema de isomorfismo). *Todo morfismo de grupos $\varphi\colon G \to G'$ induce un isomorfismo $\overline{\varphi}\colon G/\ker\varphi \to \operatorname{Im}\varphi$.*

Demostración. Es claro. □

Teorema 13.4 (Segundo teorema de isomorfismo). *Si $L \subseteq N$ son subgrupos normales de un grupo G, entonces $N/L \triangleleft G/L$ y $G/N \simeq (G/L)/(N/L)$.*

Demostración. Consideremos los morfismos canónicos $\pi_L\colon G \to G/L$ y $\pi_N\colon G \to G/N$. Por la propiedad universal de π_L hay único morfismo $\tilde{\pi}\colon G/L \to G/N$ tal que el triángulo

$$\begin{array}{ccc} G & \xrightarrow{\pi_N} & G/N \\ \downarrow{\scriptstyle \pi_L} & \nearrow_{\tilde{\pi}} & \\ G/L & & \end{array},$$

conmuta. Es fácil ver que $\tilde{\pi}$ es sobreyectivo y que $\ker\tilde{\pi} = N/L$. En consecuencia $N/L \lhd G/L$ y, por el teorema anterior, $\tilde{\pi}$ induce un isomorfismo $\overline{\pi}\colon (G/L)/(N/L) \to G/N$. □

Teorema 13.5 (Tercer teorema de isomorfismo). *Si L y N son dos subgrupos de un grupo G y N es normal en G, entonces $L \cap N \lhd L$ y $L/L \cap N \simeq NL/N$.*

Demostración. Consideremos el morfismo $\tilde{\iota}\colon L \to G/N$ obtenido componiendo la inclusión canónica $\iota\colon L \to G$ con la sobreyección canónica $\pi_N\colon G \to G/N$. Es fácil ver que $\ker\tilde{\iota} = L \cap N$ e $\operatorname{Im}\tilde{\iota} = NL/N$. Así $L \cap N \lhd L$ y, por el Teorema 13.3, la aplicación $\tilde{\iota}$ induce un isomorfismo de $L/L \cap N$ en NL/N. □

Teorema 13.6. *Si $\varphi\colon G \to G'$ es un morfismo de grupos, entonces*

$$|G| = |\operatorname{Im}\varphi||\ker\varphi|.$$

Demostración. Por el teorema de Lagrange, $|G| = |G : \ker\varphi||\ker\varphi|$, y por el primer teorema de isomorfismo, $|G : \ker\varphi| = |\operatorname{Im}\varphi|$. □

Observación 13.7. *Consideremos un morfismo de grupos $\varphi\colon G \to G'$. Por el teorema de Lagrange, sabemos que $|\operatorname{Im}\varphi|$ divide a $|G'|$, y por el Teorema 13.6, que divide a $|G|$. Por lo tanto, si G y G' son finitos, $|\operatorname{Im}\varphi|$ divide a $(|G| : |G'|)$. En particular, si $|G|$ y $|G'|$ son coprimos, entonces φ es el morfismo nulo.*

Ejemplo 13.8. *Supongamos que k es un cuerpo finito. Si G es un subgrupo de $\mathrm{GL}(n,k)$, cuyo orden es coprimo con $|k|-1$, entonces $G \leq \mathrm{SL}(n,k)$, porque la aplicación $\det\colon G \to k^\times$ es el morfismo nulo. En particular, todos los subgrupos de orden impar de $\mathrm{GL}(n,\mathbb{Z}_3)$ están incluídos en $\mathrm{SL}(n,\mathbb{Z}_3)$.*

Recordemos que un *orden parcial* en un conjunto X es una relación binaria $\leq$ en X, que es reflexiva, antisimétrica y transitiva. Un *conjunto parcialmente ordenado* es un conjunto X provisto de un orden parcial. El *supremo* de un subconjunyo Y de X es un elemento $y \in X$, que satisface:

- $x \leq y$ para todo $x \in Y$,
- Si $x \leq w$ para todo $x \in Y$, entonces $y \leq w$,

y el *ínfimo* es un elemento $z \in X$, que satisface:

- $z \leq x$ para todo $x \in Y$,
- Si $w \leq x$ para todo $x \in Y$, entonces $w \leq z$.

Si existen, el supremo y el ínfimo de Y son únicos, y se los denota $\bigvee_{x\in Y} x$ y $\bigwedge_{x\in Y} x$, respectivamente. Dada una familia $(x_i)_{i\in I}$ denotamos (si existen) con $\bigvee_{i\in I} x_i$ al supremo de $\{x_i : i \in I\}$ y con $\bigwedge_{i\in I} x_i$ al ínfimo de $\{x_i : i \in I\}$. Un conjunto ordenado X es un *reticulado completo* si todo subconjunto de X tiene supremo e ínfimo. Por ejemplo, el conjunto $\mathrm{Sub}_H(G)$, de los subgrupos de G que incluyen a un subgrupo dado H, es un reticulado completo vía el orden

dado por la inclusión. El ínfimo de una familia $(G_i)_{i\in I}$ de subgrupos de G es la intersección $\bigcap_{i\in I} G_i$, y el supremo es el subgrupo $\bigvee_{i\in I} G_i$. Cuando $H = 1$ escribiremos $\mathrm{Sub}(G)$ en lugar de $\mathrm{Sub}_1(G)$.

PROPOSICIÓN 13.9. *Para cada conjunto ordenado X son equivalentes:*

1. *X es un reticulado completo.*
2. *Todo subconjunto de X tiene supremo.*
3. *Toda subconjunto de X tiene ínfimo.*

DEMOSTRACIÓN. Es claro que 1) $\Rightarrow$ 2) y 1) $\Rightarrow$ 3). Veamos que 2) $\Rightarrow$ 1). Notemos primero que el supremo del subconjunto vacío de X es el mínimo de X. En consecuencia todo subconjunto Y de X tiene cotas inferiores. Por lo tanto el conjunto

$$Z := \{y \in X : y \leq x \text{ para todo } x \in Y\}$$

no es vacío. Denotemos con z al supremo de Z. Como cada $x \in Y$ es una cota superior de Z se sigue de la misma definición de supremo, que $z \leq x$ para todo $x \in Y$. Supongamos ahora que $w \leq x$ para todo $x \in Y$. Entonces $w \in Z$ y así $w \leq z$. Por lo tanto z es el ínfimo de Y. Un razonamiento similar prueba que 3) $\Rightarrow$ 1). □

Un *morfismo* de reticulados completos $f\colon X \to X'$ es una terna (X, f, X'), donde f es una función del conjunto subyacente de X en el de X', que es creciente y preserva supremos e ínfimo. En símbolos:

- $x_1 \leq x_2 \Rightarrow f(x_1) \leq f(x_2)$ para todo $x_1, x_2 \in X$,
- $f(\bigwedge_{i\in I} x_i) = \bigwedge_{i\in I} f(x_i)$ para toda familia $(x_i)_{i\in I}$ de elementos de X,
- $f(\bigvee_{i\in I} x_i) = \bigvee_{i\in I} f(x_i)$ para toda familia $(x_i)_{i\in I}$ de elementos de X.

El reticulado completo X es el dominio, y X' el codominio. Las condiciones pedidas son redundantes. De hecho, no es difícil probar que cualquiera de las dos últimas implica la primera. En efecto, si $x < y$ en X, entonces $x = x \wedge y$ e $y = x \vee y$, y por lo tanto, de la segunda afirmación se sigue que $f(x) = f(x) \wedge f(y)$, mientras que de la tercera, se sigue que $f(y) = f(x) \vee f(y)$. En ambos caso obtenemos que $f(x) \leq f(y)$. Un morfismo de reticulados completos $f\colon X \to X'$ es un *isomorfismo* si hay un morfismo $f^{-1}\colon X' \to X$, llamado la *inversa* de f, tal que $f^{-1} \circ f = \mathrm{id}_X$ y $f \circ f^{-1} = \mathrm{id}_{X'}$. Usaremos el siguiente resultado.

PROPOSICIÓN 13.10. *Consideremos dos reticulados completeos X y X' y una función f, del conjunto subyacente de X en el de X'. Si f es biyectiva y tanto f como f^{-1} preservan el orden, entonces f es un isomorfismo de reticulados.*

DEMOSTRACIÓN. Consideremos una familia arbitraria $(x_i)_{i\in I}$ de elementos de X. Dado que $\bigwedge_{i\in I} x_i \leq x_j$ para todo $j \in I$, se sigue de la hipótesis acerca de f, que $f\left(\bigwedge_{i\in I} x_i\right) \leq f(x_j)$ para todo $j \in I$. Por lo tanto $f(\bigwedge_{i\in I} x_i) \leq \bigwedge_{i\in I} f(x_i)$. El mismo argumento, pero usando la hipótesis acerca de f^{-1} y aplicado a la familia $(f(x_i))_{i\in I}$ de elementos de X', demuestra que $f^{-1}(\bigwedge_{i\in I} f(x_i)) \leq \bigwedge_{i\in I} x_i$. En consecuencia $\bigwedge_{i\in I} f(x_i) \leq f(\bigwedge_{i\in I} x_i)$ y, así, f respeta ínfimos. Un argumento similar muestra que f^{-1} también lo hace y, que además, ambas funciones respetan supremos. □

TEOREMA 13.11 (Teorema de la correspondencia). *Si $\varphi\colon G \to G'$ es un morfismo sobreyectivo de grupos, entonces las funciones*

$$\begin{array}{ccc} \mathrm{Sub}_{\ker\varphi}(G) & \longrightarrow & \mathrm{Sub}(G') \\ H & \longmapsto & \varphi(H) \end{array} \qquad y \qquad \begin{array}{ccc} \mathrm{Sub}(G') & \longrightarrow & \mathrm{Sub}_{\ker\varphi}(G) \\ H' & \longmapsto & \varphi^{-1}(H') \end{array}$$

son isomorfismos de reticulados, inversos uno del otro. Esta correspondencia tiene las siguientes propiedades:

- $|L : H| = |\varphi(L) : \varphi(H)|$,
- $H \lhd L$ *si y sólo si* $\varphi(H) \lhd \varphi(L)$, *y entonces* $L/H \simeq \varphi(L)/\varphi(H)$.

para cada $H, L \in \mathrm{Sub}_{\ker\varphi}(G)$ *con* $H \leq L$.

DEMOSTRACIÓN. Es claro que si $\ker\varphi \leq H \leq L \leq G$, entonces $\varphi(H) \leq \varphi(L) \leq G'$; y que si $H' \leq L' \leq G'$, entonces $\varphi^{-1}(H') \leq \varphi^{-1}(L') \leq G$. Como φ es sobreyectiva,

$$\varphi(\varphi^{-1}(H')) = H'$$

para todo subconjunto H' de G'. Además,

$$\varphi^{-1}(\varphi(H)) = H\ker\varphi$$

para cada $H \leq G$, porque

$$g \in \varphi^{-1}(\varphi(H)) \Leftrightarrow \exists\, h \in H \text{ tal que } \varphi(g) = \varphi(h) \Leftrightarrow \exists\, h \in H \text{ tal que } h^{-1}g \in \ker\varphi,$$

cualquiera sea $g \in G$. La primera afirmación es una consecuencia inmediata de estas observaciones.

Para probar que si $\ker\varphi \leq H \leq L$, entonces $|L : H| = |\varphi(L) : \varphi(H)|$, será suficiente mostrar que la correspondencia $lH \mapsto \varphi(l)\varphi(H)$, del conjunto de las coclases a izquierda de H en L en el de las coclases a izquierda de $\varphi(H)$ en $\varphi(L)$, es biyectiva. Pero es evidente que esta es sobreyectiva, y es inyectiva porque

$$\varphi(l)\varphi(H) = \varphi(l')\varphi(H) \Rightarrow \varphi(l^{-1}l') \in \varphi(H) \Rightarrow l^{-1}l' \in H \Rightarrow lH = l'H.$$

Además, los resultados obtenidos al comienzo de la Sección 12 muestran en particular que $H \lhd L$ si y sólo si $\varphi(H) \lhd \varphi(L)$. Resta ver que

$$\frac{L}{H} \simeq \frac{\varphi(L)}{\varphi(H)},$$

lo que se sigue del primer teorema del isomorfismo aplicado al morfismo de L en $\varphi(L)/\varphi(H)$ obtenido componiendo φ con el epimorfismo canónico $\pi\colon \varphi(L) \to \varphi(L)/\varphi(H)$. □

OBSERVACIÓN 13.12. *Por el teorema anterior si $\varphi\colon G \to G'$ es un morfismo sobreyectivo de grupos y H es un subgrupo de G, entonces $|G' : \varphi(H)| = |G : H\ker\varphi|$ y, por lo tanto, divide a $|G : H|$.*

DEFINICIÓN 13.13. *Un grupo G es* simple *si $G \neq 1$ y $H \lhd G \Rightarrow H = 1$ o $H = G$.*

DEFINICIÓN 13.14. *Un subgrupo normal H de un grupo G es* maximal *si es propio y no existe ningún subgrupo normal L de G tal que $H \subsetneq L \subsetneq G$.*

COROLARIO 13.15. *$H \lhd G$ es maximal si y sólo si G/H es simple.*

Consideremos un morfismo de grupos $\varphi\colon G\to G'$ y subgrupos normales H de G y H' de G'. Si $\varphi(H)\subseteq H'$, entonces existe un único morfismo $\overline{\varphi}\colon G/H\to G'/H'$ tal que el cuadrado

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi'} \\ G/H & \xrightarrow{\overline{\varphi}} & G'/H', \end{array}$$

donde π y π' son las proyecciones canónicas, conmuta. De hecho, esto es una consecuencia directa de la propiedad universal del cociente. Recordemos que cuando establecimos dicha propiedad, calculamos también el núcleo y la imagen del morfismo inducido. De los resultados obtenidos en ese momento se deduce de inmediato que

$$\operatorname{Im}\overline{\varphi}=\frac{\varphi(G)H'}{H'}\qquad\text{y}\qquad\ker\overline{\varphi}=\frac{\varphi^{-1}(H')}{H}.$$

Proposición 13.16. *La construcción anterior tiene las siguientes propiedades:*

1. *Para todo $H\lhd G$, el morfismo $\overline{\mathrm{id}}\colon G/H\to G/H$ es la identidad de G/H.*
2. *Consideremos morfismos de grupos $\varphi\colon G\to G'$ y $\psi\colon G'\to G''$ y subgrupos normales H de G, H' de G' y H'' de G''. Si $\varphi(H)\subseteq H'$ y $\psi(H')\subseteq H''$, entonces $(\psi\circ\varphi)(H)\subseteq H''$ y $\overline{\psi\circ\varphi}=\overline{\psi}\circ\overline{\varphi}$.*

Demostración. Por la unicidad de los morfismos $\overline{\mathrm{id}}$ y $\overline{\psi\circ\varphi}$, basta observar que el cuadrado

$$\begin{array}{ccc} G & \xrightarrow{\mathrm{id}} & G \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\ G/H & \xrightarrow{\mathrm{id}} & G/H \end{array}$$

y el rectángulo exterior del diagrama

$$\begin{array}{ccccc} G & \xrightarrow{\varphi} & G' & \xrightarrow{\psi} & G'' \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi'} & & \downarrow{\scriptstyle\pi''} \\ G/H & \xrightarrow{\overline{\varphi}} & G'/H' & \xrightarrow{\overline{\psi}} & G''/H'' \end{array}$$

conmutan. □

Ejercicio 13.17. *Pruebe que si $\varphi\colon G\to G'$ es un morfismo de grupos y $H'\lhd G'$, entonces $\varphi^{-1}(H')\lhd G$ y existe un único morfismo inyectivo $\overline{\varphi}\colon G/\varphi^{-1}(H')\to G'/H'$ de grupos, tal que el diagrama*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi'} \\ G/\varphi^{-1}(H') & \xrightarrow{\overline{\varphi}} & G'/H', \end{array}$$

donde $\pi\colon G\to G/\varphi^{-1}(H')$ y $\pi'\colon G'\to G'/H'$ son las proyecciones canónicas, conmuta. Pruebe también que $\operatorname{Im}\overline{\varphi}=\frac{H'\operatorname{Im}\varphi}{H'}$.

14. Grupos libres y presentaciones

Intuitivamente, dar una presentación de un grupo G es dar un conjunto de generadores X de G y un conjunto de relaciones que los elementos de X satisfacen y que determinan G. Por ejemplo, en la Sección 5 introdujimos los grupos diedral D_n y cuaterniónico generalizado H_n para cada número natural $n > 1$, y vimos que el primero tiene generadores x, y que satisfacen las relaciones

$$x^n = 1, \quad y^2 = 1 \quad \text{e} \quad yxy^{-1} = x^{-1},$$

y el segundo, generadores x, y que satisfacen las relaciones

$$x^n = y^2 \quad \text{e} \quad yxy^{-1} = x^{-1}.$$

En esta sección precisamos el concepto de presentación y mostramos que las anteriores son, efectivamente, presentaciones de los grupos diedrales y cuaterniónicos. Para ello necesitamos primero introducir los grupos libres, los cuales, a groso modo, pueden describirse como aquellos con un conjunto de generadores que no satisfacen ninguna relación, salvo las determinadas por los axiomas de grupo.

14.1. Grupos libres

Para cada conjunto X, denotamos con $X^{\pm 1}$ a la unión disjunta de dos copias X^{+1} y X^{-1} de X. Para cada elemento $x \in X$ hay un elemento correspondiente $x^{+1} \in X^{+1}$ y otro $x^{-1} \in X^{-1}$. Nosotros diremos que x^{+1} y x^{-1} están *asociados*. Una *palabra en* X es una expresión

$$w := x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n} \qquad (\text{con } x_{\alpha_i} \in X \text{ y } \epsilon_i = \pm 1 \text{ para } i = 1, \ldots, n).$$

Si en la misma ningún símbolo aparece junto a su asociado, decimos que w es una palabra *reducida*. La cantidad n de símbolos que tiene, es la *longitud* $l(w)$ de w. Consideramos también como una palabra reducida a la expresión vacía. Por definición, esta palabra tiene longitud cero. Nuestro próximo objetivo será definir el *producto* $w_1 w_2$ de dos palabras reducidas

$$w_1 := x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n} \quad \text{y} \quad w_2 := x_{\beta_1}^{\delta_1} \cdots x_{\beta_m}^{\delta_m}.$$

Para ello escribimos

$$x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n} x_{\beta_1}^{\delta_1} \cdots x_{\beta_m}^{\delta_m}. \tag{13}$$

Si esta es una palabra reducida, entonces ponemos

$$w_1 w_2 := x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n} x_{\beta_1}^{\delta_1} \cdots x_{\beta_m}^{\delta_m}.$$

Si no, primero eliminamos de (13) sucesivamente pares de símbolos asociados, hasta obtener una que lo sea.

Teorema 14.1. *El conjunto $L(X)$, de la palabras reducidas en X, es un grupo vía el producto que acabamos de definir.*

Demostración. Es claro que la palabra vacía es el elemento neutro. Probaremos ahora por inducción en $l(w_2)$, que

$$w_1(w_2 w_3) = (w_1 w_2) w_3$$

para toda terna w_1, w_2, w_3 de palabras reducidas. Si $l(w_2) = 1$ (esto es, si $w_2 = x^\epsilon$ con $x \in X$ y $\epsilon = \pm 1$) hay cuatro casos para analizar: que el último símbolo de w_1 y el primero de w_3 sean distintos del elemento de $X^{\pm 1}$ asociado a x^ϵ; que el último símbolo de w_1 sea el elemento

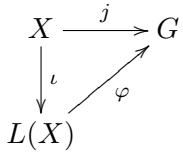
de $X^{\pm 1}$ asociado a x^ϵ, pero que el primero de w_3 no lo sea; que el primer símbolo de w_3 sea el elemento de $X^{\pm 1}$ asociado a x^ϵ, pero que el último de w_1 no lo sea; y que el último símbolo que w_1 y el primero de w_3 sean el elemento de $X^{\pm 1}$ asociado a x^ϵ. Es fácil ver que en todos vale que $w_1(w_2w_3) = (w_1w_2)w_3$. Supongamos ahora que la asociatividad vale cuando $l(w_2) \leq n$ y que $l(w_2) = n+1$. Escribamos $w_2 = w_2'x^\epsilon$. Entonces, por hipótesis inductiva

$$\begin{aligned} w_1(w_2w_3) &= w_1((w_2'x^\epsilon)w_3) \\ &= w_1(w_2'(x^\epsilon w_3)) \\ &= (w_1w_2')(x^\epsilon w_3) \\ &= ((w_1w_2')x^\epsilon)w_3 \\ &= (w_1(w_2'x^\epsilon))w_3 \\ &= (w_1w_2)w_3. \end{aligned}$$

Resta probar que cada palabra reducida es inversible, pero es claro que la inversa de la palabra reducida $x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n}$ es la palabra $x_{\alpha_n}^{-\epsilon_n} \cdots x_{\alpha_1}^{-\epsilon_1}$. □

El *grupo libre sobre un conjunto* X es, por definición, el grupo $L(X)$ construído arriba. Identificando cada elemento $x \in X$ con la palabra reducida x^{+1}, obtenemos una aplicación canónica $\iota\colon X \to L(X)$. Claramente $\iota(X)$ genera $L(X)$ como grupo. En el siguiente teorema establecemos la propiedad universal de $(L(X), \iota)$.

Teorema 14.2. *Para cada función $j\colon X \to G$, de X en un grupo G, hay un único morfismo $\varphi\colon L(X) \to G$ que extiende a j. Vale decir, con la propiedad de que el triángulo*



conmuta.

Demostración. Si φ es un morfismo de grupos que extiende a j, forzosamente debe ser

$$\varphi(x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n}) = j(x_{\alpha_1})^{\epsilon_1} \cdots j(x_{\alpha_n})^{\epsilon_n}.$$

Pero es claro que la función definida por esta fórmula es un morfismo de grupos. □

Ampliando un poco la definición dada arriba del Teorema 14.2, diremos que un *grupo libre sobre* X es cualquier par (G, j), formado por un grupo G y una función $j\colon X \to G$, que tiene la misma propiedad universal que $(L(X), \iota)$. Por extensión, en este caso decimos también que G es libre.

Observación 14.3. *Si $l\colon Y \to X$ es una función biyectiva, (G, j) es un grupo libre sobre X y $\psi\colon G \to H$ es un isomorfismo de grupos, entonces $(H, \psi \circ j \circ l)$ es un grupo libre sobre Y.*

Proposición 14.4. *Un par (G, j), formado por un grupo G y una función $j\colon X \to G$, es un grupo libre si y sólo si el morfismo $\varphi\colon L(X) \to G$ cuya existencia y unicidad fue probada en el Teorema 14.2 es un isomorfismo. En consecuencia, j es inyectivo.*

DEMOSTRACIÓN. Por la Observación14.3, si φ es un isomorfismo, entonces (G, j) tiene la propiedad universal de $(L(X), \iota)$. Supongamos ahora que (G, j) tiene esta propiedad. Entonces hay un único morfismo $\psi\colon G \to L(X)$ tal que el triángulo

$$\begin{array}{ccc} X & \xrightarrow{\ j\ } & G \\ {\scriptstyle\iota}\downarrow & \swarrow{\scriptstyle\psi} & \\ L(X) & & \end{array}$$

conmuta y, como

$$\psi \circ \varphi \circ \iota = \psi \circ j = \iota \quad \text{y} \quad \varphi \circ \psi \circ j = \varphi \circ \iota = j,$$

se sigue de las propiedades universales de $(L(X), \iota)$ y (G, j), que

$$\varphi \circ \psi = \mathrm{id}_G \quad \text{y} \quad \psi \circ \varphi = \mathrm{id}_{L(X)},$$

lo que prueba que φ es un isomorfismo. □

Una *base* de un grupo G es cualquier subconjunto X de G tal que el par (G, ι_X), donde $\iota_X\colon X \to G$ es la inclusión canónica de X en G, es un grupo libre. Obviamente esto ocurre si y sólo si el morfismo de $L(X)$ en G, inducido por ι_X, es biyectivo. Es claro que un grupo tiene una base si y sólo si es libre, ya que por la Observación 14.3, si (G, j) es libre, entonces $\operatorname{Im} j$ es una base de G. El siguiente teorema será probado más adelante.

TEOREMA 14.5. *Dos grupos libres $L(X)$ y $L(Y)$ son isomorfos si y sólo si $|X| = |Y|$. Equivalentemente, todas las bases de un grupo libre G tienen el mismo cardinal.*

Este resultado permite definir el *rango* de un grupo libre como el cardinal de cualquiera de sus bases. Los grupos libres de rango 1 son los grupos cíclicos infinitos. Por otra parte si $|X| \geq 2$, entonces $L(X)$ no es conmutativo, porque si x_1 y x_2 son elementos distintos de X, entonces $x_1^{+1}x_2^{+1} \neq x_2^{+1}x_1^{+1}$.

PROPOSICIÓN 14.6. *Todo grupo es isomorfo a un cociente de un grupo libre.*

DEMOSTRACIÓN. Si X es un conjunto de generadores de G, entonces el único morfismo

$$\varphi\colon L(X) \to G$$

que extiende a la inclusión canónica de X en G es sobreyectivo. Así, por el primer teorema del isomorfismo, $G \simeq L(X)/\ker\varphi$. □

14.2. Presentaciones

Si $G = L(X)/N$ es un cociente de un grupo libre $L(X)$ por un subgrupo normal N, decimos que G es el *grupo generado por los elementos de X, sujetos a las relaciones dadas por los elementos de N*, los cuales son las palabras reducidas

$$x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n}$$

de $L(X)$, que se convierten en 1 al pasar al cociente. Decimos que un subconjunto R de N es un *conjunto de relaciones para G* y que (X, R) es una *presentación* de G, si N es el subgrupo normal de G generado por R. Además, en este caso escribimos $G = \langle X|R\rangle$. Por la Proposición 14.6, todo grupo tiene una presentación, o es isomorfo a uno que la tiene. Un grupo es *finitamente presentado* si es isomorfo a un grupo $\langle X|R\rangle$, con X y R finitos. Por razones estéticas escribiremos $\langle x_1, \ldots, x_n|p_1, \ldots, p_m\rangle$ en lugar de $\langle\{x_1, \ldots, x_n\}|\{p_1, \ldots, p_m\}\rangle$.

Si $G = \langle x_1, \ldots, x_n | p_1, \ldots, p_m \rangle$, entonces también decimos que G es el *grupo con generadores* $x_1, \ldots, x_n$ *sujetos a las relaciones* $p_1 = 1, \ldots, p_m = 1$. Recordemos que para cada grupo cociente G/N, de un grupo G por un subgrupo normal N, y cada elemento $g \in G$, el símbolo $[g]$ denota a la clase de g en G/N.

EJEMPLO 14.7. $\langle x|\emptyset\rangle \simeq \mathbb{Z}$.

EJEMPLO 14.8. *Por las propiedades universales del grupo libre y del cociente, hay un único morfismo*

$$p\colon \langle x|x^n\rangle \to \mathbb{Z}_n,$$

que envía x *a* 1. *Dado que* p *es sobreyectiva y* $\langle x|x^n\rangle$ *tiene a lo sumo* n *elementos,* p *es un isomorfismo y, en consecuencia,* $\langle x|x^n\rangle$ *es un grupo cíclico de orden* n.

EJEMPLO 14.9. *Por la propiedades universales del grupo libre y del cociente, hay un único morfismo*

$$p\colon \langle x_1, x_2 | x_1^{n_1}, x_2^{n_2}, x_1x_2x_1^{-1}x_2^{-1}\rangle \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2},$$

que envía x_1 *a* $(1,0)$ *y* x_2 *a* $(0,1)$. *Usando que*

$$[x_1]^{n_1} = [x_2]^{n_2} = [x_1][x_2][x_1]^{-1}[x_2]^{-1} = 1$$

es fácil probar que el conjunto subyacente del grupo $\langle x_1, x_2 | x_1^{n_1}, x_2^{n_2}, x_1x_2x_1^{-1}x_2^{-1}\rangle$ *es*

$$\{[x_1]^i[x_2]^j : 0 \le i < n_1 \text{ y } 0 \le j < n_2\}.$$

En consecuencia,

$$|\langle x_1, x_2 | x_1^{n_1}, x_2^{n_2}, x_1x_2x_1^{-1}x_2^{-1}\rangle| \le n_1n_2.$$

Como p *es sobreyectivo y* $|\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}| = n_1n_2$, *esto implica que*

$$\langle x_1, x_2 | x_1^{n_1}, x_2^{n_2}, x_1x_2x_1^{-1}x_2^{-1}\rangle \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}.$$

EJEMPLO 14.10. *Recordemos que el grupo diedral* D_n *es el subgrupo de* $\mathrm{GL}(2,\mathbb{R})$ *generado por las matrices*

$$x := \begin{pmatrix} \cos\theta & \operatorname{sen}\theta \\ -\operatorname{sen}\theta & \cos\theta \end{pmatrix} \qquad e \qquad y := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

donde $\theta = 2\pi/n$ *con* $n > 1$. *Como* $x^n = y^2 = yxy^{-1}x = 1$ *hay un único morfismo*

$$p\colon \langle x_1, x_2 | x_1^n, x_2^2, x_2x_1x_2^{-1}x_1\rangle \to D_n,$$

que envía x_1 *a* x *y* x_2 *a* y. *Dado que*

$$[x_1]^n = [x_2]^2 = [x_2][x_1][x_2]^{-1}[x_1] = 1,$$

el conjunto subyacente del grupo $\langle x_1, x_2 | x_1^n, x_2^2, x_2x_1x_2^{-1}x_1\rangle$ *es*

$$\{1, [x_1], \ldots, [x_1]^{n-1}, [x_2], [x_1][x_2], \ldots, [x_1]^{n-1}[x_2]\}$$

y, en consecuencia,

$$|\langle x_1, x_2 | x_1^n, x_2^2, x_2x_1x_2^{-1}x_1\rangle| \le 2n.$$

Como $|D_n| = 2n$ *y* p *es sobreyectivo, de esto se sigue que*

$$\langle x_1, x_2 | x_1^n, x_2^2, x_2x_1x_2^{-1}x_1\rangle \simeq D_n.$$

EJEMPLO 14.11. *Recordemos que el grupo cuaterniónico generalizado H_n es el subgrupo de $\mathrm{GL}(2,\mathbb{C})$ generado por las matrices*

$$x := \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix} \qquad e \qquad y := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

donde $w := e^{i\pi/n}$ con $n > 1$. Dado que $x^n = y^2$ e $yxy^{-1} = x^{-1}$, hay un único morfismo

$$p\colon \langle x_1, x_2 | x_1^n x_2^{-2}, x_2 x_1 x_2^{-1} x_1 \rangle \to H_n,$$

que envía x_1 a x y x_2 a y. Usando las igualdades

$$[x_1]^n = [x_2]^2 \quad y \quad [x_2][x_1][x_2]^{-1} = [x_1]^{-1},$$

y razonando como en el Ejemplo 5.9, es fácil probar que $[x_1]^{2n} = 1$. Es evidente ahora que el conjunto subyacente del grupo $\langle x_1, x_2 | x_1^n x_2^{-2}, x_2 x_1 x_2^{-1} x_1 \rangle$ es

$$\{1, [x_1], \ldots, [x_1]^{2n-1}, [x_2], [x_1][x_2], \ldots, [x_1]^{2n-1}[x_2]\}.$$

En consecuencia,

$$|\langle x_1, x_2 | x_1^n x_2^{-2}, x_2 x_1 x_2^{-1} x_1 \rangle| \leq 4n$$

y, por lo tanto, como $|H_n| = 4n$ y p es sobreyectivo,

$$\langle x_1, x_2 | x_1^n x_2^{-2}, x_2 x_1 x_2^{-1} x_1 \rangle \simeq H_n.$$

OBSERVACIÓN 14.12. *En los últimos dos ejemplos solamente se usaron las relaciones que satisfacían x e y, nunca que eran matrices. De hecho, los argumentos dados prueban que todo grupo de orden $2n$ generado por un conjunto $\{x, y\}$ de dos elementos que satisfacen $x^n = 1$, $y^2 = 1$ e $yxy^{-1} = x^{-1}$ es isomorfo a $\langle x_1, x_2 | x_1^n, x_2^2, x_2 x_1 x_2^{-1} x_1 \rangle$, y todo grupo de orden $4n$ generado por un conjunto $\{x, y\}$ de dos elementos que satisfacen $x^n = y^2$ e $yxy^{-1} = x^{-1}$ es isomorfo a $\langle x_1, x_2 | x_1^n x_2^{-2}, x_2 x_1 x_2^{-1} x_1 \rangle$.*

EJEMPLO 14.13. *Es trivial que para todo divisor $r > 1$ de n, el cociente $D_n/\langle x^{n/r} \rangle$ está generado por los elementos $[x]$ e $[y]$ sujetos a las relaciones $[x]^r = [y]^2 = [y][x][y]^{-1}[x] = 1$, y que su orden es $2r$. Por lo tanto $D_n/\langle x^{n/r} \rangle$ es isomorfo a D_r.*

EJEMPLO 14.14. *Razonando como en el ejemplo anterior se comprueba fácilmente que, para todo divisor $r > 1$ de n, el cociente $H_n/\langle x^{n/r} \rangle$ es isomorfo a H_r.*

OBSERVACIÓN 14.15 (Descripción de conjuntos de homomorfismos). *Por la propiedad universal de los grupos libres, para cada grupo G y cada conjunto X, la aplicación*

$$\theta\colon \mathrm{Hom}(L(X), G) \to G^X,$$

que cada morfismo f le asigna su restricción $f_{|X}$ a X, es biyectiva. Por ejemplo, si $\langle x \rangle$ es un grupo cíclico infinito, entonces

$$\theta\colon \mathrm{Hom}(\langle x \rangle, G) \to G$$

es la función biyectiva dada por $\theta(f) = f(x)$. Ahora, por la propiedad universal del cociente, si $R = \{r_i : i \in I\}$ es una familia de elementos de $L(X)$, entonces la aplicación

$$\overline{\theta}\colon \mathrm{Hom}(L(X)/\overline{\langle R \rangle}, G) \to G^X,$$

definida por $\overline{\theta}(f)(x) = f([x])$, es inyectiva, y su imagen es el conjunto de todas la funciones $h\colon X \to G$ tales que para cada $i \in I$, reemplazando en r_i cada $x \in X$ por $h(x)$, se obtiene el elemento neutro de G. Por ejemplo, si $\langle x \rangle$ es un grupo cíclico de orden n, entonces

$$\mathrm{Hom}(\langle x \rangle, G) \simeq \{a \in G : a^n = 1\}.$$

Similarmente,

$$\mathrm{Hom}(D_n, G) \simeq \{(a,b) \in G \times G : \ a^n = 1,\ b^2 = 1 \ y\ bab^{-1}a = 1\}$$

y

$$\mathrm{Hom}(H_n, G) \simeq \{(a,b) \in G \times G : \ a^n b^{-2} = 1 \ y\ bab^{-1}a = 1\}.$$

Notemos que si G es un grupo abeliano y consideramos a G^X como un grupo abeliano via la operación $(\varphi + \psi)(x) := \varphi(x) + \psi(x)$, entonces $\overline{\theta}$ es un morfismo de grupos (ver la Subsección 11.1).

Ejemplo 14.16. *Consideremos $n, m \in \mathbb{N}$ mayores que 1 tales que n es un múltiplo impar de m y escribamos $H_n = \langle x, y\rangle$ y $H_m = \langle \bar{x}, \bar{y}\rangle$ donde x, y, $\bar{x}$ y $\bar{y}$ satisfacen*

$$x^n = y^2, \quad yxy^{-1} = x^{-1}, \quad \bar{x}^m = \bar{y}^2 \quad e \quad \bar{y}\bar{x}\bar{y}^{-1} = \bar{x}^{-1}.$$

Como n/m es impar,

$$\bar{x}^n = (\bar{x}^m)^{\frac{n}{m}} = (\bar{y}^2)^{\frac{n}{m}} = \bar{y}^2$$

y, por lo tanto, existe un morfismo sobreyectivo $\pi\colon H_n \to H_m$ tal que $\pi(x) = \bar{x}$ y $\pi(y) = \bar{y}$. Es fácil ver que el núcleo de este morfismo es $\langle x^{2m}\rangle$. Dejamos los detalles de esto último al lector.

Ejemplo 14.17. *Consideremos un grupo cíclico $C_n := \langle x\rangle$ de orden n. Por la Observación 14.15, para cada $i \geq 0$ hay un morfismo*

$$\upsilon_i\colon C_n \to C_n$$

tal que $\upsilon_i(x) := x^i$. Como $\upsilon_i(x^j) = x^{ji} = 1$ si y sólo si ji es múltiplo de n, el núcleo de υ_i es $\langle x^{n/(n:i)}\rangle$, donde, como en el Ejemplo 5.8, el símbolo $(n:i)$ denota al máximo divisor común de n e i. En particular υ_i es un automorfismo si y sólo si i es coprimo con n. Por lo tanto la aplicación

$$\phi\colon \mathrm{Aut}(C_n) \to U(\mathbb{Z}_n)$$

definida por $\phi(f) := i$ si $f(x) = x^i$ es una biyección que claramente es un morfismo de grupos.

Ejemplo 14.18. *Recordemos que el grupo diedral D_n está generado por dos elementos x e y sujetos a las relaciones $x^n = 1$, $y^2 = 1$ e $yxy^{-1}x = 1$, y que*

$$D_n = \{1, x, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y\}.$$

Supongamos que $n > 2$ y que $f \in \mathrm{Aut}(D_n)$. Como los órdenes de x y $f(x)$ coinciden, necesariamente $f(x) = x^i$ con $0 \leq i < n$ e i coprimo con n. Así f define por restricción un automorfismo de $\langle x\rangle$. En consecuencia existe $0 \leq j < n$ tal que $f(y) = x^j y$. Por lo tanto queda definida una aplicación inyectiva

$$\phi\colon \mathrm{Aut}(D_n) \to \mathbb{Z}_n \times U(\mathbb{Z}_n),$$

tal que $\phi(f) := (j, i)$ si $f(y) = x^j y$ y $f(x) = x^i$. Se sigue fácilmente de la Observación 14.15 que ϕ también es sobreyectiva. Supongamos ahora que g es otro automorfismo del grupo D_n y que $g(x) = x^{i'}$ y $g(y) = x^{j'}y$. Como

$$g(f(x)) = g(x^i) = g(x)^i = x^{i'i} \quad y \quad g(f(y)) = g(x^j y) = g(x)^j g(y) = x^{i'j} x^{j'} y = x^{i'j+j'} y,$$

es evidente que ϕ se convierte en un isomorfismo de grupos si definimos el producto en el codominio de ϕ por $(j', i')(j, i) := (i'j + j', i'i)$.

EJEMPLO 14.19. *Recordemos ahora que H_n es un grupo generado por dos elementos x, y sujetos a las relaciones $x^n y^{-2} = 1$ e $yxy^{-1}x = 1$ y que*

$$H_n = \{1, x, \ldots, x^{2n-1}, y, xy, \ldots, x^{2n-1}y\}.$$

Supongamos que $n > 2$. El mismo razonamiento que el realizado en el ejemplo anterior muestra que hay una biyección

$$\phi\colon \operatorname{Aut}(H_n) \to \mathbb{Z}_{2n} \times U(\mathbb{Z}_{2n}),$$

tal que $\phi(f) := (j, i)$ si $f(y) = x^j y$ y $f(x) = x^i$, y que ϕ se convierte en un isomorfismo de grupos si definimos el producto en el codominio de ϕ por $(j', i')(j, i) := (i'j + j', i'i)$.

Terminamos esta sección mostrando que los grupos diedrales aparecen naturalmente como subgrupos de grupos finitos.

TEOREMA 14.20. *Si G es un grupo finito, $x, y \in G$ tienen orden 2 e $y \notin \{x, x^{-1}\}$, entonces $\langle x, y\rangle \simeq D_n$, donde n es el orden de yx.*

DEMOSTRACIÓN. Escribamos $s = yx$. Como

$$y^2 = 1, \quad ysy^{-1}s = yyxy^{-1}yx = x^2 = 1 \quad \text{y} \quad \langle x, y\rangle = \langle s, y\rangle,$$

se sigue de la Observación 14.12, que para probar el teorema es suficiente ver que $|\langle x, y\rangle| = 2n$. Ahora bien, debido a las relaciones que aparecen arriba

$$\langle s, y\rangle = \{1, s, \ldots, s^{n-1}, y, sy, \ldots, s^{n-1}y\},$$

y, en consecuencia, $\langle s, y\rangle$ tiene a lo sumo $2n$ elementos. Así, por el teorema de Lagrangre, para terminar la demostración será suficiente ver que el subgrupo de n elementos $\langle s\rangle$ de $\langle s, y\rangle$ es propio, lo que es consecuencia inmediata de que $|x| = |y| = 2$ y de que un grupo cíclico no puede tener dos elementos de orden 2. □

15. Producto directo

Ahora vamos a estudiar una construcción, llamada producto directo de grupos, que es la manera más simple de obtener un nuevo grupo a partir de otros. Comenzamos considerando el producto directo interno, que nos da la forma más sencilla en que un grupo puede recuperase a partir de varios de sus subgrupos. Luego introducimos las nociones de producto directo y producto directo restringido, y estudiamos algunas de sus propiedades y como se relacionan estas construcciones con el producto directo interno.

15.1. Producto directo interno

Consideremos un grupo G y subgrupos $G_1, \ldots, G_n$ de G. Decimos que $G_1 \cdots G_n$ es *producto directo interno de $G_1, \ldots, G_n$* si cada $g \in G_1 \cdots G_n$ se escribe de manera única como un producto

$$g = g_1 \cdots g_n$$

con $g_1 \in G_1, \ldots, g_n \in G_n$ y

$$(g_1 \cdots g_n)(g_1' \cdots g_n') = g_1 g_1' \cdots g_n g_n' \tag{14}$$

para todo $g_1, g_1' \in G_1, \ldots, g_n, g_n' \in G_n$. Es claro que si $G_1 \cdots G_n$ es producto directo interno de $G_1, \ldots, G_n$ entonces $G_1 \cdots G_n$ es un subgrupo de G y que $g_i g_j = g_j g_i$ para cada $g_i \in G_i$ y $g_j \in G_j$, con $i \neq j$. En consecuencia $G_1 \cdots G_n$ es producto directo interno de $G_{\sigma_1}, \ldots, G_{\sigma_n}$

para todo $\sigma \in \mathrm{S}_n$ y $G_i \triangleleft G_1 \cdots G_n$ para todo i. Notemos también que las inclusiones canónicas $\iota_i \colon G_i \to G_1 \cdots G_n$ y las aplicaciones $\pi_i \colon G_1 \cdots G_n \to G_i$, definidas por $\pi_i(g_1 \cdots g_n) = g_i$, son morfismos de grupos, y que

$$g = \prod_{i=1}^{n} (\iota_i \circ \pi_i)(g)$$

para cada $g \in G$.

TEOREMA 15.1. *Consideremos subgrupos normales $G_1, \ldots, G_n$ de un grupo G. Por brevedad, denotemos con $G_{\widehat{i}}$ a $G_1 \cdots \widehat{G_i} \cdots G_n$. Son equivalentes:*

1. *$G_1 \cdots G_n$ es producto directo interno de $G_1, \ldots, G_n$.*
2. *$\bigcap_{i=1}^{n} G_{\widehat{i}} = 1$.*
3. *$G_i \cap G_{\widehat{i}} = 1$ para todo i.*
4. *$G_i \cap (G_1 \ldots G_{i-1}) = 1$ para todo $i > 1$.*
5. *Si $1 = g_1 \cdots g_n$ con $g_1 \in G_1, \ldots, g_n \in G_n$, entonces $g_1 = \cdots = g_n = 1$.*

DEMOSTRACIÓN. 1) $\Rightarrow$ 2) Es trivial.

2) $\Rightarrow$ 3) Porque $G_i \subseteq \bigcap_{j \neq i} G_{\widehat{j}}$.

3) $\Rightarrow$ 4) Es trivial.

4) $\Rightarrow$ 5) Supongamos que el item 5) es falso. Entonces hay un mínimo $j > 1$ tal que existen $g_1 \in G_1, \ldots, g_j \in G_j$ con $g_j^{-1} = g_1 \cdots g_{j-1} \neq 1$. Pero esto se contradice con el item 4).

5) $\Rightarrow$ 1) Veamos primero que $G_i \cap G_j = 1$ cuando $i \neq j$. Para ello podemos suponer que $i < j$ y observar que si $x \in G_i \cap G_j$, entonces $1 = xx^{-1} \in G_i G_j$, debido a lo cual, por hipótesis, $x = 1$. Notemos ahora que $g_i g_j = g_j g_i$ para cada $g_i \in G_i$ y $g_j \in G_j$ con $i \neq j$, porque

$$g_i(g_j g_i^{-1} g_j^{-1}) = (g_i g_j g_i^{-1}) g_j^{-1} \in G_i \cap G_j = 1.$$

Pero entonces

$$g_1 \cdots g_n = h_1 \cdots h_n \Rightarrow g_1 h_1^{-1} \cdots g_n h_n^{-1} = 1 \Rightarrow g_1 = h_1, \ldots, g_n = h_n,$$

para todo $g_1, h_1 \in G_1, \ldots, g_n, h_n \in G_n$, y además la multiplicación de G está dado por la fórmula (14). □

COROLARIO 15.2. *Supongamos que $G_1, \ldots, G_n$ son subgrupos normales finitos de un grupo G. Si $|G_i|$ es coprimo con $|G_j|$ siempre que $i \neq j$, entonces $G_1 \cdots G_n$ es producto directo interno de $G_1, \ldots, G_n$.*

DEMOSTRACIÓN. Tomemos $1 < i \neq n$. Por la Proposición 8.2,

$$|G_1 \cdots G_{i-1}| \text{ divide a } |G_1| \cdots |G_{i-1}|$$

y, por lo tanto, es coprimo con $|G_i|$. En consecuencia $G_i \cap (G_1 \cdots G_{i-1}) = 1$ y, así, debido a la equivalencia entre los items 1) y 4) del teorema anterior, $G_1 \cdots G_n$ es producto directo interno de $G_1, \ldots, G_n$. □

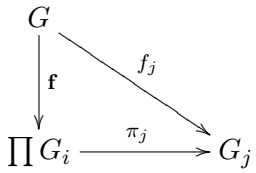
EJEMPLO 15.3. *Consideremos $n \in \mathbb{N}$ impar y mayor que 1 y $D_{2n} = \langle x, y \rangle$ donde x e y satisfacen $x^{2n} = y^2 = 1$ e $yxy^{-1} = x^{-1}$. Como $\langle x^2, y \rangle \cap \langle x^n \rangle = 1$ y $\langle x^2, y \rangle$ y $\langle x^n \rangle$ son subgrupos normales de D_{2n}, se sigue del teorema anterior que D_{2n} es el producto directo interno de $\langle x^2, y \rangle$ y $\langle x^n \rangle$. Notemos que $\langle x^2, y \rangle \simeq D_n$ y $\langle x^n \rangle \simeq \mathbb{Z}_2$.*

15.2. Producto directo

El *producto directo* $\prod_{i\in I} G_i$ de una familia de grupos $(G_i)_{i\in I}$, es un grupo vía la multiplicación coordenada a coordenada. Esta operación está definida adrede para que las proyecciones canónicas $\pi_j\colon \prod_{i\in I} G_i \to G_j$ sean morfismos de grupos. Cuando no haya posibilidad de confusión escribiremos $\prod G_i$ en lugar de $\prod_{i\in I} G_i$, y también haremos muchas otras simplificaciones similares sin prevenir antes al lector, cuando resulte evidente que pueden realizarse sin riesgo de perder claridad en la exposición. Además, siguiendo una costumbre bien establecida escribiremos $G_1 \times \cdots \times G_n$ en lugar de $\prod_{i\in \mathbb{I}_n} G_i$, donde $\mathbb{I}_n$ denota al conjunto de los primeros n números naturales.

El producto directo tiene la siguiente propiedad universal:

- Para cada familia $(f_i\colon G \to G_i)_{i\in I}$ de morfismos de grupos, existe un único morfismo $\mathbf{f}\colon G \to \prod G_i$ tal que para cada $j \in I$ el diagrama



  conmuta.

Claramente $\mathbf{f}(g) = (f_i(g))_{i\in I}$ y $\ker \mathbf{f} = \bigcap \ker(f_i)$. Una manera equivalente de establecer la propiedad universal de $\prod G_i$ es diciendo que, para cada grupo G, la correspondencia

$$\begin{aligned} \operatorname{Hom}\big(G, \textstyle\prod G_i\big) &\xrightarrow{\ \Psi\ } \prod \operatorname{Hom}(G, G_i) \\ f &\longmapsto (\pi_i \circ f)_{i\in I} \end{aligned}$$

es biyectiva. Es fácil ver que si los G_i's son conmutativos, entonces Ψ también es un morfismo de grupos.

Observación 15.4. *Consideremos subgrupos normales $G_1, \ldots, G_n$ de un grupo G. Como en el Teorema 15.1, escribamos $G_{\widehat{i}} := G_1 \cdots \widehat{G_i} \cdots G_n$. Por la propiedad universal del producto, las proyecciones canónicas $\pi_{\widehat{i}}\colon G \to G/G_{\widehat{i}}$ inducen un morfismo*

$$G \xrightarrow{\ \boldsymbol{\pi}\ } G/G_{\widehat{1}} \times \cdots \times G/G_{\widehat{n}}\ ,$$

cuyo núcleo es $\bigcap_{i=1}^n G_{\widehat{i}}$. Afirmamos que $\boldsymbol{\pi}$ es sobreyectivo si y sólo si $G_1 \cdots G_n = G$. En efecto, si se satisface esta condición, entonces para cada $([g_1], \ldots, [g_n]) \in G/G_{\widehat{1}} \times \cdots \times G/G_{\widehat{n}}$, existen $g_{ij} \in G_i$ para $1 \le i, j \le n$, tales que $g_j = g_{1j} \cdots g_{nj}$ para todo j. En consecuencia

$$\boldsymbol{\pi}(g_{11} \cdots g_{nn}) = (\pi_{\widehat{1}}(g_{11}), \ldots, \pi_{\widehat{n}}(g_{nn})) = (\pi_{\widehat{1}}(g_1), \ldots, \pi_{\widehat{n}}(g_n)) = ([g_1], \ldots, [g_n]).$$

Recíprocamente, si $\boldsymbol{\pi}$ es sobreyectivo, entonces para cada $g \in G$ hay un $x \in G$ tal que

$$\boldsymbol{\pi}(x) = ([g], 1, \ldots, 1).$$

En particular $x^{-1}g \in G_{\widehat{1}}$ y $x \in G_{\widehat{2}}$ y, por lo tanto, existen

$$g_2 \in G_2, \ldots, g_n \in G_n \quad y \quad g_1' \in G_1, g_3' \in G_3, \ldots, g_n' \in G_n$$

tales que $g = x g_2 \cdots g_n$ y $x = g_1' g_3' \cdots g_n'$. Pero entonces

$$g = g_1' g_3' \cdots g_n' g_2 \cdots g_n \in G_1 G_3 \cdots G_n G_2 \cdots G_n = G_1 \cdots G_n,$$

donde la última igualdad vale porque $G_iG_j = G_jG_i$ para todo i, j, debido a la Observación 10.6.

COROLARIO 15.5. *El morfismo $\boldsymbol{\pi}$ es biyectivo si y sólo si G es producto directo interno de $G_1, \ldots, G_n$.*

DEMOSTRACIÓN. Por el Teorema 15.1 y de la Observación 15.4. □

PROPOSICIÓN 15.6. *Para cada familia $(f_i\colon H_i \to G_i)_{i\in I}$ de morfismos de grupos, existe un único morfismo*

$$\prod f_i\colon \prod H_i \to \prod G_i$$

tal que los diagramas

$$\begin{array}{ccc} \prod H_i & \xrightarrow{\prod f_i} & \prod G_i \\ \downarrow{\scriptstyle \pi_j} & & \downarrow{\scriptstyle \pi_j} \\ H_j & \xrightarrow{f_j} & G_j \end{array}$$

conmutan.

DEMOSTRACIÓN. Se sigue de la propiedad universal de $\prod G_i$. □

Es fácil ver que

$$\Big(\prod f_i\Big)((h_i)_{i\in I}) = (f_i(h_i))_{i\in I}, \quad \ker\Big(\prod f_i\Big) = \prod \ker(f_i) \quad \text{e} \quad \operatorname{Im}\Big(\prod f_i\Big) = \prod \operatorname{Im}(f_i).$$

OBSERVACIÓN 15.7. *La correspondencia introducida en la Proposición 15.6 tiene las siguientes propiedades:*

1. $\prod \mathrm{id}_{H_i} = \mathrm{id}_{\prod H_i}$.
2. *Para cada par de familias de morfismos de grupos $(f_i\colon H_i \to L_i)_{i\in I}$ y $(g_i\colon L_i \to G_i)_{i\in I}$,*

$$\Big(\prod g_i\Big) \circ \Big(\prod f_i\Big) = \prod (g_i \circ f_i).$$

OBSERVACIÓN 15.8. *Si $H_i \triangleleft G_i$ para todo $i \in I$, entonces la familia de los epimorfismos canónicos $\pi_i\colon G_i \to G_i/H_i$, induce un morfismo sobreyectivo*

$$\prod G_i \xrightarrow{\prod \pi_i} \prod \frac{G_i}{H_i},$$

cuyo núcleo es $\prod H_i$. Por consiguiente,

$$\frac{\prod G_i}{\prod H_i} \simeq \prod \frac{G_i}{H_i}.$$

15.3. Producto directo restringido

El *producto directo restringido* de una familia de grupos $(G_i)_{i\in I}$, es el subgrupo $\bigsqcup_{i\in I} G_i$ de $\prod G_i$ formado por todos los elementos con soporte finito. Esto es:

$$\bigsqcup G_i := \Big\{ g \in \prod G_i : g_i = 1 \text{ salvo para finitos índices } i \in I \Big\}.$$

Las restricciones a $\bigsqcup G_i$ de las proyecciones canónicas son morfismos de grupos, y son importantes, pero hay otros morfismos relacionados con el producto directo restringido, que lo son aún más. Se trata de las *inclusiones canónicas* $\iota_j\colon G_j \to \bigsqcup G_i$, definidas por

$$\iota_j(g)_i := \begin{cases} 1 & \text{si } i \neq j, \\ g & \text{si } i = j. \end{cases}$$

Es evidente que

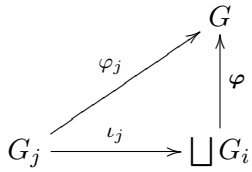
- $\pi_j(\iota_j(g)) = g$ para todo $j \in I$ y $g \in G_j$,
- $\pi_i(\iota_j(g)) = 1$ para todo $i, j \in I$ distintos y $g \in G_j$,
- $\iota_i(g_i)\iota_j(g_j) = \iota_j(g_j)\iota_i(g_i)$ para todo $i, j \in I$ distintos, $g_i \in G_i$ y $g_j \in G_j$,
- $\prod \iota_i(\pi_i(g)) = g$ para todo $g \in \bigsqcup G_i$.

El producto directo restringido también tiene una propiedad universal, y la importancia de las inclusiones canónicas tiene que ver con esto. Recién vimos que las imágenes de inclusiones canónicas distintas ι_i y ι_j conmutan entre si. La familia $(\iota_i)_{i\in I}$ es inicial entre las que satisfacen esta condición. Dicho de otra forma, tiene la siguiente característica:

- Para cada familia morfismos de grupos $(\varphi_i\colon G_i \to G)_{i\in I}$ tal que

  $\varphi_i(g_i)\varphi_j(g_j) = \varphi_j(g_j)\varphi_i(g_i)$ para todo $i, j \in I$ distintos, $g_i \in G_i$ y $g_j \in G_j$,

  existe un único morfismo de grupos $\boldsymbol{\varphi}\colon \bigsqcup G_i \to G$ tal que para cada $j \in I$ el diagrama



  conmuta.

En efecto, si $\boldsymbol{\varphi}$ existe, entonces forzosamente

$$\boldsymbol{\varphi}(g) = \boldsymbol{\varphi}\Big(\prod \iota_j(\pi_j(g))\Big) = \prod \varphi_j(\pi_j(g)),$$

para cada $g \in \bigsqcup G_i$. Así pues sólo debemos probar que la fórmula $\boldsymbol{\varphi}(g) := \prod \varphi_i(\pi_i(g))$ define un morfismo de grupos que tiene la propiedad requerida. Pero

$$\begin{aligned} \boldsymbol{\varphi}(gg') &= \prod \varphi_i(\pi_i(gg')) \\ &= \prod \varphi_i(\pi_i(g)\pi_i(g')) \\ &= \prod \varphi_i(\pi_i(g))\varphi_i(\pi_i(g')) \\ &= \Big(\prod \varphi_i(\pi_i(g))\Big)\Big(\prod \varphi_i(\pi_i(g'))\Big) \\ &= \boldsymbol{\varphi}(g)\boldsymbol{\varphi}(g') \end{aligned}$$

para todo $g, g' \in \bigsqcup G_i$, y

$$\boldsymbol{\varphi} \circ \iota_j(g) = \prod \varphi_i\big(\pi_i(\iota_j(g))\big) = \varphi_j(g)$$

para cada $g \in G_j$. La propiedad universal de $\bigsqcup G_i$ dice que para cada grupo G, la función

$$\Psi\colon \operatorname{Hom}\Big(\bigsqcup G_i, G\Big) \to \prod \operatorname{Hom}(G_i, G),$$

definida por $\Psi(\varphi) := (\varphi \circ \iota_i)_{i\in I}$, es inyectiva y su imagen es

$$\left\{(\varphi_i)_{i\in I} \in \prod_{i\in I} \operatorname{Hom}(G_i, G) : \varphi_h(g_h)\varphi_k(g_k) = \varphi_k(g_k)\varphi_h(g_h)\ \forall\, g_h \in G_h \text{ y } g_k \in G_k \text{ con } h \neq k\right\}.$$

En particular, cuando G es conmutativo, Ψ es biyectiva; y es fácil ver que, en este caso, es un isomorfismo de grupos.

Proposición 15.9. *Para cada familia $(\varphi_i\colon H_i \to G_i)_{i\in I}$ de morfismos de grupos existe un único morfismo*

$$\bigsqcup \varphi_i\colon \bigsqcup H_i \to \bigsqcup G_i$$

tal que los diagramas

$$\begin{array}{ccc} H_j & \xrightarrow{\varphi_j} & G_j \\ \downarrow{\scriptstyle \iota_j} & & \downarrow{\scriptstyle \iota_j} \\ \bigsqcup H_i & \xrightarrow{\bigsqcup \varphi_i} & \bigsqcup G_i \end{array}$$

conmutan.

Demostración. Por la propiedad universal de $\bigsqcup H_i$. □

Es obvio que

$$\Big(\bigsqcup \varphi_i\Big)((g_i)_{i\in I}) = (\varphi_i(g_i))_{i\in I}, \quad \ker\Big(\bigsqcup \varphi_i\Big) = \bigsqcup \ker(\varphi_i) \quad \text{e} \quad \operatorname{Im}\Big(\bigsqcup \varphi_i\Big) = \bigsqcup \operatorname{Im}(\varphi_i).$$

Observación 15.10. *La correspondencia introducida en la Proposición 15.9 tiene las siguientes propiedades:*

1. $\bigsqcup \mathrm{id}_{H_i} = \mathrm{id}_{\bigsqcup H_i}$.
2. *Pra cada par de familias de morfismos de grupos $(\varphi_i\colon H_i \to L_i)_{i\in I}$ y $(\psi_i\colon L_i \to G_i)_{i\in I}$,*

$$\Big(\bigsqcup \psi_i\Big) \circ \Big(\bigsqcup \varphi_i\Big) = \bigsqcup (\psi_i \circ \varphi_i).$$

Observación 15.11. *Si $H_i \triangleleft G_i$ para todo $i \in I$, entonces la familia de las epimorfismos canónicos $\pi_i\colon G_i \to G_i/H_i$, induce un morfismo sobreyectivo*

$$\bigsqcup G_i \xrightarrow{\bigsqcup \pi_i} \bigsqcup \frac{G_i}{H_i},$$

cuyo núcleo es $\bigsqcup H_i$. Por consiguiente,

$$\frac{\bigsqcup G_i}{\bigsqcup H_i} \simeq \bigsqcup \frac{G_i}{H_i}.$$

Ejercicio 15.12. *Pruebe que un elemento $g \in \bigsqcup G_i$ tiene orden finito si y sólo si cada una de sus coordenadas g_i lo tiene, y que el orden de g es el mínimo multiplo común de los ordenes de sus coordenadas.*

OBSERVACIÓN 15.13. *Supongamos que $G_1, \dots, G_n$ son subgrupos de un grupo G. Es fácil ver que la función*

$$\begin{array}{rcl} G_1 \times \cdots \times G_n & \xrightarrow{\varsigma} & G \\ (g_1, \dots, g_n) & \longmapsto & g_1 \cdots g_n \end{array}$$

es un morfismo de grupos si y sólo si los elementos de G_i conmutan con los de G_j para todo $i \neq j$. Es obvio además que, en este caso, vale lo siguiente

- $\ker \varsigma = \{(g_1, \dots, g_n) \in G_1 \times \cdots \times G_n : g_1 \cdots g_n = 1\}$,
- $\operatorname{Im} \varsigma = G_1 \cdots G_n$,
- *si ς es biyectivo, entonces ls G_i's son subgrupos normales de G y la composición $\boldsymbol{\pi} \circ \varsigma$, del isomorfismo $\boldsymbol{\pi}$ introducido en la Observación 15.4, con ς, identifica al subgrupo $\iota_i(G_i)$ de $G_1 \times \cdots \times G_n$ con el subgrupo $\iota_i(G/G_{\widehat{i}})$ de $(G/G_{\widehat{1}}) \times \cdots \times (G/G_{\widehat{n}})$.*

PROPOSICIÓN 15.14. *Si $G_1, \dots, G_n$ son subgrupos de G, entonces son equivalentes:*

1. *$G_1 \cdots G_n$ es producto directo interno de $G_1, \dots, G_n$.*
2. *La función $\varsigma\colon G_1 \times \cdots \times G_n \to G$, definida por $\varsigma(g_1, \dots, g_n) = g_1 \cdots g_n$, es un morfismo inyectivo de grupos.*

DEMOSTRACIÓN. Se lo comprueba inmediatamente a partir de la definición de producto directo interno. □

COROLARIO 15.15. *Supongamos que $G_1, \dots, G_n$ son subgrupos normales finitos de un grupo G. Si $|G_i|$ es coprimo con $|G_j|$ siempre que $i \neq j$, entonces la aplicación*

$$\varsigma\colon G_1 \times \cdots \times G_n \to G,$$

definida por $\varsigma(g_1, \dots, g_n) = g_1 \cdots g_n$, es un morfismo inyectivo de grupos. Además ς es un isomorfismo si y sólo si $|G| = |G_1| \cdots |G_n|$.

DEMOSTRACIÓN. Se sigue inmediatamente del Corolario 15.2 y la Proposición 15.14 que la aplicación ς es un el morfismo inyectivo de grupos. Es obvio que es sobreyectivo si y sólo si $|G| = |G_1| \cdots |G_n|$. □

Recordemos que la función $\phi\colon \mathbb{N} \to \mathbb{N}$ de Euler, presentada arriba del Ejemplo 5.8, asigna a cada número natural el cardinal del conjunto de los enteros no negativos menores que él y coprimos con él.

COROLARIO 15.16. *Si $n = rs$ con $r, s \in \mathbb{N}$ coprimos, entonces $\phi(n) = \phi(r)\phi(s)$.*

DEMOSTRACIÓN. Consideremos un grupo cíclico $\langle g \rangle$ de orden n. Como, por el Corolario 15.15, la aplicación

$$\begin{array}{rcl} \langle g^r \rangle \times \langle g^s \rangle & \xrightarrow{\varphi} & \langle g \rangle \\ (g^{ru}, g^{sv}) & \longmapsto & g^{ru+sv} \end{array}$$

es un isomorfismo, basta observar que

$$\begin{aligned} (g^{ru}, g^{sv}) \text{ genera } \langle g^r \rangle \times \langle g^s \rangle &\Leftrightarrow (g^{ru}, g^{sv}) \text{ tiene orden } n \\ &\Leftrightarrow g^{ru} \text{ tiene orden } s \text{ y } g^{sv} \text{ tiene orden } r \\ &\Leftrightarrow g^{ru} \text{ genera } \langle g^r \rangle \text{ y } g^{sv} \text{ genera } \langle g^s \rangle; \end{aligned}$$

y que $\phi(n)$, $\phi(r)$ y $\phi(s)$ son la cantidad de generadores de $\langle g \rangle$, $\langle g^s \rangle$ y $\langle g^r \rangle$, respectivamente. □

EJERCICIO 15.17. *Supongamos que H y L son dos subgrupos normales distintos de un grupo G. Pruebe que si H es simple y tiene índice 2 en G y L no es trivial, entonces $|L| = 2$ y $G \simeq H \times L$.*

NOTA 15.18. *Si $(G_i)_{i\in I}$ es una familia de subgrupos de un grupo G y los elementos de G_i conmutan con los de G_j para todo $i \neq j$, entonces por la propiedad universal del producto restringido hay un único morfismo*

$$\theta\colon \bigsqcup_{i\in I} G_i \to G$$

tal que $\theta \circ \iota_j$ es la inclusión canónica de G_j en G para todo $j \in J$. Cuando θ es inyectivo decimos que los G_i's están en producto directo interno restringido y denotamos también con $\bigsqcup G_i$ a la imagende θ. Es fácil ver que esto sucede si para cada subconjunto finito $\{i_1, \ldots, i_n\}$ de I, el subgrupo $G_{i_1} \cdots G_{i_n}$ de G, es el producto directo interno de $G_{i_1}, \ldots, G_{i_n}$. En el caso en que todos los grupos involucrados son aditivos se suele decir suma directa *y* suma directa interna *en lugar de producto directo restringido y producto directo interno restringido, respectivamente, y se suele usar el símbolo $\bigoplus$ en lugar del símbolo $\bigsqcup$ (tanto para la suma directa como para la suma directa interna).*

15.4. Morfismos entre productos directos finitos de grupos

Para cada par $\mathbf{H} := (H_1, \ldots, H_r)$ y $\mathbf{K} := (K_1, \ldots, K_s)$ de familias finitas de grupos, denotamos con el símbolo $\mathrm{M}_{s\times r}\big(\mathrm{Hom}(\mathbf{H}, \mathbf{K})\big)$ al conjunto de todas las matrices

$$(\varsigma_{ij}) := \begin{pmatrix} \varsigma_{11} & \cdots & \varsigma_{1r} \\ \vdots & \ddots & \vdots \\ \varsigma_{s1} & \cdots & \varsigma_{sr} \end{pmatrix},$$

con $\varsigma_{ij} \in \mathrm{Hom}(H_j, K_i)$, tales que

$$\varsigma_{ij}(h)\varsigma_{ij'}(h') = \varsigma_{ij'}(h')\varsigma_{ij}(h) \qquad \text{para todo } i,\ j \neq j',\ h \in H_j \text{ y } h' \in H_{j'}.$$

Si $\mathbf{H} = \mathbf{K}$ escribiremos $\mathrm{M}_r\big(\mathrm{End}(\mathbf{H})\big)$ en lugar de $\mathrm{M}_{s\times r}\big(\mathrm{Hom}(\mathbf{H}, \mathbf{K})\big)$.

PROPOSICIÓN 15.19. *La aplicación*

$$\theta\colon \mathrm{M}_{s\times r}(\mathrm{Hom}(\mathbf{H}, \mathbf{K})) \to \mathrm{Hom}(H_1 \times \cdots \times H_r, K_1 \times \cdots \times K_s),$$

definida por

$$\theta(\varsigma_{ij})(h_1, \ldots, h_r) := \Big(\prod_j \varsigma_{1j}(h_j), \ldots, \prod_j \varsigma_{sj}(h_j)\Big),$$

es biyectiva.

DEMOSTRACIÓN. Es una consecuencia inmediata de las propiedades universales del producto directo y el producto directo restringido. Más aún, es fácil ver que $\theta^{-1}(\varsigma)$ es la matriz $(\pi_i \circ \varsigma \circ \iota_j)$, donde

$$\iota_j\colon H_j \to H_1 \times \cdots \times H_r \qquad \text{y} \qquad \pi_i\colon K_1 \times \cdots \times K_s \to K_i$$

son los morfismos canónicos. □

Si escribimos los elementos de

$$H_1 \times \cdots \times H_r \qquad \text{y} \qquad K_1 \times \cdots \times K_s$$

como vectores columna, entonces $\theta(\varsigma_{ij})(h_1, \ldots, h_r)$ es calculado por el producto de matrices

$$\begin{pmatrix} \varsigma_{11} & \cdots & \varsigma_{1r} \\ \vdots & \ddots & \vdots \\ \varsigma_{s1} & \cdots & \varsigma_{sr} \end{pmatrix} \begin{pmatrix} h_1 \\ \vdots \\ h_r \end{pmatrix} := \begin{pmatrix} \varsigma_{11}(h_1) \cdots \varsigma_{1r}(h_r) \\ \vdots \\ \varsigma_{s1}(h_1) \cdots \varsigma_{sr}(h_r) \end{pmatrix}. \tag{15}$$

Notemos que en cada fila de la matriz columna del lado derecho de la última igualdad, las sumas que aparecen usualmente al efectuar el producto de las matrices de la izquierda han sido reemplazadas por productos. Esto se debe a que la operación en cada uno de los K_j es denotada multiplicativamente.

Cuando los K_i son grupos abelianos, entonces cada uno de los Hom que aparecen en la proposición anterior también lo son, via la suma de morfismos introducida en la Proposición 11.16 y, en este caso, θ es un isomorfismo de grupos abelianos si consideramos a $\mathrm{M}_{s\times r}(\mathrm{Hom}(\mathbf{H}, \mathbf{K}))$ como un grupo via la suma usual de matrices.

Consideremos ahora otra matriz

$$\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1s} \\ \vdots & \ddots & \vdots \\ \varphi_{t1} & \cdots & \varphi_{ts} \end{pmatrix} \in \mathrm{M}_{t\times s}(\mathrm{Hom}(\mathbf{K}, \mathbf{L})),$$

donde $\mathbf{L} := (L_1, \ldots, L_t)$ es otra familia finita de grupos y definamos

$$\psi_{ij} \colon H_j \to L_i \qquad \text{para } 1 \leq i \leq t \text{ y } 1 \leq j \leq r,$$

por

$$\psi_{ij}(h) := (\varphi_{i1} \circ \varsigma_{1j})(h) \cdots (\varphi_{is} \circ \varsigma_{sj})(h) \qquad \text{para } h \in H_j.$$

Afirmamos que

$$\psi_{ij}(h)\psi_{ij'}(h') = \psi_{ij'}(h')\psi_{ij}(h) \qquad \text{para todo } i,\ j \neq j',\ h \in H_j \text{ y } h' \in H_{j'},$$

y que

$$\begin{pmatrix} \psi_{11} & \cdots & \psi_{1r} \\ \vdots & \ddots & \vdots \\ \psi_{t1} & \cdots & \psi_{tr} \end{pmatrix} \begin{pmatrix} h_1 \\ \vdots \\ h_r \end{pmatrix} = \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1s} \\ \vdots & \ddots & \vdots \\ \varphi_{t1} & \cdots & \varphi_{ts} \end{pmatrix} \begin{pmatrix} \varsigma_{11} & \cdots & \varsigma_{1r} \\ \vdots & \ddots & \vdots \\ \varsigma_{s1} & \cdots & \varsigma_{sr} \end{pmatrix} \begin{pmatrix} h_1 \\ \vdots \\ h_r \end{pmatrix}.$$

En efecto lo primero se sigue fácilmente de que

$$\varphi_{ik}(\varsigma_{kj}(h)) \text{ conmuta con } \varphi_{ik'}(\varsigma_{k'j'}(h')) \quad \text{para todo } (j', k') \neq (j, k),\ h \in H_j \text{ y } h' \in H_{j'},$$

lo cual es evidente si $k \neq k'$ y en otro caso vale pues

$$\varphi_{ik}(\varsigma_{kj}(h))\varphi_{ik}(\varsigma_{kj'}(h')) = \varphi_{ik}\big(\varsigma_{kj}(h)\varsigma_{kj'}(h')\big) = \varphi_{ik}\big(\varsigma_{kj'}(h')\varsigma_{kj}(h)\big) = \varphi_{ik}(\varsigma_{kj'}(h'))\varphi_{ik}(\varsigma_{kj}(h));$$

mientras que lo segundo sale por cálculo directo.

Es natural ahora escribir

$$\begin{pmatrix} \psi_{11} & \cdots & \psi_{1r} \\ \vdots & \ddots & \vdots \\ \psi_{t1} & \cdots & \psi_{tr} \end{pmatrix} := \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1s} \\ \vdots & \ddots & \vdots \\ \varphi_{t1} & \cdots & \varphi_{ts} \end{pmatrix} \begin{pmatrix} \varsigma_{11} & \cdots & \varsigma_{1r} \\ \vdots & \ddots & \vdots \\ \varsigma_{s1} & \cdots & \varsigma_{sr} \end{pmatrix}. \tag{16}$$

Si los L_j son grupos abelianos y denotamos aditivamente tanto la operación de cada uno de ellos como la de los grupos $\mathrm{Hom}(K_k, L_j)$ y $\mathrm{Hom}(H_i, L_j)$, entonces el producto de matrices (16) toma el aspecto habitual.

16. Producto semidirecto

Por el Teorema 15.1 sabemos que un grupo G es producto directo interno de dos subgrupos N y H si y sólo si cada $g \in G$ se escribe de manera única como un producto $g = nh$ con $n \in N$ y $h \in H$, y tanto N como H son subgrupos normales de G. Debilitando el último requisito se obtiene la noción de producto semidirecto interno, que consideraremos ahora. Luego de estudiar con algún detalle esta contrucción, y motivados por el entendimiento de su estructura, introduciremos la noción de producto semidirecto, y estudiaremos algunas de sus propiedades y las relaciones con la versión interna.

16.1. Producto semidirecto interno

Consideremos dos subgrupos N y H de un grupo G. Decimos que G es *producto semidirecto interno* de N con H si $N \lhd G$ y cada $g \in G$ se escribe de manera única como un producto $g = nh$, con $n \in N$ y $h \in H$. Es fácil escribir la multiplicación de dos elementos nh y $n'h'$ de G expresando el resultado en términos de la descomposición $G = NH$. En efecto, como N es un subgrupo normal, $hn'h^{-1} \in N$ para cada $n' \in N$ y $h \in H$, por lo que la fórmula

$$(nh)(n'h') = nhn'h^{-1}hh' \tag{17}$$

da la expresión deseada. De esta igualdad se sigue inmediatamente que la inclusión canónica $\iota_H \colon H \to G$ y la función $\pi_H \colon G \to H$, definida por $\pi_H(nh) := h$, son morfismos de grupos. Además $\pi_H \circ \iota_H = \mathrm{id}_H$ y el núcleo de π_H es la inclusión canónica $\iota_N \colon N \to G$.

Teorema 16.1. *Consideremos un grupo G y subgrupos N y H de G tales que $G = NH$. Son equivalentes:*

1. *G es producto semidirecto interno de N con H.*
2. *$N \lhd G$ y $N \cap H = 1$.*
3. *$N \lhd G$ y si $1 = nh$ con $n \in N$ y $h \in H$, entonces $n = h = 1$.*

Demostración. 1) $\Rightarrow$ 2) Tomemos $x \in N \cap H$. Como $1 = xx^{-1}$ se sigue de la unicidad de la escritura que $x = 1$.
2) $\Rightarrow$ 3) Si $1 = nh$ con $n \in N$ y $h \in H$, entonces $h^{-1} = n \in N \cap H$ y, por lo tanto, $n = h = 1$.
3) $\Rightarrow$ 1) Si $nh = n'h'$, entonces $n^{-1}n'h'h^{-1} = 1$ y, por consiguiente, $n^{-1}n' = h'h^{-1} = 1$. □

Ejercicio 16.2. *Supongamos que N y L son subgrupos de un grupo G con L no contenido en N. Pruebe que si N tiene índice 2 en G y L es simple, entonces $|L| = 2$ y G es el producto semidirecto interno de N y L.*

Si G se descompone como producto semidirecto interno en la forma $G = NH$, entonces, para cada $h \in H$ la aplicación

$$\begin{array}{ccc} N & \xrightarrow{\varsigma(h)} & N \\ n & \longmapsto & hnh^{-1} \end{array}$$

es un automorfismo. Además la función $\varsigma\colon H \to \mathrm{Aut}(N)$, obtenida de este modo, es un morfismo y, con estas notaciones, la fórmula (17) se escribe

$$(nh)(n'h') = n\varsigma(h)(n')hh'.$$

Esto justifica la construcción que sigue.

16.2. Producto semidirecto

Consideremos un morfismo de grupos

$$\varsigma\colon H \to \mathrm{Aut}(N)$$

y escribamos $h \cdot_\varsigma n$ en lugar de $\varsigma(h)(n)$, o incluso $h \cdot n$ si ς está claro. Con estas notaciones, que $\varsigma(h)$ sea un morfismo de grupos significa que

$$h \cdot (nn') = (h \cdot n)(h \cdot n') \quad \text{y} \quad h \cdot 1 = 1 \qquad \text{para todo } h \in H \text{ y } n, n' \in N,$$

y que lo sea ς se traduce en que

$$(hh') \cdot n = h \cdot (h' \cdot n) \quad \text{y} \quad 1 \cdot n = n \qquad \text{para todo } h, h' \in H \text{ y } n \in N.$$

Notemos que las condiciones $h \cdot 1 = 1$ y $1 \cdot n = n$ son redundantes.

Proposición 16.3. *El producto cartesiano $N \times H$, dotado de la multiplicación*

$$(n, h)(n', h') := (n(h \cdot n'), hh'),$$

es un grupo. El neutro es $(1, 1)$ y el inverso de un elemento (n, h) es $(h^{-1} \cdot n^{-1}, h^{-1})$.

Demostración. Comprobemos primero que la multiplicación es asociativa. Para ello debemos mostrar que para cada (n, h), (n', h') y (n'', h'') en $N \times H$, los elementos

$$((n, h)(n', h'))(n'', h'') = (n(h \cdot n'), hh')(n'', h'') = (n(h \cdot n')(hh' \cdot n''), hh'h'')$$

y

$$(n, h)((n', h')(n'', h'')) = (n, h)(n'(h' \cdot n''), h'h'') = (n(h \cdot (n'(h' \cdot n'')), hh'h''),$$

coinciden. Pero esto es cierto, porque

$$h \cdot (n'(h' \cdot n'') = (h \cdot n')(h \cdot (h' \cdot n'')) = (h \cdot n')(hh' \cdot n'').$$

Por la Proposición 4.2, para terminar la demostración es suficiente ver que $(1, 1)$ es neutro a izquierda de $N \rtimes_\varsigma H$ y que $(h^{-1} \cdot n^{-1}, h^{-1})$ es inverso a izquierda de (n, h), pero

$$(1, 1)(n', h') = (1(1 \cdot n'), 1h') = (n', h')$$

y

$$(h^{-1} \cdot n^{-1}, h^{-1})(n, h) = ((h^{-1} \cdot n^{-1})(h^{-1} \cdot n), h^{-1}h) = (h^{-1} \cdot (n^{-1}n), 1) = (1, 1),$$

como deseamos. □

Fijados grupos N, H y un morfismo $\varsigma\colon H \to \mathrm{Aut}(N)$, llamamos *producto semidirecto de N y H asociado a ς*, y designamos con $N \rtimes_\varsigma H$, al grupo construído en la proposición anterior.

Proposición 16.4. *El producto semidirecto tiene las siguientes propiedades:*

1. *Las funciones*

$$\begin{array}{ccc} N \rtimes_\varsigma H \xrightarrow{\pi} H & \quad y \quad & H \xrightarrow{s} N \rtimes_\varsigma H \\ (n,h) \longmapsto h & & h \longmapsto (1,h) \end{array}$$

son morfismos de grupos, $\ker \pi = N \times 1$ *y* $\pi \circ s = \mathrm{id}_H$.

2. $N \times 1$ *es un subgrupo normal de* $N \rtimes_\varsigma H$ *y la función* $\iota\colon N \to N \rtimes_\varsigma H$, *definida por* $\iota(n) := (n,1)$, *es un isomorfismo de* N *con su imagen* $N \times 1$.
3. $1 \times H$ *es un subgrupo de* $N \rtimes_\varsigma H$
4. $(1,h)(n,1) = (h \cdot n, 1)(1,h)$ *para todo* $h \in H$ *y* $n \in N$.
5. $(n,1)(1,h) = (n,h)$ *para todo* $h \in H$ *y* $n \in N$.
6. $(N \times 1) \cap (1 \times H) = 1$ *y* $(N \times 1)(1 \times H) = N \rtimes_\varsigma H$.

Demostración. Es evidente que π y s son morfismos de grupos, $\pi \circ s = \mathrm{id}_H$, $\ker \pi = N \times 1$ y $(N \times 1) \cap (1 \times H) = 1$. En consecuencia $N \times 1 \lhd N \rtimes_\varsigma H$ y $1 \times H \leq N \rtimes_\varsigma H$. Como

$$(n,1)(n',1) = (n(1 \cdot n'),1) = (nn',1),$$

también ι es un morfismo de grupos. Un cálculo directo muestra que

$$(1,h)(n,1) = (h \cdot n, 1)(1,h) \qquad \text{y} \qquad (n,1)(1,h) = (n,h),$$

lo que muestra en particular que $(N \times 1)(1 \times H) = N \rtimes_\varsigma H$. □

Corolario 16.5. $N \rtimes_\varsigma H$ *es producto semidirecto interno de* $N \times 1$ *con* $1 \times H$.

Demostración. Por los items 2), 3) y 6) del teorema anterior y por el Teorema 16.1. □

Proposición 16.6. *Si un grupo* G *es producto semidirecto interno de un subgrupo normal* N *con un subgrupo* H, *entonces la función*

$$\begin{array}{c} N \rtimes_\varsigma H \xrightarrow{\theta} G \ , \\ (n,h) \longmapsto nh \end{array}$$

donde $\varsigma(h)(n) := hnh^{-1}$, *es un isomorfismo.*

Demostración. la función θ es un morfismo de grupos ya que

$$\theta((n,h)(n',h')) = \theta\big(n(h \cdot_\varsigma n'), hh'\big) = n(h \cdot_\varsigma n')hh' = nhn'h^{-1}hh' = nhn'h' = \theta(n,h)\theta(n',h').$$

Como evidentemente θ es bijectiva, esto termina la demostración. □

Observación 16.7. *Si* $s\colon H \to N \rtimes_\varsigma H$ *es una sección conjuntista del epimorfismo canónico* $\pi\colon N \rtimes_\varsigma H \to H$, *entonces existe una aplicación* $\varpi\colon H \to N$ *tal que*

$$s(h) = (\varpi(h), h) \qquad \textit{para todo } h \in H.$$

Dado que

$$(\varpi(h),h)(\varpi(h'),h') = \big(\varpi(h)(h \cdot_\varsigma \varpi(h')), hh'\big) \quad \textit{para todo } h,h' \in H,$$

la aplicación s *es un morfismo de grupos si y sólo si,*

$$\varpi(hh') = \varpi(h)(h \cdot_\varsigma \varpi(h')) \quad \textit{para todo } h,h' \in H.$$

EJEMPLO 16.8. *Fijado un grupo abeliano G consideremos el morfismo*

$$\varsigma\colon C_2 \to \mathrm{Aut}(G),$$

definido por $\varsigma(1)(g) := g$ y $\varsigma(x)(g) := g^{-1}$, donde $C_2 := \{1, x\}$ es un grupo cíclico de orden 2. El producto semidirecto $G \rtimes_\varsigma C_2$ es el grupo con conjunto subyacente $G \times C_2$ y multiplicación

$$(g', x^b)(g, x^a) = \begin{cases} (g'g, x^a) & \text{si } b = 0, \\ (g'g^{-1}, x^{a+1}) & \text{si } b = 1. \end{cases}$$

Es fácil ver que si G es el grupo cíclico de orden n, esta construcción da el grupo diedral D_n.

EJEMPLO 16.9. *Consideremos dos grupos cíclicos $C_n := \langle x \rangle$ y $C_m := \langle y \rangle$ de orden n y m, respectivamente. Como vimos en el Ejemplo 14.17 para cada $0 \leq i < n$ hay un morfismo*

$$\upsilon_i\colon C_n \to C_n,$$

que es un automorfismo si y sólo si i es coprimo con n, y que aplica x en x^i. Notemos que $\upsilon_i^m(x) = x^{i^m}$, de manera que $\upsilon_i^m = \mathrm{id}$ si y sólo si $i^m \equiv 1 \pmod{n}$, y que además esto implica que i y n son coprimos. En consecuencia, por la Observación 14.15, existe un morfismo

$$\varsigma\colon C_m \to \mathrm{Aut}(C_n),$$

que aplica y en υ_i, si y sólo si $i^m \equiv 1 \pmod{n}$. Es fácil ver que el producto semidirecto $C_n \rtimes_\varsigma C_m$ es isomorfo al grupo $\langle x, y | x^n, y^m, yxy^{-1}x^{-i} \rangle$. Para terminar, señalemos que, salvo este último punto, todo sigue valiendo si reemplazamos C_n por un grupo abeliano de exponente finito n.

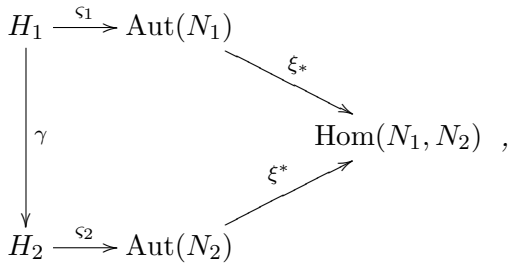
EJEMPLO 16.10. *Fijemos $m \in \mathbb{N}$ y consideremos el grupo cuaterniónico generalizado H_{2^m} de orden 2^{m+2}. Afirmamos que H_{2^m} no es producto semidirecto de dos subgrupos propios. En efecto, por el teorema de Lagrange todos los subgrupos no nulos de H_{2^m} tienen orden par. En consecuencia, por la Observación 6.7 todos tienen elementos de orden 2. Pero como vimos en el Ejemplo 5.9—, el grupo H_n tiene un sólo elemento de este orden, cualquiera sea n. Así, la intersección de dos subgrupos no triviales de H_{2^m} nunca puede ser el grupo nulo, y por lo tanto es imposible escribir H_{2^m} como producto $H_{2^m} = KL$ de dos subgrupos propios cuya intersección sea el grupo nulo (observese que no hemos asumido que ni K ni L sean normales).*

PROPOSICIÓN 16.11. *Consideremos productos semidirectos $N_1 \rtimes_{\varsigma_1} H_1$ y $N_2 \rtimes_{\varsigma_2} H_2$ y morfismos $\gamma\colon H_1 \to H_2$ y $\xi\colon N_1 \to N_2$. Son equivalentes:*

1. *La función*

   $$\chi\colon N_1 \rtimes_{\varsigma_1} H_1 \to N_2 \rtimes_{\varsigma_2} H_2,$$

   definida por $\chi(n, h) := (\xi(n), \gamma(h))$, es un morfismo de grupos.
2. *$\xi(h \cdot_{\varsigma_1} n) = \gamma(h) \cdot_{\varsigma_2} \xi(n)$ para todo $h \in H_1$ y $n \in N_1$.*
3. *El diagrama*



donde ξ_* y ξ^* están definidos por $\xi_*(\zeta) := \xi \circ \zeta$ y $\xi^*(\zeta) := \zeta \circ \xi$, conmuta.

Además, en este caso χ es biyectivo si y sólo si ξ y γ lo son.

DEMOSTRACIÓN. La equivalencia entre los items (1) y (2) se sigue de que

$$\chi((n,h)(n',h')) = \chi(n(h \cdot_{\varsigma_1} n'), hh') = \big(\xi\big(n(h \cdot_{\varsigma_1} n')\big), \gamma(hh')\big)$$

y

$$\chi(n,h)\chi(n',h') = (\xi(n),\gamma(h))(\xi(n'),\gamma(h')) = (\xi(n)(\gamma(h) \cdot_{\varsigma_2} \xi(n')), \gamma(h)\gamma(h')),$$

mientras que la equivalencia entre los item (2) y (3) es consecuencia de que

$$\xi(h \cdot_{\varsigma_1} n') = \xi(\varsigma_1(h)(n')) = \xi_*(\varsigma_1(h))(n')$$

y

$$\gamma(h) \cdot_{\varsigma_2} \xi(n') = \varsigma_2(\gamma(h))(\xi(n')) = \xi^*(\varsigma_2(\gamma(h)))(n').$$

Para terminar, es claro que la afirmación adicional es verdadera. □

17. Sucesiones exactas cortas

Una sucesión de grupos y morfismos

$$\cdots \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \xrightarrow{\varsigma} D \longrightarrow \cdots$$

es una *sucesión exacta* si la imagen de cada morfismo es el núcleo del siguiente. Por ejemplo, todas las sucesiones

$$G \xrightarrow{\varphi} G' \ ,$$

consistentes de un sólo morfismo, son exactas. Las de la forma

$$1 \longrightarrow G \xrightarrow{\varphi} G'$$

lo son si y sólo si φ es un monomorfismo, y las de la forma

$$G \xrightarrow{\varphi} G' \longrightarrow 1,$$

si y sólo si φ es un epimorfismo. Una *sucesión exacta corta* es una sucesión exacta de la forma

$$1 \longrightarrow G' \xrightarrow{\varphi} G \xrightarrow{\psi} G'' \longrightarrow 1 \ . \tag{18}$$

Es fácil ver que este es el caso si y sólo si φ es inyectiva, ψ es sobreyectiva e $\operatorname{Im}\varphi = \ker\psi$. La sucesión exacta corta (18) es escindida a derecha si ψ es una retracción y a izquierda si φ es una sección. Si hay un sucesión exacta corta de grupos como (18), decimos que G es una *extensión de G' por G''*.

EJEMPLO 17.1. *Si $N \rtimes_\varsigma H$ es un producto semidirecto, entonces*

$$1 \longrightarrow N \xrightarrow{\iota_N} N \rtimes_\varsigma H \xrightarrow{\pi_H} H \longrightarrow 1 \ , \tag{19}$$

donde ι_N y π_H son los morfismos canónicos, es una sucesión exacta corta escindida a derecha. Si $\varsigma\colon H \to \operatorname{Aut}(N)$ es el morfismo trivial (esto es, si $N \rtimes_\varsigma H$ es el producto directo de N con H), entonces esta sucesión también es escindida a izquierda.

Ejemplo 17.2. *La sucesión de morfismos*

$$0 \longrightarrow \mathbb{Z}_2 \xrightarrow{\iota} \mathbb{Z}_4 \xrightarrow{\pi} \mathbb{Z}_2 \longrightarrow 0\ ,$$

donde ι y π son los morfismos definidos por $\iota(1) \coloneqq 2$ y $\pi(1) := 1$, es una sucesión exacta corta que no es escindida ni a izquierda ni a derecha.

Diremos que la sucesión exacta corta (18) es *equivalente* a la sucesión exacta corta

$$1 \longrightarrow G' \xrightarrow{\iota} L \xrightarrow{\pi} G'' \longrightarrow 1\ , \tag{20}$$

si existe un morfismo $\alpha\colon G \to L$ tal que el diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G' & \xrightarrow{\varphi} & G & \xrightarrow{\psi} & G'' & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_{G'}} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{id}_{G''}} & & \\ 1 & \longrightarrow & G' & \xrightarrow{\iota} & L & \xrightarrow{\pi} & G'' & \longrightarrow & 1 \end{array}$$

conmuta. Afirmamos que entonces α es necesariamente un isomorfismo. Para probarlo notemos primero que

$$\begin{aligned} \alpha(g) = 1 &\Rightarrow \exists\, g' \in G' \text{ tal que } \varphi(g') = g && \text{porque } \psi(g) = (\pi \circ \alpha)(g) = 1 \text{ y (18) es exacta} \\ &\Rightarrow g' = 1 && \text{porque } \iota(g') = \alpha(g) = 1 \text{ y (20) es exacta} \\ &\Rightarrow g = \varphi(g') = 1, \end{aligned}$$

y, por lo tanto, α es inyectivo. Nos queda ahora la tarea de probar que es sobreyectiva. Dado que ψ lo es, para cada $l \in L$ existe $g \in G$ tal que $\psi(g) = \pi(l)$, por lo que

$$\pi(\alpha(g^{-1})l) = \pi(\alpha(g^{-1}))\pi(l) = \psi(g^{-1})\pi(l) = 1.$$

En consecuencia, debido a la exactitud de (20), hay un $g' \in G'$ tal que $\iota(g') = \alpha(g^{-1})l$ y, así,

$$l = \alpha(g)\iota(g') = \alpha(g)\alpha(\varphi(g')) = \alpha(g\varphi(g')),$$

como queremos.

Ejercicio 17.3. *Consideremos un diagrama conmutativo de morfismos de grupos*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G' & \xrightarrow{\varphi} & G & \xrightarrow{\psi} & G'' & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha''} & & \\ 1 & \longrightarrow & L' & \xrightarrow{\iota} & L & \xrightarrow{\pi} & L'' & \longrightarrow & 1 \end{array}$$

cuyas filas son exactas. Pruebe lo siguiente:

1. *Si α' y α'' son inyectivas, entonces α también lo es.*
2. *Si α' y α'' son sobreyectivas, entonces α también lo es.*

De la definición resulta evidente que la relación de equivalencia de sucesiones exactas cortas es reflexiva y transitiva. Ahora es claro que también es simétrica. Notemos que si dos sucesiones como las (18) y (20) son equivalentes, entonces una de ellas es escindida a un lado si y sólo si la otra lo es. En el Ejemplo 17.1 vimos que las sucesiones exactas cortas asociadas a productos semidirectos son escindidas a derecha, y que si el producto es directo, entonces dicha sucesión es escindida a izquierda. En consecuencia, toda sucesión exacta corta equivalente a una asociada a un producto semidirecto es escindida a derecha, y también a izquierda si el producto es directo. Nuestro próximo objetivo es mostrar que vale la recíproca,

de lo cual se seguirá inmediatamente que las sucesiones exactas cortas escindidas a izquierda, también lo son a derecha.

TEOREMA 17.4. *Si una sucesión exacta corta*

$$1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow 1 \tag{21}$$

es escindida a derecha, entonces existe un producto semidirecto $N \rtimes_\varsigma H$ tal que las sucesiones exactas cortas (19) *y* (21)*, son equivalentes.*

DEMOSTRACIÓN. Fijemos una sección s de π. Tomemos $g, g' \in G$ y $h \in H$. La igualdad

$$s(h)gg's(h)^{-1} = s(h)gs(h)^{-1}s(h)g's(h)^{-1}$$

muestra que para cada $h \in H$ la función

$$\begin{array}{ccc} G & \xrightarrow{\Phi_{s(h)}} & G \\ g & \longmapsto & s(h)gs(h)^{-1} \end{array}$$

es un morfismo de grupos, y de hecho un automorfismo, con inversa $g \mapsto s(h)^{-1}gs(h)$. Además, $\Phi_{s(h)}$ induce por restricción un automorfismo de $\iota(N)$, porque

$$\pi\big(s(h)gs(h)^{-1}\big) = h\pi(g)h^{-1} = 1 \quad \text{para cada } g \in \iota(N).$$

Por lo tanto, hay una única aplicación $\varsigma\colon H \to \mathrm{Aut}(N)$, tal que

$$\iota(\varsigma(h)(n)) = s(h)\iota(n)s(h)^{-1} \quad \text{para todo } h \in H \text{ y todo } n \in N.$$

Además ς es un morfismo de grupos, porque

$$\begin{aligned} \iota(\varsigma(hh')(n)) &= s(hh')\iota(n)s(hh')^{-1} \\ &= s(h)s(h')\iota(n)s(h')^{-1}s(h)^{-1} \\ &= s(h)\iota(\varsigma(h')(n))s(h)^{-1} \\ &= \iota\big(\varsigma(h)(\varsigma(h')(n))\big). \end{aligned}$$

Así tiene sentido considerar el producto semidirecto $N \rtimes_\varsigma H$. Para terminar la prueba será suficiente mostrar que la aplicación $\alpha\colon N \rtimes_\varsigma H \to G$, definida por $\alpha(n,h) := \iota(n)s(h)$ es un morfismo de grupos, y que el diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\iota_N} & N \rtimes_\varsigma H & \xrightarrow{\pi_H} & H & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_N} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{id}_H} & & \\ 1 & \longrightarrow & N & \xrightarrow{\iota} & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \end{array}$$

conmuta. Pero las igualdades

$$\alpha(\iota_N(n)) = \alpha(n,1) = \iota(n) \qquad \text{y} \qquad \pi(\alpha(n,h)) = \pi(\iota(n)s(n)) = \pi(\iota(n))\pi(s(h)) = h$$

muestran que lo último es cierto, y las igualdades

$$\begin{aligned}\alpha((n,h)(n',h')) &= \alpha(n(h\cdot n'),hh')\\ &= \iota(n(h\cdot n'))s(hh')\\ &= \iota(n)\iota(h\cdot n')s(h)s(h')\\ &= \iota(n)s(h)\iota(n')s(h)^{-1}s(h)s(h')\\ &= \iota(n)s(h)\iota(n')s(h')\\ &= \alpha(n,h)\alpha(n',h'),\end{aligned}$$

que lo primero también lo es. □

Observación 17.5. *En la demostración del Teorema 17.4 no sólo probamos que la sucesión exacta corta* (21) *es equivalente a una asociada a un producto semidirecto. También pudimos construir explícitamente la equivalencia. Muchas veces, cuando citemos dicho teorema, en realidad nos estaremos refiriendo a este resultado más preciso.*

Ejemplo 17.6. *Si G es producto semidirecto interno $G = NH$ de un subgrupo normal N con un subgrupo H, entonces la sucesión de morfismos*

$$1 \longrightarrow N \xrightarrow{\ \iota\ } G \xrightarrow{\ \pi\ } H \longrightarrow 1\ ,$$

donde ι es la inclusión canónica y π está dado por $\pi(nh) := h$ es una sucesión exacta corta. Por el Teorema 17.4, como la inclusión canónica de H en G es una sección de π, el diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\iota_N} & N\rtimes_{\varsigma} H & \xrightarrow{\pi_H} & H & \longrightarrow & 1\\ & & \downarrow{\scriptstyle \mathrm{id}_N} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{id}_H} & & \\ 1 & \longrightarrow & N & \xrightarrow{\ \iota\ } & G & \xrightarrow{\ \pi\ } & H & \longrightarrow & 1 \end{array}\ ,$$

donde $\varsigma(h)(n) := hnh^{-1}$ y α es el morfismo definido por $\alpha(n,h) := nh$, conmuta y, por lo tanto, da una equivalencia de sucesiones exactas cortas. Como el lector habrá notado, el producto semidirecto involucrado y el isomorfismo α fueron antes obtenidos en la Proposición 16.6.

Proposición 17.7. *Las sucesiones exactas cortas asociadas a dos productos semidirectos $N\rtimes_{\varsigma_1} H$ y $N\rtimes_{\varsigma_2} H$ son equivalentes si y sólo si existe una función $\varpi\colon H\to N$ que satisface:*

$$\varpi(hh') = \varpi(h)\big(h\cdot_{\varsigma_2}\varpi(h')\big) \qquad y \qquad (h\cdot_{\varsigma_1} n)\varpi(h) = \varpi(h)(h\cdot_{\varsigma_2} n), \tag{22}$$

para todo $h,h'\in H$ y $n\in N$.

Demostración. Evidentemente para cada función $\chi\colon N\rtimes_{\varsigma_1} H\to N\rtimes_{\varsigma_1} H$, la conmutatividad del diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\iota_N} & N\rtimes_{\varsigma_1} H & \xrightarrow{\pi_H} & H & \longrightarrow & 1\\ & & \downarrow{\scriptstyle \mathrm{id}_N} & & \downarrow{\scriptstyle \chi} & & \downarrow{\scriptstyle \mathrm{id}_H} & & \\ 1 & \longrightarrow & N & \xrightarrow{\iota_N} & N\rtimes_{\varsigma_2} H & \xrightarrow{\pi_H} & H & \longrightarrow & 1 \end{array}$$

equivale a que existe una función $\omega\colon N\rtimes_{\varsigma_1} H\to N$ tal que

$$\chi(n,h) = (\omega(n,h),h) \qquad \text{y} \qquad \omega(n,1) = n \tag{23}$$

Es claro ahora que

$$\chi\big((n,1)(1,h)\big)=\chi(n,h)=(\omega(n,h),h) \quad \text{y} \quad \chi(n,1)\chi(1,h)=(n,1)(\omega(1,h),h)=(n\omega(1,h),h).$$

En consecuencia

$$\chi\big((n,1)(1,h)\big) = \chi(n,1)\chi(1,h) \qquad \text{para todo } n\in N \text{ y } h\in H \tag{24}$$

si y sólo si ω es de la forma $\omega(n,h)=n\varpi(h)$, donde ϖ es una función de H en N. Además la segunda igualdad en (23) se satisface si y sólo si $\varpi(1)=1$. Supongamos que estamos en esta situación. Entonces,

$$\chi\big((n,h)(n',h')\big) = \chi\big(n(h\cdot_{\varsigma_1} n'),hh'\big) = \big(n(h\cdot_{\varsigma_1} n')\varpi(hh'),hh'\big)$$

y

$$\chi(n,h)\chi(n',h') = (n\varpi(h),h)(n'\varpi(h'),h') = \big(n\varpi(h)(h\cdot_{\varsigma_2}(n'\varpi(h'))),hh'\big).$$

Por lo tanto χ es un morfismo de grupos si y sólo si

$$(h\cdot_{\varsigma_1} n')\varpi(hh') = \varpi(h)(h\cdot_{\varsigma_2}(n'\varpi(h'))).$$

Considerando los caso $n'=1$ y $h'=1$, y usando que $\varpi(1)=1$, obtenemos las dos igualdades de (22).

$$\varpi(hh') = \varpi(h)(h\cdot_{\varsigma_2}\varpi(h')) \qquad \text{y} \qquad (h\cdot_{\varsigma_1} n')\varpi(h) = \varpi(h)(h\cdot_{\varsigma_2}(n'\varpi(1))).$$

Pero entonces, debido a la primera de estas igualdades $\varpi(1)=\varpi(1)\varpi(1)$, lo que implica que $\varpi(1)=1$ y, en consecuencia, (22) se satisface. Recíprocamente si este es el caso, entonces

$$(h\cdot_{\varsigma_1} n')\varpi(hh')=(h\cdot_{\varsigma_1} n')\varpi(h)(h\cdot_{\varsigma_2}\varpi(h'))=\varpi(h)(h\cdot_{\varsigma_2} n')(h\cdot_{\varsigma_2}\varpi(h'))=\varpi(h)(h\cdot_{\varsigma_2}(n'\varpi(h'))),$$

como queremos. □

Notemos que la primera igualdad en (22) aparece también en la Observación 16.7. Esto no es casualidad, se debe a que la composición de χ con la inclusión canónica de H en $N\rtimes_{\varsigma_1} H$ es una sección del epimorfismo canónica $\pi\colon N\rtimes_{\varsigma_2} H\to H$.

Teorema 17.8. *Si una sucesión exacta corta*

$$1 \longrightarrow N \xrightarrow{\ \iota\ } G \xrightarrow{\ \pi\ } H \longrightarrow 1 \tag{25}$$

es escindida a izquierda, entonces es equivalente a la asociada al producto directo $N\times H$.

Demostración. Dada una retracción γ de ι, consideremos el morfismo

$$(\gamma,\pi)\colon G\to N\times H.$$

Como

$$(\gamma,\pi)\circ\iota(n)=(n,1) \quad \text{y} \quad \pi_H\circ(\gamma,\pi)(g)=\pi(g) \qquad \text{para todo } n\in N \text{ y } g\in G,$$

el diagrama

$$\begin{array}{ccccccccc}
1 & \longrightarrow & N & \xrightarrow{\ \iota\ } & G & \xrightarrow{\ \pi\ } & H & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \mathrm{id}_N} & & \downarrow{\scriptstyle (\gamma,\pi)} & & \downarrow{\scriptstyle \mathrm{id}_H} & & \\
1 & \longrightarrow & N & \xrightarrow{\ \iota_N\ } & N\times H & \xrightarrow{\ \pi_H\ } & H & \longrightarrow & 1
\end{array}$$

conmuta, lo que prueba el resultado. □

18. Complementos

Terminamos con el estudio de la parte básica de grupos con la presentación de algunos nuevos conceptos y también de algunas variantes de los que ya hemos dado.

18.1. Centro y automorfismos interiores

Un elemento g de un grupo G es *central* si $gh = hg$ para todo $h \in G$. El *centro* $\mathrm{Z}\,G$ de G es el conjunto de todos los elementos centrales de G.

Observación 18.1. *Para toda familia $(G_i)_{i\in I}$ de grupos,*

$$\mathrm{Z}(\prod G_i) = \prod \mathrm{Z}(G_i) \qquad y \qquad \mathrm{Z}(\bigsqcup G_i) = \bigsqcup \mathrm{Z}(G_i).$$

Ejemplo 18.2. *A continuación calculamos el centro de los grupos diedrales y cuaterniónicos. Recordemos que el grupo diedral D_n está generado por dos elementos x e y sujetos a las relaciones $x^n = 1$, $y^2 = 1$ e $yxy^{-1}x = 1$, y que*

$$D_n = \{1, x, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y\}.$$

Es claro que D_2 es conmutativo. Consideremos el caso $n > 2$. Entonces $x^2 \neq 1$ y, así, de la igualdad $x(x^iy)x^{-1} = x^{i+2}y$ se sigue que $x^iy \notin \mathrm{Z}\,D_n$ para ningún i. Por otro lado, dado que

$$yx^iy^{-1} = x^{-i} \qquad y \qquad x^i \text{ conmuta con } x,$$

obtenemos que $x^i \in \mathrm{Z}\,D_n$ si y sólo si $i = 0$ o $i = n/2$. Por lo tanto,

$$\mathrm{Z}\,D_n = \begin{cases} D_n & \text{si } n = 2, \\ 1 & \text{si } n \text{ es impar}, \\ \{1, x^{n/2}\} & \text{si } n \text{ es par y } n > 2. \end{cases}$$

Recordemos ahora que H_n es un grupo generado por dos elementos x e y sujetos a las relaciones $x^ny^{-2} = 1$ e $yxy^{-1}x = 1$ y que

$$H_n = \{1, x, \ldots, x^{2n-1}, y, xy, \ldots, x^{2n-1}y\}.$$

De la igualdad $x(x^iy)x^{-1} = x^{i+2}y$ se sigue que $x^iy \notin \mathrm{Z}\,H_n$ para ningún i, y puesto que

$$yx^iy^{-1} = x^{-i} \qquad y \qquad x^i \text{ conmuta con } x,$$

es claro que $x^i \in \mathrm{Z}\,H_n$ si y sólo si $i = 0$ o $i = n$. Por consiguiente, $\mathrm{Z}\,H_n = \{1, x^n\}$.

Ejercicio 18.3. *Muestre que si $f\colon G \to G$ es un endomorfismo de grupos, entonces no necesariamente $f(\mathrm{Z}\,G) \subseteq \mathrm{Z}\,G$.*

Ejercicio 18.4. *Pruebe que si $f\colon G \to G'$ es un morfismo sobreyectivo de grupos, entonces $f(\mathrm{Z}\,G) \subseteq \mathrm{Z}\,G'$.*

Ejercicio 18.5. *Pruebe que si N es un subgrupo normal de $H \times L$ y*

$$N \cap (H \times 1) = N \cap (1 \times L) = 1,$$

entonces $N \subseteq \mathrm{Z}(H \times L)$.

Para cada $g \in G$, consideremos la función $\Phi_g \colon G \to G$, definida por $\Phi_g(h) := ghg^{-1}$. Es claro que Φ_g es biyectiva, con inversa $\Phi_{g^{-1}}$, y la igualdad

$$\Phi_g(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = \Phi_g(h)\Phi_g(k)$$

muestra que, de hecho, es un automorfismo, llamado *el automorfismo interior* de G *asociado a* g. Además es fácil ver que la aplicación

$$\begin{array}{ccc} G & \xrightarrow{\Phi} & \mathrm{Aut}(G) \\ g & \longmapsto & \Phi_g \end{array}$$

es un morfismo de grupos cuya imagen es el conjunto $\mathrm{Int}(G)$ de los automorfismos interiores de G, y cuyo núcleo es el centro de G. En consecuencia $\mathrm{Z}\,G$ es un subgrupo normal de G. Hasta ahora nos hemos limitado a repetir el razonamiento hecho en la demostración del Teorema 17.4. Aunque sencillo, el siguiente es el primer resultado escencialmente nuevo.

Proposición 18.6. *La igualdad* $\varphi \circ \Phi_g \circ \varphi^{-1} = \Phi_{\varphi(g)}$ *vale para cada* $\varphi \in \mathrm{Aut}(G)$ *y* $g \in G$. *En part—icular,* $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$.

Demostración. En efecto,

$$(\varphi \circ \Phi_g \circ \varphi^{-1})(h) = \varphi(\Phi_g(\varphi^{-1}(h))) = \varphi(g\varphi^{-1}(h)g^{-1}) = \varphi(g)h\varphi(g)^{-1} = \Phi_{\varphi(g)}(h),$$

para todo $h \in G$. □

Ejercicio 18.7. *Pruebe que todos los subgrupos de* H_2 *son normales.*

Al grupo cociente $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Int}(G)$ se lo conoce como el grupo de *automorfismos exteriores* de G (aunque sus elementos no son automorfismos). Es obvio que la sucesión

$$1 \longrightarrow \mathrm{Z}\,G \xrightarrow{\iota} G \xrightarrow{\Phi} \mathrm{Aut}(G) \xrightarrow{\pi} \mathrm{Out}(G) \longrightarrow 1\ ,$$

donde ι es la inclusión canónica y π la proyección al cociente, es exacta.

Ejemplo 18.8. *Consideremos al grupo diedral* D_n *presentado como en el Ejemplo 18.2. Un cálculo directo muestra que*

$$\Phi_{x^j}(x) = x, \quad \Phi_{x^j}(y) = x^{2j}y, \quad \Phi_{x^jy}(x) = x^{-1} \quad y \quad \Phi_{x^jy}(y) = x^{2j}y.$$

En consecuencia si $n > 2$ *y* ϕ *es como en el Ejemplo 14.18, entonces*

$$\phi(\mathrm{Int}(D_n)) = \begin{cases} \{(j,1) : 0 \le j < n\} \cup \{(j,n-1) : 0 \le j < n\} & \text{si } n \text{ es impar,} \\ \{(2j,1) : 0 \le j < n/2\} \cup \{(2j,n-1) : 0 \le j < n/2\} & \text{si } n \text{ es par.} \end{cases}$$

Consideremos ahora al grupo cuaterniónico H_n *presentado también como en el Ejemplo 18.2. De la misma manera que para* D_n

$$\Phi_{x^j}(x) = x, \quad \Phi_{x^j}(y) = x^{2j}y, \quad \Phi_{x^jy}(x) = x^{-1} \quad y \quad \Phi_{x^jy}(y) = x^{2j}y,$$

y, en consecuencia, si $n > 2$ *y* ϕ *es como en el Ejemplo 14.19, entonces*

$$\phi(\mathrm{Int}(H_n)) = \{(2j,1) : 0 \le j < n\} \cup \{(2j,n-1) : 0 \le j < n\}.$$

El siguiente es un resultado sencillo pero muy útil.

Proposición 18.9. *Si* $G/\mathrm{Z}\,G$ *es cíclico, entonces* G *es abeliano.*

DEMOSTRACIÓN. Por hipótesis existe $g \in G$ tal que $G = \langle g \rangle \operatorname{Z} G$. Puesto que, para todo $m, n \in \mathbb{Z}$ y todo $h, k \in \operatorname{Z} G$,

$$(g^m h)(g^n k) = g^m g^n hk = g^n g^m kh = (g^n k)(g^m h),$$

el grupo G es conmutativo. □

18.2. Elementos conjugados

Dos elementos g y h de un grupo G son *conjugados* si existe $k \in G$ tal que

$$h = \Phi_k(g) = kgk^{-1}.$$

Como uno se obtiene del otro aplicando un automorfismo, los ordenes de g y h coinciden. La relación $\sim$, definida en G por $g \sim h$ si y sólo si g y h son conjugados, es de equivalencia y, por lo tanto, tiene asociada una partición, cuyos elementos son las *clases de conjugación de* G.

PROPOSICIÓN 18.10. *Dos elementos g, h de G son conjugados si y sólo si existen $k, l \in G$ tales que $g = kl$ y $h = lk$.*

DEMOSTRACIÓN. Para empezar kl y lk son conjugados, ya que $lk = k^{-1}(kl)k$. Recíprocamente, si g y h son conjugados y $h = kgk^{-1} = k(gk^{-1})$, entonces $(gk^{-1})k = g$. □

EJERCICIO 18.11. *Calcule las clases de conjugación en los grupos D_n y H_n.*

EJERCICIO 18.12. *Pruebe que si un grupo G contiene un elemento de orden $n > 1$ y dos clases de conjugación, entonces $|G| = 2$.*

18.3. Subgrupos característicos y completamente normales

Un subgrupo H de G es normal si y sólo si $\Phi_g(H) \subseteq H$ para todo $g \in G$ (es decir si es unión de clases de conjugación). Decimos que un subgrupo H de G es un subgrupo *característico* de G si $\varphi(H) \subseteq H$ para todo $\varphi \in \operatorname{Aut}(G)$. Entonces $\varphi(H) = H$ para todo $\varphi \in \operatorname{Aut}(G)$. En efecto,

$$\varphi^{-1}(H) \subseteq H \Rightarrow H \subseteq \varphi(H).$$

Es evidente que todo subgrupo característico de G es normal. Afirmamos que $\operatorname{Z} G$ es un subgrupo característico de G. Para probar esto debemos mostrar que si $g \in \operatorname{Z} G$ y $\varphi \in \operatorname{Aut}(G)$, entonces $\varphi(g) \in \operatorname{Z} G$. Pero esto es cierto, porque

$$\varphi(g)h = \varphi(g)\varphi(\varphi^{-1}(h)) = \varphi(g\varphi^{-1}(h)) = \varphi(\varphi^{-1}(h)g) = \varphi(\varphi^{-1}(h))\varphi(g) = h\varphi(g),$$

para todo $h \in G$.

EJEMPLO 18.13. *Consideremos al grupo diedral D_n presentado como en el Ejemplo 18.2. De los cálculos realizados en los Ejemplos 10.2 y 14.18 se sigue fácilmente que si $n > 2$, entonces los subgrupos característicos de D_n son D_n y los subgrupos de $\langle x \rangle$. Algo similar ocurre con el grupo H_n, pero en este caso hay que usar los cálculos realizados en los Ejemplos 10.3 y 14.19 en lugar de los realizados en los Ejemplo 10.2 y 14.18.*

OBSERVACIÓN 18.14. *Puede suceder que $H \lhd L \lhd G$, pero que H no sea normal en G. Por ejemplo, este es el caso cuando $G = \mathrm{S}_4$, $L = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$, donde σ_1, σ_2 y σ_3 son las*

permutaciones definidas por

$$\begin{aligned}
&\sigma_1(1)=2, \quad \sigma_1(2)=1, \quad \sigma_1(3)=4, \quad \sigma_1(4)=3,\\
&\sigma_2(1)=3, \quad \sigma_2(2)=4, \quad \sigma_2(3)=1, \quad \sigma_2(4)=2,\\
&\sigma_3(1)=4, \quad \sigma_3(2)=3, \quad \sigma_3(3)=2, \quad \sigma_3(4)=1,
\end{aligned}$$

y $H=\{\mathrm{id},\sigma_1\}$. *Esto no ocurre si* H *es un subgrupo característico de* L. *En efecto, como* $L\triangleleft G$, *para cada* $g\in G$ *el automorfismo interior* Φ_g *de* G *define por restricción un automorfismo* ψ *(no necesariamente interior) de* L. *Pero entonces*

$$\Phi_g(H)=\psi(H)=H,$$

porque H *es característico en* L. *También vale que si* H *es un subgrupo característico de* L *y* L *un subgrupo característico de* G, *entonces* H *es un subgrupo característico de* G. *La demostración es la misma, pero en lugar de automorfismos interiores de* G *hay que considerar automorfismos arbitrarios.*

Decimos que un subgrupo H de un grupo G es *completamente normal* si $\varphi(H)\subseteq H$ para todo $\varphi\in\mathrm{End}(G)$. Claramente todo subgrupo completamente normal de G es característico. Por el Ejercicio 18.3 sabemos que la recíproca no vale. Si $H\subseteq L\subseteq G$ es una cadena de subgrupos con H completamente normal en L y L es completamente normal en G, entonces H es completamente normal en G. La demostración es similar a las dadas en la observación anterior.

Ejercicio 18.15. *Pruebe que si* H *es un subgrupo normal de un grupo finito* G *y* $|H|$ *es coprimo con* $|G/H|$, *entonces* H *es un subgrupo completamente normal de* G.

Proposición 18.16. *Supongamos que* $H\leq L\leq G$.

1. *Si* H *es normal en* G *y* L/H *es normal en* G/H, *entonces* L *es normal en* G.
2. *Si* H *es característico en* G *y* L/H *es característico en* G/H, *entonces* L *es característico en* G.
3. *Si* H *es completamente normal en* G *y* L/H *es completamente normal en* G/H, *entonces* L *es completamente normal en* G.

Demostración. Recordemos que para cada $g\in G$ denotamos con $[g]$ a su clase en G/H. Como $\Phi_{[g]}(L/H)=\Phi_g(L)/H$ y L/H es normal en G/H,

$$\Phi_g(L)/H=L/H,$$

lo cual implica que $\Phi_g(L)=L$. Esto prueba el item 1). Los items 2) y 3) pueden probarse en forma similar, pero usando, en lugar de automorfismos interiores, automorfismos al tratar el primero, y endomorfismos al tratar el segundo. □

18.4. Subgrupo conmutador y abelianizado

El *conmutador* de un grupo G es el subgrupo $[G,G]$ de G generado por los conmutadores $[g,h]:=ghg^{-1}h^{-1}$, con $g,h\in G$. Claramente $\varphi([g,h])=[\varphi(g),\varphi(h)]$ para todo morfismo de grupos $\varphi\colon G\to G'$ y todo par de elementos g y h de G. Por lo tanto, $\varphi([G,G])\subseteq[G',G']$. En particular, tomando $G'=G$ se deduce que $[G,G]$ es un subgrupo completamente normal de G. Al cociente $G/[G,G]$ se lo denomina el *abelianizado de* G. Es un grupo conmutativo, porque $gh=[g,h]hg$. En consecuencia, por el teorema de la correspondencia, si H es un subgrupo

de G que contiene a $[G,G]$, entonces H es normal y G/H es conmutativo. Recíprocamente, si H es un subgrupo normal de G y G/H es conmutativo, entonces $[G,G] \subseteq H$ puesto que la clase de $[g,h] = ghg^{-1}h^{-1}$ en G/H es el elemento neutro de G/H, para todo $g, h \in G$. Una consecuencia de esta reflexión es que $[G,G] = 1$ si y sólo si G es conmutativo (lo que por otra parte es obvio).

Si φ es un morfismo de G en un grupo conmutativo G', entonces $\varphi([G,G]) = 1$. Por consiguiente existe un único morfismo $\varphi' \colon G/[G,G] \to G'$ tal que el diagrama

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow{\scriptstyle \pi} & \nearrow_{\varphi'} & \\ G/[G,G] & & \end{array} ,$$

donde π denota a la proyección canónica, conmuta. Esta es la propiedad universal del abelianizado de G.

Por el comentario que precede a la Proposición 13.16, para cada morfismo de grupos

$$\varphi \colon G \to G'$$

existe un único morfismo $\overline{\varphi} \colon \frac{G}{[G,G]} \to \frac{G'}{[G',G']}$ tal que el diagrama

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ G/[G,G] & \xrightarrow{\overline{\varphi}} & G'/[G',G'] \end{array} ,$$

conmuta. Es evidente que $\overline{\mathrm{id}_G} = \mathrm{id}_{G/[G,G]}$ y que si $\varphi \colon G \to G'$ y $\psi \colon G' \to G''$ son dos morfismos de grupos, entonces $\overline{\psi \circ \varphi} = \overline{\psi} \circ \overline{\varphi}$.

Ejemplo 18.17. *Consideremos el grupo diedral D_n, presentado como en el Ejemplo 18.2. Vamos a determinar su subgrupo conmutador. Puesto que $[x,y] = x^2$, el subgrupo $\langle x^2 \rangle$ de D_n está incluído en $[D_n, D_n]$. Pero como $\langle x^2 \rangle$ es un subgrupo normal de D_n y $D_n/\langle x^2 \rangle \simeq D_2$ es conmutativo, $[D_n, D_n] = \langle x^2 \rangle$. Consideremos ahora el grupo cuaterniónico generalizado, también con la presentación dada en el Ejemplo 18.2. Como $\langle x^2 \rangle \lhd H_n$, el cociente $H_n/\langle x^2 \rangle$ es conmutativo y $[x,y] = x^2$, el subgrupo conmutador de H_n es $\langle x^2 \rangle$.*

18.5. El conmutador de dos subgrupos

El *conmutador* $[H,L]$, de dos subgrupos H y L de G es el subgrupo de G generado por los conmutadores $[h,l]$, con $h \in H$ y $l \in L$. Es claro que $[H,L] = 1$ si y sólo si los elementos de H conmutan con los de L, que $[L,H] = [H,L]$, y que $\varphi([H,L]) = [\varphi(H), \varphi(L)]$ para cada morfismo de grupos $\varphi \colon G \to G'$.

Proposición 18.18. *Si H y L son subgrupos normales, característicos o completamente normales de G, entonces $[H,L]$ también lo es.*

Demostración. Supongamos que H y L son normales en G. Entonces

$$\Phi_g([H,L]) = [\Phi_g(H), \Phi_g(L)] = [H,L]$$

para todo $g \in G$. Esto prueba que $[H,L]$ es un subgrupo normal de G. Los otros casos pueden tratarse de manera similar. □

OBSERVACIÓN 18.19. *Si H y L son subgrupos de un grupo G y $K \triangleleft G$, entonces $[H,L] \subseteq K$ si y sólo si las clases en G/K de los elementos de H conmutan con las de los de L. En particular $[G,H] \subseteq K$ si y sólo si $HK/K \subseteq Z(G/K)$. Denotemos con $\overline{H}$, $\overline{L}$ y $\overline{[H,L]}$ a los mínimos subgrupos normales de G que contienen a H, L y $[H,L]$ respectivamente. Obviamente, el mínimo K tal que $[H,L] \subseteq K$ es $\overline{[H,L]}$. Como $[H,L] \subseteq [\overline{H},\overline{L}]$ y, por la Proposición 18.18, el subgrupo $[\overline{H},\overline{L}]$ de G es normal, $\overline{[H,L]}$ está incluído en $[\overline{H},\overline{L}]$.*

Supongamos que H y L son subgrupos normales de un grupo G. Si $\varphi\colon G \to G'$ es un morfismo de grupos y los elementos de $\varphi(H)$ conmutan con los de $\varphi(L)$, entonces existe un único morfismo $\varphi'\colon G/[H,L] \to G'$ tal que el diagrama

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow{\scriptstyle \pi} & \nearrow_{\varphi'} & \\ G/[H,L] & & \end{array}$$

donde π denota a la proyección canónica, conmuta.

Consideremos ahora un morfismo de grupos $\varphi\colon G \to G'$, y subgrupos normales H, L de G y H', L' de G'. Por el comentario que precede a la Proposición 13.16, si $\varphi(H) \subseteq H'$ y $\varphi(L) \subseteq L'$, entonces existe un único morfismo $\overline{\varphi}\colon \frac{G}{[H,L]} \to \frac{G'}{[H',L']}$ tal que el diagrama

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ G/[H,L] & \xrightarrow{\overline{\varphi}} & G'/[H',L'] \end{array},$$

conmuta. Es claro que $\overline{\mathrm{id}_G} = \mathrm{id}_{G/[H,L]}$ y que si $\varphi\colon G \to G'$ es como arriba y $\psi\colon G' \to G''$ es un morfismo de grupos que satisface $\psi(H') \subseteq H''$ y $\psi(L') \subseteq L''$, donde H'' y L'' son subgrupos normales de G'', entonces $\overline{\psi \circ \varphi} = \overline{\psi} \circ \overline{\varphi}$.

OBSERVACIÓN 18.20. *Para cada terna $(H_i)_{i\in I}$, $(L_i)_{i\in I}$ y $(G_i)_{i\in I}$, de familias de grupos tal que $H_i, L_i \leq G_i$ para todo i,*

$$\left[\prod H_i, \prod L_i\right] = \prod [H_i, L_i] \qquad y \qquad \left[\bigsqcup H_i, \bigsqcup L_i\right] = \bigsqcup [H_i, L_i].$$

EJERCICIO 18.21. *Pruebe que el conmutador $[-,-]\colon G \times G \to G$ tiene las siguientes propiedades*

1. *$[a,bc] = [a,b]b[a,c]b^{-1}$ y $[ab,c] = a[b,c]a^{-1}[a,c]$.*
2. *$[cac^{-1},[b,c]][bcb^{-1},[a,b]][aba^{-1},[c,a]] = 1$ (identidad de Hall).*
3. *$b[a,[b^{-1},c]]b^{-1}c[b,[c^{-1},a]]c^{-1}a[c,[a^{-1},b]]a^{-1} = 1$ (identidad de Jacobi).*

18.6. Subgrupos conjugados

Dos subgrupos L y H de un grupo G son *conjugados* si existe $g \in G$ tal que $L = gHg^{-1}$. Es evidente que los ordenes de dos subgrupos conjugados coinciden. Además, puesto que $gHg^{-1} = \Phi_g(H)$, se sigue del Teorema 13.11 que también coinciden sus índices. Claramente la relación $\sim$, definida en el conjunto de los subgrupos de G por $L \sim H$ si L y H son conjugados, es de equivalencia. Los elementos de la partición asociada son llamados *clases de*

conjugación de subgrupos de G. De la definición se sigue fácilmente que un subgrupo H de G es normal si y sólo si es el único elemento de su clase de conjugación. Más aún, para cada subgrupo H de G, la intersección

$$N := \bigcap_{g\in G} gHg^{-1},$$

de todos los subgrupos conjugados a H, es el máximo subgrupo normal de G incluído en H. En efecto, N es normal porque

$$hNh^{-1} \subseteq \bigcap_{g\in G} hgHg^{-1}h^{-1} = \bigcap_{g\in G} gHg^{-1} = N,$$

para todo $h \in G$, y N es máximo entre los subgrupos normales de G incluídos en H, porque si $L \subseteq H$ es normal en G, entonces $L = gLg^{-1} \subseteq gHg^{-1}$ para todo $g \in G$. Notemos además que si $\{g_i : i \in I\}$ es un conjunto de representantes de las coclases a izquierda de H en G (i. e. un conjunto de elementos de G tales que $gH \cap \{g_i : i \in I\}$ tiene exáctamente un elemento para cada $g \in G$), entonces

$$N = \bigcap_{i\in I} g_iHg_i^{-1},$$

puesto que $(g_ih)H(g_ih)^{-1} = g_iHg_i^{-1}$, para todo $i \in I$ y $h \in H$.

Observación 18.22. *Supongamos que H es un subgrupo de G de índice finito n. Consideremos un conjunto de representantes $\{g_1, \dots, g_n\}$ de las coclases a izquierda de H en G. Por la Observación 6.12*

$$|G/N| \leq \prod_{i=1}^{n} |G/g_iHg_i^{-1}| = n^n.$$

Esta desigualdad será mejorada más adelante.

Observación 18.23. *Es evidente que si g es un elemento de orden 2 de G, entonces $\langle g'\rangle$ es conjugado de $\langle g\rangle$ si y sólo si g' lo es de g.*

18.7. El normalizador y el centralizador

El *normalizador* y el *centralizador* de un subconjunto H de G son los subgrupos

$$\mathrm{N}_G(H) := \{g \in G : gHg^{-1} = H\} \quad \text{y} \quad \mathrm{C}_G(H) := \{g \in G : ghg^{-1} = h \text{ para todo } h \in H\}$$

de G, respectivamente. Es obvio que $\mathrm{C}_G(H) \leq \mathrm{N}_G(H)$. Además, si $g \in \mathrm{N}_G(H)$ y $l \in \mathrm{C}_G(H)$, entonces

$$glg^{-1}h(glg^{-1})^{-1} = gl(g^{-1}hg)l^{-1}g^{-1} = g(g^{-1}hg)g^{-1} = h,$$

para todo $h \in H$ y, por lo tanto, $\mathrm{C}_G(H) \lhd \mathrm{N}_G(H)$. De las definiciones se sigue que:

1. $\mathrm{C}_G(gHg^{-1}) = g\,\mathrm{C}_G(H)g^{-1}$ y $\mathrm{N}_G(gHg^{-1}) = g\,\mathrm{N}_G(H)g^{-1}$ para todo $g \in G$.
2. $H \subseteq \mathrm{C}_G(H)$ si y sólo si los elementos de H conmutan entre si y, en ese caso, $\mathrm{C}_G(H)$ es el máximo subgrupo de G en el que los elementos de H son centrales.
3. Si H es un subgrupo de G, entonces $\mathrm{N}_G(H)$ es máximo subgrupo de G en el que H es normal.
4. $\mathrm{C}_G(H) = \mathrm{C}_G(\langle H\rangle)$ y $\mathrm{N}_G(H) \subseteq \mathrm{N}_G(\langle H\rangle)$.
5. $\bigcap_{i\in I} \mathrm{C}_G\big(H_i\big) = \mathrm{C}_G\left(\bigcup_{i\in I} H_i\right)$ para cada familia $(H_i)_{i\in I}$ de subconjuntos de G.

6. $\bigcup_{i\in I} \mathrm{C}_G(H_i) \subseteq \mathrm{C}_G\left(\bigcap_{i\in I} H_i\right)$ para cada familia $(H_i)_{i\in I}$ de subconjuntos de G.
7. $\bigcap_{i\in I} \mathrm{N}_G(H_i) \subseteq \mathrm{N}_G\left(\bigcap_{i\in I} H_i\right)$ para cada familia $(H_i)_{i\in I}$ de subconjuntos de G.
8. $\bigcap_{i\in I} \mathrm{N}_G(H_i) \subseteq \mathrm{N}_G\left(\bigcup_{i\in I} H_i\right)$ para cada familia $(H_i)_{i\in I}$ de subconjuntos de G.

Observación 18.24. *Si $(H_i)_{i\in I}$ y $(G_i)_{i\in I}$ es un par de familias de grupos, tal que $H_i \leq G_i$ para todo i, entonces*

$$\mathrm{N}_{\prod G_i}\left(\prod H_i\right) = \prod \mathrm{N}_{G_i}(H_i), \qquad \mathrm{N}_{\bigsqcup G_i}\left(\bigsqcup H_i\right) = \bigsqcup \mathrm{N}_{G_i}(H_i),$$
$$\mathrm{C}_{\prod G_i}\left(\prod H_i\right) = \prod \mathrm{C}_{G_i}(H_i) \qquad y \qquad \mathrm{C}_{\bigsqcup G_i}\left(\bigsqcup H_i\right) = \bigsqcup \mathrm{C}_{G_i}(H_i).$$

Observación 18.25. *Es evidente que si $g \in G$ tiene orden 2, entonces $\mathrm{C}_G(g) = \mathrm{N}_G(\langle g\rangle)$. En consecuencia $\langle g\rangle \triangleleft G$ si y sólo si $g \in \mathrm{Z}\, G$.*

Ejercicio 18.26. *Calcule los centralizadores de los elementos de D_n y H_n.*

Decimos que un subgrupo L de G *normaliza* a otro subgrupo H si $L \subseteq \mathrm{N}_G(H)$. Similarmente, decimos que L *centraliza* a H si $L \subseteq \mathrm{C}_G(H)$. Es fácil ver que L normaliza a H si y sólo si $[H, L] \subseteq H$ y que centraliza a H si y sólo si $[H, L] = 1$. Supongamos que L normaliza a H. Entonces, como $H, L \subseteq \mathrm{N}_G(H)$ y H es normal en $\mathrm{N}_G(H)$, el conjunto HL es un subgrupo de $\mathrm{N}_G(H)$ y, por lo tanto, de G. Además $H/(H \cap L) \simeq HL/H$, porque $H \triangleleft HL$.

Observación 18.27. *Consideremos un grupo G y subgrupos H y L de G. Si L normaliza a H y $[H, L] \cap H = 1$, entonces $[H, L] = 1$, porque, como vimos antes, $[H, L] \subseteq H$. En otras palabras, los elementos de H conmutan con los de L. En particular, si H es un subgrupo normal de G y $[G, H] \cap H = 1$ (lo que ocurre por ejemplo si $[G, G] \cap H = 1$), entonces $H \subseteq \mathrm{Z}\, G$.*

Ejercicio 18.28. *Supongamos que H y L son subgrupos de un grupo G y que L está incluído en $\mathrm{N}_G(H)$. Pruebe que si K es un subgrupo normal de L, entonces HK es un subgrupo normal de HL.*

Capítulo 2

El grupo simétrico

En este capítulo estudiamos los grupos simétricos o de permutaciones S_n para $n \geq 2$. En particular probamos que S_n tiene un subgrupo canónico A_n, de índice 2, llamado grupo alternado en n símbolos. También encontramos conjuntos de generadores y presentaciones de S_n y A_n, calculamos sus centros y subgrupos conmutadores y probamos que A_n es simple para todo $n \geq 3$ y distinto de 4, siendo este el resultado más importante que obtendremos.

Empecemos recordando que el orden de S_n es $n!$. Una forma bastante usual (pero que nosotros no utilizaremos nunca) de describir una permutación σ es escribiendo:

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

Recoremos que $\mathbb{I}_n$ denota al conjunto $\{1, \dots, n\}$, de modo que $\mathrm{S}_n = \mathrm{S}_{\mathbb{I}_n}$. Para cada $\sigma \in \mathrm{S}_n$ y $j \in \mathbb{I}_n$ decimos que σ *fija* j si $\sigma(j) = j$ y que lo *mueve* si $\sigma(j) \neq j$. Notemos que si σ mueve j, entonces también mueve $\sigma(j)$, de manera que σ induce una permutación en el conjunto de los elementos movidos por ella. Dos permutaciones σ y τ son *disjuntas* si cada $j \in \mathbb{I}_n$ movido por una de ellas es dejado fijo por la otra. Si este es el caso, entonces σ y τ conmutan entre si y $\sigma \circ \tau$ satisface

$$\sigma(\tau(j)) = \begin{cases} \sigma(j) & \text{si } \tau \text{ fija } j, \\ \tau(j) & \text{si } \sigma \text{ fija } j. \end{cases}$$

Es evidente que si σ se escribe como un producto $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$ de permutaciones disjuntas dos a dos, entonces el conjunto de puntos movidos por σ es la unión disjunta de los conjuntos de puntos movidos por cada σ_i.

1. Estructura cíclica

Una permutación $\sigma \in \mathrm{S}_n$ es un r-ciclo si existen $i_1, \dots, i_r \in \mathbb{I}_n$ distintos, tales que σ deja fijos los elementos de $\mathbb{I}_n \setminus \{i_1, \dots, i_r\}$ y

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\ \dots,\ \sigma(i_{r-1}) = i_r \quad \text{y} \quad \sigma(i_r) = i_1.$$

Emplearemos el símbolo $(i_1, \ldots, i_r)$ para denotar a este r-ciclo. Esta escritura no es única. Los sinónimos de $(i_1, \ldots, i_r)$ son

$$(i_2, \ldots, i_r, i_1) = (i_3, \ldots, i_r, i_1, i_2) = \cdots = (i_r, i_1, \ldots, i_{r-1}).$$

Es fácil ver que el orden de un r-ciclo es r y que hay

$$\frac{1}{r} n(n-1)\cdots(n-r+1)$$

r-ciclos en S_n. El único 1-ciclo es la permutación identidad. A los 2 ciclos también se los llama *transposiciones*. El hecho que el mismo símbolo (i, j) designe a un par ordenado y a una permutación no es grave, porque en cada caso el significado quedará claro por el contexto.

TEOREMA 1.1. *Toda permutación $\sigma \in \mathrm{S}_n$ se escribe como un producto $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$ de ciclos de orden mayor que 1 disjuntos dos a dos (y que por lo tanto conmutan entre si). Además el orden de σ es el mínimo de los múltiplos comunes de los órdenes de los σ_i's, y esta escritura es única, salvo el orden en que aparecen sus factores.*

DEMOSTRACIÓN. Primero probaremos la existencia, por inducción en la cantidad k de elementos de $\mathbb{I}_n$ que son movidos por σ. Si $k = 0$, entonces σ es la identidad, que puede pensarse como la composición de la familia vacía de ciclos. Supongamos que $k > 0$ y que el resultado vale para las permutaciones que mueven menos que k elementos. Tomemos $i_1 \in \mathbb{I}_n$ tal que $\sigma(i_1) \neq i_1$ y definamos $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$, $i_4 = \sigma(i_3)$, etcétera. Como $\mathbb{I}_n$ es finito existe un mínimo número natural r tal que $i_{r+1} \in \{i_1, \ldots, i_r\}$ y, como σ es inyectiva, forzosamente debe ser $i_{r+1} = i_1$. Consideremos el r-ciclo σ_1 definido por

$$\sigma_1(i_1) = i_2,\ \sigma_1(i_2) = i_3,\ \ldots,\ \sigma_1(i_{r-1}) = i_r \quad \text{y} \quad \sigma_1(i_r) = i_1.$$

Dado que el conjunto de puntos fijados por $\sigma_1^{-1} \circ \sigma$ es la unión disjunta de $\{i_1, \ldots, i_r\}$ y el conjunto de los puntos fijados por σ, se sigue de la hipótesis inductiva, que existen ciclos disjuntos $\sigma_2, \ldots, \sigma_s$ tales que

$$\sigma_1^{-1} \circ \sigma = \sigma_2 \circ \cdots \circ \sigma_s.$$

Como $\{i_1, \ldots, i_r\}$ es dejado fijo por cada uno de los ciclos $\sigma_2, \ldots, \sigma_s$ la expresión

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_s$$

es un producto de ciclos disjuntos dos a dos. Veamos ahora la unicidad. Supongamos que

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_s = \sigma'_1 \circ \cdots \circ \sigma'_{s'}$$

Si $s = 0$, entonces σ es la identidad, y también $s' = 0$. Supongamos que $s > 0$. Tomemos un elemento i_1 movido por σ_1. Entonces i_1 también es movido por un σ'_i y, como los σ'_j conmutan entre si, podemos suponer que $i = 1$. Es fácil ver que $\sigma_1^k(i_1) = \sigma^k(i_1) = {\sigma'_1}^k(i_1)$ para todo $k \in \mathbb{N}$. Pero entonces $\sigma_1 = \sigma'_1$ y, por lo tanto,

$$\sigma_2 \circ \cdots \circ \sigma_s = \sigma_2 \circ \cdots \circ \sigma_{s'}.$$

Un argumento inductivo muestra ahora que $s' = s$ y $\{\sigma_2, \ldots, \sigma_s\} = \{\sigma'_2, \ldots, \sigma'_{s'}\}$. Denotemos con r_j al orden de σ_j, con r' al de σ y con r al mínimo de los múltiplos comunes de los r_j's. Para terminar la demostración resta ver que $r = r'$. Por una parte, r' divide a r porque $\sigma^r = \sigma_1^r \circ \cdots \circ \sigma_s^r = \mathrm{id}$. Pero por otra parte, si i_j es movido por σ_j, entonces $\sigma_j^{r'}(i_j) = \sigma^{r'}(i_j) = i_j$, de manera que r_j divide a r' para todo j y así r divide a r'. □

Por ejemplo, del teorema anterior se sigue que los elementos de S_4 que son un 2-ciclo o producto de dos 2-ciclos disjuntos tienen orden 2, los 3-ciclos tienen orden 3 y los 4-ciclos, orden 4.

Escribamos una permutación $\sigma \in \mathrm{S}_n$ como un producto de ciclos distintos de la identidad y disjuntos dos a dos

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_s.$$

Denotemos con α_1 a la cantidad de puntos dejados fijos por σ y con α_j, para $1 < j \leq n$, a la cantidad de j-ciclos que aparecen en $\{\sigma_1, \ldots, \sigma_s\}$. Es claro $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n$. A la sucesión $[\alpha_1, \ldots, \alpha_n]$ la llamamos la *estructura cíclica* de σ.

Teorema 1.2. *Dos permutaciones son conjugadas en* S_n *si y sólo si tienen la misma estructura cíclica. Además si*

$$\sigma = (i_1, \ldots, i_{r_1}) \circ (i_{r_1+1}, \ldots, i_{r_2}) \circ \cdots \circ (i_{r_{s-1}+1}, \ldots, i_{r_s})$$

y τ *es una permutación arbitraria, entonces*

$$\tau \circ \sigma \circ \tau^{-1} = \big(\tau(i_1), \ldots, \tau(i_{r_1})\big) \circ \big(\tau(i_{r_1+1}), \ldots, \tau(i_{r_2})\big) \circ \cdots \circ \big(\tau(i_{r_{s-1}+1}), \ldots, \tau(i_{r_s})\big).$$

Demostración. Un cálculo sencillo muestra que, para cada r-ciclo $(i_1, \ldots, i_r)$ cada permutación τ,

$$\tau \circ (i_1, \ldots, i_r) \circ \tau^{-1} = (\tau(i_1), \ldots, \tau(i_r)).$$

En consecuencia, si σ se escribe como un producto de ciclos disjuntos dos a dos en la forma $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$, entonces

$$\tau \circ \sigma \circ \tau^{-1} = (\tau \circ \sigma_1 \circ \tau^{-1}) \circ \cdots \circ (\tau \circ \sigma_s \circ \tau^{-1})$$

tiene la misma estructura cíclica que σ. Recíprocamente, supongamos que σ y σ' son dos permutaciones que tienen la misma estructura cíclica y, más precisamente, que

$$\sigma = (i_1, \ldots, i_{r_1}) \circ (i_{r_1+1}, \ldots, i_{r_2}) \circ \cdots \circ (i_{r_{s-1}+1}, \ldots, i_{r_s})$$

y

$$\sigma' = (i'_1, \ldots, i'_{r_1}) \circ (i'_{r_1+1}, \ldots, i'_{r_2}) \circ \cdots \circ (i'_{r_{s-1}+1}, \ldots, i'_{r_s}).$$

Entonces la permutación $\tau \in \mathrm{S}_n$ definida por

$$\tau(i) := \begin{cases} i'_j & \text{si } i = i_j \text{ con } 1 \leq j \leq r_s, \\ \varphi(i) & \text{si } i \in \mathbb{I}_n \setminus \{i_1, \ldots, i_{r_s}\}, \end{cases}$$

donde $\varphi\colon \mathbb{I}_n \setminus \{i_1, \ldots, i_{r_s}\} \to \mathbb{I}_n \setminus \{i'_1, \ldots, i'_{r_s}\}$ es una función biyectiva arbitraria, satisface $\tau \circ \sigma \circ \tau^{-1} = \sigma'$. □

Por el teorema anterior cada clase de conjugación de S_n queda determinada unívocamente por la estructura cíclica de cada uno de sus elementos. Por consiguiente hay tantas clases de conjugación como sucesiones $\alpha_1, \ldots, \alpha_n \geq 0$ que satisfacen

$$\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n.$$

Para cada una de esta sucesiones, consideremos los números $\mu_j := \alpha_j + \cdots + \alpha_n$. Por su misma definición

$$\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n \qquad \text{y} \qquad \mu_1 + \cdots + \mu_n = n. \tag{26}$$

Las sucesiones de énteros no negativos que satisfacen (26) son llamadas *particiones* de n porque dan las formas de "partir" n como suma de n o menos números naturales. Por otro lado, dada una partición $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n$ de n, podemos definir

$$\alpha_j := \begin{cases} \mu_j - \mu_{j+1} & \text{si } j < n, \\ \mu_n & \text{si } j = n, \end{cases}$$

y claramente

$$\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = \mu_1 + \cdots + \mu_n = n.$$

Dado que estas correspondencias son inversa una de la otra, hay tantas clases de conjugación de S_n como particiones de n.

Ejemplo 1.3. *Las particiones de* 5 *son*

$(1,1,1,1,1)$, $(2,1,1,1,0)$, $(2,2,1,0,0)$, $(3,1,1,0,0)$, $(3,2,0,0,0)$, $(4,1,0,0,0)$ *y* $(5,0,0,0,0)$.

Por lo tanto S_5 *tiene* 7 *clases de conjugación.*

Por último, la cantidad de elementos que tiene la clase de conjugación asociada a la estructura cíclica $[\alpha_1, \ldots, \alpha_n]$ es

$$\frac{n!}{1^{\alpha_1}\alpha_1!2^{\alpha_2}\alpha_2! \ldots n^{\alpha_n}\alpha_n!}. \tag{27}$$

En efecto, esto se sigue de que cada j-ciclo se puede obtener de j formas distintas

$$(i_1, \ldots, i_j) = (i_2, \ldots, i_j, i_1) = \cdots = (i_j, i_1, \ldots, i_{j-1})$$

y de que si permutamos entre si ciclos de orden j, obtenemos la misma permutación de S_n. La expresión (27) es conocida como fórmula de Cauchy.

Observación 1.4. *El Teorema 1.2 puede usarse para probar que si un morfismo de grupos* $f\colon G \to H$ *no es sobreyectivo, entonces tampoco es un epimorfismo. Con este fin escribamos* $K := \operatorname{Im} f$ *y supongamos que* K *es un subgrupo propio de* H*. Debemos mostrar que hay un grupo* N *y morfismos distintos* $\alpha, \beta\colon H \to N$ *tales que* $\alpha_{|K} = \beta_{|K}$*. Tomemos* $N := \mathrm{S}_X$*, donde* X *es el conjunto de las coclases a izquierda de* K *en* H*, junto con un elemento adicional* $*$*. Definamos* α *por*

$$\alpha(h)(x) := \begin{cases} * & \text{si } x = *, \\ hx & \text{si } x \neq *, \end{cases}$$

y β *como la composición* $\Phi_\tau \circ \alpha$*, donde* Φ_τ *es la conjugación por la transposición* τ *de* X *que intercambia* K *con* $*$*. Es fácil ver que* α *es un morfismo de grupos y es evidente que* $*$ *es un punto fijo de* $\alpha(h)$ *para todo* $h \in H$*, mientras que* K *es un punto fijo de* $\alpha(h)$ *si y sólo si* $h \in K$*. En consecuencia, por la segunda afirmación del Teorema 1.2,*

$$\beta(h) = \Phi_\tau(\alpha(h)) = \alpha(h)$$

si y sólo si $h \in K$*, que es más que lo que necesitábamos probar.*

En los ejemplos que siguen encontramos condiciones sobre n y m para que S_m contenga un subgrupo isomorfo a $\mathbb{Z}_n$ y a D_n respectivamente. Para realizar los cálculos es conveniente usar la estructura cíclica de las permutaciones involucradas en ellos.

EJEMPLO 1.5. *Supongamos que $n \geq 2$ y tomemos $\sigma := (1, \ldots, n)$. Como $|\sigma| = n$ el grupo $\langle\sigma\rangle$ es cíclico y tiene orden n. Supongamos ahora que $n \geq 2$ y que $n = n_1 \cdots n_r$ con los n_i coprimos dos a dos. De la misma manera que arriba, para cada i podemos elegir $\sigma_i \in \mathrm{S}_{n_1+\cdots+n_r}$ tal que $|\sigma_i| = n_i$ y*

$$\sigma_i(j) = j \quad \text{para todo } j \text{ tal que } j \leq n_1 + \cdots + n_{i-1} \text{ o } j > n_1 + \cdots + n_i.$$

Como evidentemente $\sigma := \sigma_1 \circ \cdots \circ \sigma_r$ tiene orden n, el grupo $\mathrm{S}_{n_1+\cdots+n_r}$ contiene un subgrupo isomorfo a $\mathbb{Z}_n$.

EJEMPLO 1.6. *Supongamos que $n > 2$ y tomemos τ y σ en S_n definidos por*

$$\sigma := (1, \ldots, n) \quad y \quad \tau := \begin{cases} (1,n) \circ (2,n-1) \circ \cdots \circ ((n-1)/2, (n+3)/2) & \text{si } n \text{ es impar,} \\ (1,n) \circ (2,n-1) \circ \cdots \circ (n/2, (n+2)/2) & \text{si } n \text{ es par.} \end{cases}$$

Como

$$|\tau| = 2, \quad |\sigma| = n \quad y \quad \tau \circ \sigma \circ \tau = \sigma^{-1} \tag{28}$$

el grupo $\langle\sigma, \tau\rangle$ no es conmutativo y tiene orden menor o igual a $2n$. Dado que por otra parte $\langle\sigma\rangle$ es un subgrupo conmutativo de orden n de $\langle\sigma, \tau\rangle$, se sigue del teorema de Lagrange que necesariamente $|\langle\sigma, \tau\rangle| = 2n$. Así, debido a la Observación 14.12 del Capítulo 1, el subgrupo $\langle\sigma, \tau\rangle$ de S_n es isomorfo a D_n. Supongamos ahora que $n > 2$ y que $n = n_1 \cdots n_r$ con los n_i coprimos dos a dos. De la misma manera que arriba, para cada i podemos elegir σ_i y τ_i en $\mathrm{S}_{n_1+\cdots+n_r}$ tales que

$$|\tau_i| = 2, \qquad |\sigma_i| = n_i, \qquad \tau_i \circ \sigma_i \circ \tau_i = \sigma_i^{-1}$$

y

$$\sigma_i(j) = \tau_i(j) = j \quad \text{para todo } j \text{ tal que } j \leq n_1 + \cdots + n_{i-1} \text{ o } j > n_1 + \cdots + n_i$$

Es evidente que $\sigma := \sigma_1 \circ \cdots \circ \sigma_r$ y $\tau := \tau_1 \circ \cdots \circ \tau_r$ satisfacen las condiciones de (28). Así el mismo argumento que antes muestra que $\mathrm{S}_{n_1+\cdots+n_r}$ contiene un subgrupo isomorfo a D_n.

2. Generadores de $\mathrm{S_n}$

Un cálculo directo muestra que

$$(i_1, \ldots, i_r) = (i_1, i_r) \circ (i_1, i_{r-1}) \circ \cdots \circ (i_1, i_2) \quad \text{y} \quad (1, i_1) \circ (1, i_j) \circ (1, i_1) = (i_1, i_j).$$

Como cada permutación es producto de ciclos se sigue de esto que

$$\mathrm{S}_n = \langle (1,2), (1,3), \ldots, (1,n) \rangle.$$

Como además $(i, i+1) \circ (1, i) \circ (i, i+1) = (1, i+1)$ para todo $i < n$, es claro que también

$$\mathrm{S}_n = \langle (1,2), (2,3), \ldots, (n-1,n) \rangle.$$

Por último, usando la igualdad $(1, \ldots, n)^{i-1} \circ (1,2) \circ (1, \ldots, n)^{-i+1} = (i, i+1)$, válida para $i < n$, concluímos que

$$\mathrm{S}_n = \langle (1,2), (1, \ldots, n) \rangle.$$

3. El signo de una permutación

Un par $(i,j) \in \mathbb{I}_n \times \mathbb{I}_n$ es un *descenso* de una permutación $\sigma \in \mathrm{S}_n$ si $i < j$ y $\sigma(i) > \sigma(j)$. Designamos con $\mathrm{Des}(\sigma)$ al conjunto de descensos de σ. Por definición el *signo* de σ es

$$\mathrm{sg}(\sigma) := (-1)^{|\,\mathrm{Des}(\sigma)|}.$$

La propiedad más importante de la función $\mathrm{sg}\colon \mathrm{S}_n \to \{-1,1\}$ es que, como estableceremos en el Teorema 3.3, es un morfismo sobreyectivo de grupos.

Proposición 3.1. *Para cada $\sigma \in \mathrm{S}_n$ y cada $k<n$, la cantidad de descensos de $(k,k+1)\circ\sigma$ difiere en ± 1 de la de σ.*

Demostración. Es evidente que:

- Si $\sigma(\{i,j\}) \neq \{k,k+1\}$, entonces $(i,j) \in \mathrm{Des}((k,k+1)\circ\sigma)$ si y sólo si $(i,j) \in \mathrm{Des}(\sigma)$.
- Si $\sigma(\{i,j\}) = \{k,k+1\}$, entonces $(i,j) \in \mathrm{Des}((k,k+1)\circ\sigma)$ si y sólo si $(i,j) \notin \mathrm{Des}(\sigma)$.

El resultado se sigue fácilmente de estas observaciones. □

Corolario 3.2. *Si $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$, donde las σ_i's son transposiciones de elementos consecutivos, entonces s es congruente a $|\,\mathrm{Des}(\sigma)|$ módulo 2.*

Demostración. Se sigue fácilmente de la Proposición 3.1 haciendo inducción en s. □

Teorema 3.3. *La función $\mathrm{sg}\colon \mathrm{S}_n \to \{-1,1\}$ es un morfismo sobreyectivo.*

Demostración. Por el Corolario 3.2, si $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$, donde las σ_i's son transposiciones de elementos consecutivos, entonces $\mathrm{sg}(\sigma) = (-1)^s$. Usando esta caracterización es muy fácil ver que sg es un morfismo. Además es sobreyectivo porque $\mathrm{sg}(\mathrm{id}) = 1$ y $\mathrm{sg}(1,2) = -1$. □

Proposición 3.4. *Si σ es un r-ciclo $(i_1,\ldots,i_r)$, entonces $\mathrm{sg}(\sigma) = (-1)^{r-1}$.*

Demostración. Supongamos que σ es el r-ciclo $(i_1,\ldots,i_r)$. Como

$$\sigma = (i_1,i_r)\circ(i_1,i_{r-1})\circ\cdots\circ(i_1,i_2),$$

debido al teorema anterior es suficiente probar que el signo de cada transposición es -1. Es evidente que esto pasa para las transposiciones $(i,i+1)$ de elementos consecutivos. Supongamos ahora que ya sabemos que el signo de (i,j) es -1 y que $j < n$. Entonces dado que $(i,j+1) = (j,j+1)\circ(i,j)\circ(j,j+1)$ se sigue nuevamente del teorema anterior que también el signo de $(i,j+1)$ es -1. □

Proposición 3.5. *Si $\sigma \in \mathrm{S}_n$ tiene estructura cíclica $[\alpha_1,\ldots,\alpha_n]$, entonces*

$$\mathrm{sg}(\sigma) = (-1)^{n-s},$$

donde $s = \alpha_1 + \cdots + \alpha_n$.

Demostración. Escribamos $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$, de σ como producto de ciclos disjuntos, donde los primeros α_2 ciclos tienen orden 2, los siguientes α_3 tienen orden 3, etcétera. Por el Teorema 3.3 y la Proposición 3.4

$$\mathrm{sg}(\sigma) = \mathrm{sg}(\sigma_1)\cdots\mathrm{sg}(\sigma_s) = (-1)^{\sum_{j=2}^{n}\alpha_j(j-1)} = (-1)^{\sum_{j=1}^{n}\alpha_j j - \sum_{j=1}^{n}\alpha_j} = (-1)^{n-s},$$

como queríamos. □

Decimos que una permutación es par si su signo es 1 e impar si es -1. El *grupo alternado* A_n es, por definición, el subgrupo de S_n formado por las permutaciones pares. Como A_n es el núcleo de sg, es un subgrupo normal de orden $n!/2$ de S_n.

OBSERVACIÓN 3.6. *La aplicación* $\theta\colon \mathrm{S}_n \to \mathrm{A}_{n+2}$, *definida por*

$$\theta(\sigma) := \begin{cases} \sigma & \text{si } \sigma \text{ es par,} \\ \sigma \circ (n+1, n+2) & \text{si } \sigma \text{ es impar,} \end{cases}$$

es un morfismo inyectivo de grupos.

PROPOSICIÓN 3.7. *Si* H *es un subgrupo de* S_n *y* $H \not\subseteq \mathrm{A}_n$, *entonces* $H \cap \mathrm{A}_n$ *es un subgrupo normal de índice* 2 *de* H. *Además si* H *tiene una permutación impar* σ *de orden dos, entonces* H *es el producto semidirecto interno de* $H \cap \mathrm{A}_n$ *y* $\{\mathrm{id}, \sigma\}$.

DEMOSTRACIÓN. Tomemos $\sigma \in H \setminus \mathrm{A}_n$. Como la función

$$\begin{array}{ccc} H \cap \mathrm{A}_n & \longrightarrow & H \setminus \mathrm{A}_n \\ \tau & \longmapsto & \tau \circ \sigma \end{array}$$

es biyectiva, $H \cap \mathrm{A}_n$ es un subgrupo de índice 2 de H y, por lo tanto, es normal. Supongamos ahora que σ es una permutación impar de orden dos. Como

$$(H \cap \mathrm{A}_n) \cap \{\mathrm{id}, \sigma\} = \{\mathrm{id}\} \qquad \text{y} \qquad (H \cap \mathrm{A}_n)\{\mathrm{id}, \sigma\} = H,$$

el grupo H es el producto semidirecto interno de $H \cap \mathrm{A}_n$ y $\{\mathrm{id}, \sigma\}$. □

DEMOSTRACIÓN ALTERNATIVA DE LA PROPOSICIÓN 3.7. Por la Observación 6.12 del Capítulo 1 sabemos que $|H : H \cap \mathrm{A}_n| \leq |\mathrm{S}_n : A_n| = 2$. En consecuencia, como $H \cap \mathrm{A}_n \neq H$, necesariamente $|H : H \cap \mathrm{A}_n| = 2$.

4. Generadores de $\mathbf{A_n}$

Como cada elemento de A_n es producto de un número par de transposiciones y

$$(a,b) \circ (a,c) = (a,c,b), \qquad (a,b) \circ (c,d) = (a,b,c) \circ (b,c,d) \qquad \text{y} \qquad (a,b,c) = (a,c,b)^2,$$

donde a, b, c, d son elementos distintos de $\mathbb{I}_n$, el grupo alternado A_n está generado por los cuadrados de los 3-ciclos. El resultado que sigue, combinado con lo que acabamos de ver, prueba que los cuadrados de $(1,3,2), (1,4,2), \ldots, (1,n,2)$ generan a A_n.

TEOREMA 4.1. *Para todo* $n \in \mathbb{N}$,

$$\mathrm{A}_n = \langle (1,2,3), (1,2,4), \ldots, (1,2,n) \rangle.$$

DEMOSTRACIÓN. Cuando $n < 3$ el resultado es trivial. Supongamos que $n \geq 3$. Como A_n está generado por los 3-ciclos y, para cada terna a, b, c de elementos de $\mathbb{I}_n$ distintos de 1,

$$(a,b,c) = (1,c,b) \circ (1,a,b) \circ (1,a,c),$$

para concluir la demostración será suficiente mostrar que cada 3-ciclo $(1,a,b)$ con $a \neq 2$ es producto de 3-ciclos de la forma $(1,2,i)$ con $3 \leq i \leq n$. Pero esto es así, porque

$$(1,a,2) = (1,2,a)^2 \qquad \text{y} \qquad (1,a,b) = (1,2,b)^2 \circ (1,2,a) \circ (1,2,b)$$

para cada par a, b de elementos de $\mathbb{I}_n$ distintos de 1 y 2. □

COROLARIO 4.2. A_n *es un subgrupo completamente normal de* S_n.

DEMOSTRACIÓN. Para cada endomorfismo $f\colon \mathrm{S}_n \to \mathrm{S}_n$ y cada 3-ciclo $\tau \in \mathrm{S}_n$ el orden de $f(\tau)$ es 1 o 3. Por lo tanto en la descomposición cíclica de $f(\tau)$ sólo hay 3-ciclos y puntos fijos y, en consecuencia, $f(\tau) \in \mathrm{A}_n$. □

TEOREMA 4.3. *Para todo $n \in \mathbb{N}$,*

$$\begin{aligned}\mathrm{A}_n &= \langle (1,2)\circ(2,3), (1,2)\circ(3,4), \ldots, (1,2)\circ(n-1,n)\rangle \\ &= \langle (2,3)\circ(1,2), (3,4)\circ(1,2), \ldots, (n-1,n)\circ(1,2)\rangle.\end{aligned}$$

DEMOSTRACIÓN. Como

$$(1,2)\circ(2,3) = (2,3)\circ(1,2)\circ(2,3)\circ(1,2)$$

y

$$(1,2)\circ(j,j+1) = (j,j+1)\circ(1,2) \quad \text{para todo } j > 2,$$

es suficiente probar la primera igualdad. Por el teorema anterior, para ello bastará verificar que el subgrupo de A_n generado por $(1,2)\circ(2,3), \ldots, (1,2)\circ(n-1,n)$ contiene a los 3-ciclos $(1,2,3), \ldots, (1,2,n)$, lo que se sigue por inducción en j, usando que $(1,2,3) = (1,2)\circ(2,3)$ y

$$\big((1,2)\circ(j,j+1)\circ(1,2,j)\circ(1,2)\circ(j,j+1)\big)^2 = (1,j+1,2)^2 = (1,2,j+1),$$

para todo $j \geq 3$. □

5. El conmutador y el centro de $\mathbf{S_n}$ y $\mathbf{A_n}$

En esta sección calculamos el conmutador y el centro de S_n y A_n.

TEOREMA 5.1. $[\mathrm{S}_n, \mathrm{S}_n] = \mathrm{A}_n$ *para todo* $n \in \mathbb{N}$ *y* $[\mathrm{A}_n, \mathrm{A}_n] = \mathrm{A}_n$ *para todo* $n \geq 5$.

DEMOSTRACIÓN. El subgrupo conmutador de S_n está incluído en A_n, porque

$$\mathrm{sg}([\sigma,\tau]) = \mathrm{sg}(\sigma)\,\mathrm{sg}(\tau)\,\mathrm{sg}(\sigma^{-1})\,\mathrm{sg}(\tau^{-1}) = 1 \quad \text{para todo } \sigma,\tau \in \mathrm{S}_n,$$

debido a que $\mathrm{sg}(\sigma) = \mathrm{sg}(\sigma^{-1})$ y $\mathrm{sg}(\tau) = \mathrm{sg}(\tau^{-1})$. Por el Teorema 4.1, para probar que vale la inclusión opuesta será suficiente mostrar que los 3-ciclos son conmutadores, lo cual es cierto, porque de hecho,

$$(a,b,c) = [(a,b),(a,c)] \quad \text{para toda terna } a,b,c \text{ de elementos de } \mathbb{I}_n.$$

Para probar que $[\mathrm{A}_n, \mathrm{A}_n] = \mathrm{A}_n$ para todo $n \geq 5$, es suficiente observar que si $a,b,c,d,e \in \mathbb{I}_n$ son todos distintos, entonces

$$(a,b,c) = [(a,c,d),(a,d,e)][(a,b,d),(a,d,e)],$$

lo que se sigue facilmente de que

$$[(a,x,d),(a,d,e)] = (a,x,d)\circ(a,d,e)\circ(a,d,x)\circ(a,e,d) = (a,x)\circ(d,e),$$

para $x = b$ o $x = c$. □

OBSERVACIÓN 5.2. *Como* A_2 *y* A_3 *son conmutativos,* $[\mathrm{A}_i, \mathrm{A}_i] = 1$ *cuando* $i \leq 3$. *En cuanto a* $[\mathrm{A}_4, \mathrm{A}_4]$, *debido a que el subgrupo*

$$H := \{\mathrm{id}, (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3)\}$$

de A_4 *es normal y* A_4/H *es abeliano,* $[\mathrm{A}_4, \mathrm{A}_4] \subseteq H$. *Por otro lado, las igualdades*

$$(1,x)\circ(y,z) = [(1,x,y),(1,y,z)]$$

válida para $x,y,z \in \{2,3,4\}$ *distintos, muestra que la inclusión opuesta también vale.*

TEOREMA 5.3. *Si $n \geq 3$, entonces $\mathrm{Z}\,\mathrm{S}_n = 1$ y si $n \geq 4$, entonces $\mathrm{Z}\,\mathrm{A}_n = 1$.*

DEMOSTRACIÓN. Primero consideramos el grupo simétrico. Tomemos $\sigma \in \mathrm{S}_n$. Si en la descomposición cíclica de σ hay dos ciclos no triviales,

$$\sigma = (i_1, i_2, \ldots, i_{r_1}) \circ (j_1, j_2, \ldots, j_{r_2}) \circ \cdots,$$

entonces tomando $\tau := (i_1, j_1, j_2)$ obtenemos

$$\tau \circ \sigma \circ \tau^{-1} = (j_1, i_2, \ldots, i_{r_1}) \circ (j_2, i_1, j_3, \ldots, j_{r_2}) \circ \cdots \neq \sigma.$$

Si σ es un ciclo $(i_1, i_2, i_3, \ldots, i_r)$ de longitud al menos 3, entonces tomando $\tau := (i_1, i_2)$ obtenemos

$$\tau \circ \sigma \circ \tau^{-1} = (i_2, i_1, i_3, \ldots i_r) \neq \sigma.$$

Finalmente, si σ es una transposición (i_1, i_2), entonces existe $i_3 \in \mathbb{I}_n$ distinto de i_1 e i_2, y tomando $\tau := (i_2, i_3)$ obtenemos

$$\tau \circ \sigma \circ \tau^{-1} = (i_1, i_3) \neq \sigma.$$

Ahora consideramos el grupo alternado. Tomemos $\sigma \in \mathrm{A}_n$. Si en la descomposición cíclica de σ hay dos ciclos no triviales, entonces podemos proceder como con S_n. Si σ es un ciclo $(i_1, i_2, i_3, i_4, \ldots, i_r)$ de longitud al menos 5, entonces tomando $\tau := (i_1, i_2) \circ (i_3, i_4)$ obtenemos

$$\tau \circ \sigma \circ \tau^{-1} = (i_2, i_1, i_4, i_3, i_5, \ldots, i_r) \neq \sigma.$$

Finalmente, si σ es un 3-ciclo (i_1, i_2, i_3), entonces existe $i_4 \in \mathbb{I}_n$ distinto de i_1, i_2 e i_3 y tomando $\tau := (i_1, i_2)(i_3, i_4)$ obtenemos

$$\tau \circ \sigma \circ \tau^{-1} = (i_2, i_1, i_4) \neq \sigma,$$

lo que termina la demostración. □

OBSERVACIÓN 5.4. *Como S_2, A_2 y A_3 son conmutativos,*

$$\mathrm{Z}\,\mathrm{S}_2 = \mathrm{S}_2 \qquad y \qquad \mathrm{Z}\,\mathrm{A}_i = \mathrm{A}_i \quad \textit{para } i \in \{2, 3\}.$$

Simplicidad de $\mathbf{A_n}$

Claramente $\mathbb{Z}_p$ es simple para todo primo p. Esta es la familia más sencilla de grupos simples y estos son todos los grupos simples conmutativos. El siguiente resultado muestra que existe al menos una familia infinita de grupos simples no conmutativos.

TEOREMA 5.5. *El grupo alternado A_n es simple para todo $n \geq 3$ y distinto de 4.*

DEMOSTRACIÓN. El grupo A_3 es simple porque es cíclico de orden 3. Asumamos entonces que $n \geq 5$ y tomemos un subgrupo normal $H \neq 1$ de A_n. Afirmamos que H contiene a todos los 3-ciclos y que, por lo tanto, es igual a A_n. Veamos primero que H contiene a un 3-ciclo. Para ello fijemos $\sigma \in H$ distinto de la identidad. Si σ es un 3-ciclo no hay nada que probar y si σ tiene un ciclo $(i_1, i_2, i_3, i_4, i_5, \ldots, i_r)$ de longitud al menos 4 en su descomposición cíclica, entonces tomando $\tau := (i_1, i_2, i_3)$ obtenemos que H contiene a

$$\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} = (i_1, i_2, i_3) \circ (i_2, i_4, i_3) = (i_1, i_2, i_4).$$

Podemos suponer entonces que todos los ciclos de la descomposición cíclica de σ tienen longitud menor que 4 y que en esta descomposición hay al menos dos ciclos.

1. Si $\sigma = (i_1, i_2, i_3) \circ (j_1, j_2, j_3) \circ \cdots$ o $\sigma = (i_1, i_2) \circ (j_1, j_2, j_3) \circ \cdots$ tiene al menos un ciclo de longitud 3 en su descomposición cíclica, entonces tomando $\tau := (i_1, j_1, j_2)$, obtenemos que H contiene a
$$\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} = (i_1, j_1, j_2) \circ (i_2, j_3, j_2) = (i_1, j_1, j_2, i_2, j_3),$$
lo que nos reduce al caso ya tratado.
2. Si $\sigma = (i_1, i_2) \circ (i_3, i_4) \circ \cdots$ tiene al menos dos ciclos de longitud 2 en su descomposición cíclica y un punto fijo i_5, entonces tomando $\tau := (i_1, i_5, i_3)$, obtenemos que
$$\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} = (i_1, i_5, i_3) \circ (i_2, i_4, i_5) = (i_1, i_5, i_2, i_4, i_3)$$
está en H, lo que nuevamente nos reduce al caso ya tratado.
3. Si $\sigma = (i_1, i_2) \circ (i_3, i_4) \circ (i_5, i_6) \circ \cdots$ tiene al menos tres ciclos de longitud 2 en su descomposición cíclica, entonces tomando $\tau := (i_1, i_5, i_3)$, obtenemos que
$$\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} = (i_1, i_5, i_3) \circ (i_2, i_4, i_6)$$
está en H, lo que nos reduce al caso ya tratado en el item 1.

Por lo tanto, concluímos que H siempre tiene un 3-ciclo (i_1, i_2, i_3). Veamos ahora que los tiene a todos. Tomemos otro 3-ciclo arbitrario (j_1, j_2, j_3). Por el Teorema 1.2, existe $t \in \mathrm{S}_n$ tal que $(j_1, j_2, j_3) = t \circ (i_1, i_2, i_3) \circ t^{-1}$. Si $t \in \mathrm{A}_n$ entonces $(j_1, j_2, j_3) \in H$ por definición. Si no, podemos tomar $k_1, k_2 \in \mathbb{I}_n \setminus \{j_1, j_2, j_3\}$ distintos, y entonces

$$(j_1, j_2, j_3) = (k_1, k_2) \circ (j_1, j_2, j_3) \circ (k_1, k_2)^{-1} = \big((k_1, k_2) \circ t\big) \circ (i_1, i_2, i_3) \circ \big((k_1, k_2) \circ t\big)^{-1}.$$

Como $(k_1, k_2) \circ t \in \mathrm{A}_n$, esto implica que $(j_1, j_2, j_3) \in H$. □

Teorema 5.6. *Si $n \geq 5$, entonces el único subgrupo invariante y no trivial de S_n es A_n.*

Demostración. Supongamos que H es un subgrupo no trivial e invariante de S_n. Entonces $H \cap \mathrm{A}_n$ es un subgrupo invariante de A_n y, por el teorema anterior, forzosamente $H \cap \mathrm{A}_n = \mathrm{A}_n$ o $H \cap \mathrm{A}_n = 1$. Como A_n tiene índice 2, en el primer caso $H = \mathrm{A}_n$. Para terminar la demostración, debemos ver que la intersección de H con A_n no puede ser 1. Pero si $H \cap \mathrm{A}_n = 1$, entonces por la Proposición 3.7, existe $\tau \in \mathrm{S}_n$ tal que $H = \{\mathrm{id}, \tau\}$, lo que se contradice con que H es normal pues, como τ tiene orden 2 es un producto de 2-ciclos disjuntos y, en consecuencia, por el Teorema 1.2, su clase de conjugación tiene más de un elemento. □

Debido a que todo subgrupo de índice 2 de un grupo es invariante, del Teorema 5.5 se sigue que A_n no tiene subgrupos de orden $n!/4$ para ningún $n \geq 5$. El primer item del siguiente resultado muestra que A_4 también tiene esta propiedad. El segundo muestra que para S_4 vale una versión débil del teorema anterior.

Proposición 5.7. *El grupo A_4 tiene las siguientes propiedades:*

1. *No tiene subgrupos de orden 6.*
2. *Es el único subgrupo de orden 12 de S_4.*

Demostración. 1) Si H es un subgrupo de orden 6 de A_4, entonces es normal porque tiene índice 2. Pero entonces $\tau^2 \in H$ para todo $\tau \in \mathrm{A}_4$ pues la clase de τ^2 en A_4/H es 1. Dado que si τ es un 3-ciclo, $\tau = \tau^4 = (\tau^2)^2$, esto implica que H contiene a todos los 3-ciclos de S_4, lo que es absurdo porque hay 8.

2) Supongamos que $H \neq \mathrm{A}_4$ es un subgrupo de orden 12 de S_4. Entonces, por la Proposición 3.7 del Capítulo 1, el subgrupo $H \cap \mathrm{A}_4$ de A_4 tiene orden 6, lo que se contradice con el item 1). □

6. Presentaciones de $\mathbf{S_n}$ y $\mathbf{A_n}$

El objetivo de esta sección es dar presentaciones de S_n y A_n. Comenzamos con el grupo simétrico.

TEOREMA 6.1. *Para cada $n \geq 2$, el grupo simétrico S_n es canónicamente isomorfo al grupo generado por los elementos $s_1, \ldots, s_{n-1}$ sujetos a las relaciones*

$$\begin{aligned} &s_i^2 = 1, && \text{para todo } i, \\ &s_i s_j = s_j s_i, && \text{si } j - i \geq 2, \\ &s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, && \text{para } i < n-1. \end{aligned}$$

DEMOSTRACIÓN. Procedemos por inducción en n. Es obvio que el resultado es cierto para $n = 2$. Supongamos que lo es para $n-1$ y denotemos con G al grupo generado por los elementos $s_1, \ldots, s_{n-1}$ sujetos a las relaciones mencionadas arriba. Es evidente que la función $\psi\colon G \to \mathrm{S}_n$, definida por $\psi(s_i) = (i, i+1)$, es un morfismo sobreyectivo. Para terminar la demostración debemos ver que también es inyectivo, para lo cual será suficiente probar que $|G| \leq n!$. Claramente el subgrupo G' de G generado por $s_1, \ldots, s_{n-2}$ es un cociente del grupo con generadores $s_1, \ldots, s_{n-2}$, sujetos a relaciones similares a las de arriba y, por lo tanto, $|G'| \leq (n-1)!$ debido a la hipótesis inductiva. Consideremos ahora los subconjuntos $C_1, \ldots, C_n$ de G, definidos por $C_i := G' s_{n-1} s_{n-2} \cdots s_{i+1} s_i$. Afirmamos que para cada $1 \leq i \leq n$ y $1 \leq j < n$ existe $1 \leq i' \leq n$ tal que $C_i s_j = C_{i'}$. En efecto, si $i < j$

$$\begin{aligned} C_i s_j &= G' s_{n-1} s_{n-2} \cdots s_{j+1} s_j s_{j-1} s_{j-2} \cdots s_{i+1} s_i s_j \\ &= G' s_{n-1} s_{n-2} \cdots s_{j+1} s_j s_{j-1} s_j s_{j-2} \cdots s_{i+1} s_i \\ &= G' s_{n-1} s_{n-2} \cdots s_{j+1} s_{j-1} s_j s_{j-1} s_{j-2} \cdots s_{i+1} s_i \\ &= G' s_{j-1} s_{n-1} s_{n-2} \cdots s_{j+1} s_j s_{j-1} s_{j-2} \cdots s_{i+1} s_i \\ &= G' s_{n-1} s_{n-2} \cdots s_{j+1} s_j s_{j-1} s_{j-2} \cdots s_{i+1} s_i \\ &= C_i, \end{aligned}$$

donde la anteúltima igualdad se sigue de que $s_{j-1} \in G'$, porque $j - 1 < n - 1$. Si $j + 1 < i$, entonces

$$\begin{aligned} C_i s_j &= G' s_{n-1} s_{n-2} \cdots s_{i+1} s_i s_j \\ &= G' s_j s_{n-1} s_{n-2} \cdots s_{i+1} s_i \\ &= G' s_{n-1} s_{n-2} \cdots s_{i+1} s_i \\ &= C_i, \end{aligned}$$

donde la antenúltima igualdad se sigue de que $s_j \in G'$ porque $j < n - 1$. Finalmente,

$$C_j s_j = G' s_{n-1} s_{n-2} \cdots s_{j+1} s_j s_j = G' s_{n-1} s_{n-2} \cdots s_{j+1} = C_{j+1}$$

y

$$C_{j+1} s_j = G' s_{n-1} s_{n-2} \cdots s_{j+1} s_j = C_j.$$

En consecuencia, para cada $i \leq n$ y $s \in G$, existe $i' \leq n$ tal que $C_i s = C_{i'}$. Como $1 \in G' = C_n$, obtenemos en particular que $G \subseteq \bigcup_{i=1}^{n} C_i$, por lo que $|G| \leq \sum_{i=1}^{n} |C_i| = n|G'| \leq n!$. □

OBSERVACIÓN 6.2. *Las relaciones que satisfacen $s_1, \ldots, s_{n-1}$ pueden expresarse en la forma*

$$\begin{aligned} &s_i^2 = 1, && \text{para todo } i, \\ &(s_i s_j)^2 = 1, && \text{si } j - i \geq 2, \\ &(s_i s_{i+1})^3 = 1, && \text{para } i < n-1, \end{aligned}$$

que fue la utilizada al definir la noción general de presentación.

TEOREMA 6.3. *Para cada $n \geq 3$, el grupo alternado A_n es canónicamente isomorfo al grupo generado por los elementos $t_1, \ldots, t_{n-2}$ sujetos a las relaciones*

$$\begin{aligned} &t_1^3 = 1, && \\ &t_i^2 = 1, && \text{para } i > 1, \\ &(t_i t_j)^2 = 1, && \text{si } j - i \geq 2, \\ &(t_i t_{i+1})^3 = 1, && \text{para } i < n-2. \end{aligned}$$

DEMOSTRACIÓN. Consideremos el grupo G generado por los elementos $t_1, \ldots, t_{n-2}$ sujetos a las relaciones mencionadas arriba. Es evidente que la función

$$\begin{array}{ccc} \{t_1, \ldots, t_{n-2}\} & \longrightarrow & \mathrm{A}_n \\ t_i & \longmapsto & (i+1, i+2)(1,2) \end{array},$$

se extiende univocamente a un morfismo $\psi\colon G \to \mathrm{A}_n$. Dado que, por el Teorema 4.3, este morfismo es sobreyectivo, para terminar la demostración será suficiente ver que $|G| \leq n!/2$. Probaremos esto mostrando que hay un producto semidirecto $G \rtimes_\vartheta C_2$, donde C_2 es el grupo cíclico con dos elementos {1,g}, y un morfismo sobreyectivo $\mathrm{S}_n \to G \rtimes_\vartheta C_2$. Para empezar, es fácil ver que la función $\vartheta\colon C_2 \to \mathrm{Aut}(G)$, dada por $\vartheta(g)(t_i) := t_i^{-1}$, es un morfismo bien definido. Por ejemplo, la relación $(t_1 t_2)^3 = 1$ se transforma por $\vartheta(g)$ en la relación $(t_1^{-1} t_2^{-1})^3 = 1$, la cual vale porque

$$t_1 t_2 t_1 t_2 t_1 t_2 = 1 \Rightarrow t_2^{-1} t_1^{-1} t_2^{-1} t_1^{-1} t_2^{-1} t_1^{-1} = 1 \Rightarrow t_1^{-1} t_2^{-1} t_1^{-1} t_2^{-1} t_1^{-1} t_2^{-1} = 1.$$

Podemos considerar entonces el producto cruzado $G \rtimes_\vartheta C_2$. Llamemos G' al grupo generado por los elementos $s_1, t_1, \ldots, t_{n-2}$, sujetos a las relaciones

$$\begin{aligned} &s_1^2 = t_1^3 = 1, && \\ &(s_1 t_i)^2 = 1 && \text{para todo } i, \\ &t_i^2 = 1, && \text{para } i > 1, \\ &(t_i t_j)^2 = 1, && \text{si } j - i \geq 2, \\ &(t_i t_{i+1})^3 = 1, && \text{para } i < n-2, \end{aligned}$$

y escribamos $s_{i+1} = s_1 t_i$ para $1 \leq i < n-1$. La relaciones dadas arriba para $s_1, t_1, \ldots, t_{n-2}$ son equivalentes a las dadas en la Observación 6.2 para $s_1, \ldots, s_{n-1}$. Por lo tanto,

$$G' = \langle s_1, t_1, \ldots, t_{n-2} \rangle = \langle s_1, \ldots, s_{n-1} \rangle \simeq \mathrm{S}_n\,.$$

Por consiguiente, para terminar la demostración es suficiente notar que existe un morfismo de grupos $\varphi\colon G' \to G \rtimes_\vartheta C_2$, tal que $\varphi(t_i) = (t_i, 1)$ y $\varphi(s_1) = (1, g)$, puesto que este necesariamente será sobreyectivo. □

Capítulo 3

Acciones de grupos

1. Acciones y G-espacios

Una *acción a izquierda* de un grupo G sobre un conjunto X es una función

$$\rho\colon G \times X \to X$$

que satisface:

1. $(gh) \cdot x = g \cdot (h \cdot x)$ para todo $g, h \in G$ y $x \in X$,
2. $1 \cdot x = x$ para todo $x \in X$,

donde, siguiendo una práctica usual, usamos la notación $g \cdot x$ como un sinónimo de $\rho(g, x)$. Un *G-espacio a izquierda* es un conjunto X provisto de una acción a izquierda de G en X. Similarmente, una *acción a derecha* de G sobre X es una función

$$\rho\colon X \times G \to X$$

que satisface:

1. $x \cdot (gh) = (x \cdot g) \cdot h$ para todo $g, h \in G$ y $x \in X$,
2. $x \cdot 1 = x$ para todo $x \in X$,

donde $x \cdot g = \rho(x, g)$, y un *G-espacio a derecha* es un conjunto X provisto de una acción a derecha de G sobre X. Es obvio que $\rho\colon X \times G \to X$ es una acción a derecha de G sobre X si y sólo si la función $\rho^{\mathrm{op}}\colon G^{\mathrm{op}} \times X \to X$, definida por $\rho^{\mathrm{op}}(g, x) := \rho(x, g)$, es una acción a izquierda de G^{op} sobre X. Debido a esto, salvo mención en contrario sólo consideraremos acciones y G-espacios a izquierda (nos referiremos a ellos simplemente como acciones y G-espacios) y dejaremos al lector la tarea de establecer las definiciones y propiedades correspondientes para G-espacios a derecha. Notemos que tener una función $\rho\colon G \times X \to X$ es "lo mismo" que tener una función $\widetilde{\rho}\colon G \to \mathrm{Fun}(X, X)$. Dicho en forma más precisa, la correspondencia

$$\begin{array}{ccc} \mathrm{Fun}(G \times X, X) & \longrightarrow & \mathrm{Fun}(G, \mathrm{Fun}(X, X)) \\ \rho & \longmapsto & \widetilde{\rho} \end{array} ,$$

donde $\widetilde{\rho}$ es la función dada por $\widetilde{\rho}(g)(x) := \rho(g,x)$, es biunívoca. Es claro que las condiciones requeridas a ρ en la definición de acción se satisfacen si y sólo si

$$\widetilde{\rho}(gh) = \widetilde{\rho}(g) \circ \widetilde{\rho}(h) \text{ para todo } g,h \in G \quad \text{y} \quad \widetilde{\rho}(1) = \mathrm{id}\,.$$

En particular

$$\widetilde{\rho}(g^{-1}) \circ \widetilde{\rho}(g) = \widetilde{\rho}(1) = \mathrm{id} \text{ para todo } g,h \in G.$$

Por lo tanto, dar una acción de G sobre X es equivalente a dar un morfismo de G en S_X.

2. Núcleo de una acción, teorema de Cayley y aplicaciones

El *núcleo de una acción* $\rho\colon G \times X \to X$ es el conjunto

$$\ker \rho := \{g \in G : g \cdot x = x \text{ para todo } x \in X\},$$

el cual es un subgrupo normal de G, puesto que coincide con el núcleo del morfismo

$$\widetilde{\rho}\colon G \to \mathrm{S}_X$$

asociado a ρ. Una acción es *fiel* si su núcleo es 1. En este caso el morfismo asociado $\widetilde{\rho}\colon G \to \mathrm{S}_X$ es inyectivo y, por lo tanto, G es isomorfo a un subgrupo de S_X. Para cada acción

$$\rho\colon G \times X \to X$$

la fórmula $[g] \cdot x := g \cdot x$ define una acción fiel $[\rho]$ de $G/\ker\rho$ en X. La definición no depende del representante elegido, porque si $h \in \ker\rho$, entonces

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x \quad \text{para todo } x \in X.$$

Se comprueba fácilmente que el triángulo

$$\begin{array}{ccc} G & \xrightarrow{\ \widetilde{\rho}\ } & \mathrm{S}_X \\ {\scriptstyle\pi}\downarrow & \nearrow_{\widetilde{[\rho]}} & \\ \frac{G}{\ker\rho} & & \end{array},$$

donde π es la proyección al cociente, conmuta. Esto muestra que $\widetilde{[\rho]}$ es el morfismo inducido por $\widetilde{\rho}$ gracias a la propiedad universal del cociente, y da un método alternativo para obtener $[\rho]$, con el cual es innecesario comprobar la buena definición.

Ejemplo 2.1. *Todo grupo G actúa sobre el conjunto G/L, de las coclases a izquierda de un subgrupo L de G, vía traslaciones a izquierda. En otras palabras, $g \cdot (hL) = ghL$. El núcleo de esta acción es el máximo subgrupo $N := \bigcap_{h\in G} hLh^{-1}$ de L, que es normal en G (ver la Subsección 18.6 del Capítulo 1). De ahora en más siempre consideraremos a G/L provisto de esta estructura de G-espacio.*

Teorema 2.2 (Cayley). *La función*

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{S}_G \\ g & \longmapsto & l_g \end{array}$$

es un morfismo inyectivo.

Demostración. Tómese $L = 1$ en el ejemplo anterior. □

COROLARIO 2.3. *Todo grupo finito G es subgrupo de un grupo generado por dos elementos.*

DEMOSTRACIÓN. Por el teorema de Cayley existe $n \in \mathbb{N}$ tal que G es isomorfo a un subgrupo de S_n y, como vimos en la Sección 2 del Capítulo 2, el grupo simétrico S_n está generado por los ciclos $(1,2)$ y $(1,\ldots,n)$. □

COROLARIO 2.4. *Todo grupo finito G es subgrupo de un grupo finito simple.*

DEMOSTRACIÓN. Por el teorema de Cayley y la Observación 3.6 del Capítulo 2, sabemos que G es isomorfo a un subgrupo de A_n, para un $n \geq 5$. Para terminar la demostración basta observar que, por el Teorema 5.5 del Capítulo 2, el grupo alternado A_n es simple. □

Todas las nociones introducidas y los resultados obtenidos al estudiar el grupo simétrico S_n (salvo la noción de descensos de una permutación, que depende en forma escencial del orden de $\mathbb{I}_n$) tienen sentido y valen para los grupos S_X, con X finito. Esto se debe a que o no dependen del orden; o en principio si dependen (como por ejemplo la definición de signo de una permutación), pero tienen caracterizaciones que no; o se vuelven independientes luego de ser reformuladas en una forma más general, aunque equivalente (por ejemplo la propiedad de que $(1,2)$ y $(1,2,\ldots,n)$ generan S_n puede reformularse como sigue: dada una numeración $j_1,\ldots,j_n$ de $\mathbb{I}_n$, los ciclos (j_1,j_2) y $(j_1,j_2,\ldots,j_n)$ generan S_n). Denotamos con A_X al subgrupo de S_X formado por las permutaciones pares. Este comentario es relevante en relación al resultado que sigue.

PROPOSICIÓN 2.5. *Consideremos un grupo G de orden $2^k m$, con m impar. Para cada $g \in G$, la permutación $l_g \in \mathrm{S}_G$ no pertenece a A_G si y sólo si $k > 0$ y 2^k divide a $|g|$.*

DEMOSTRACIÓN. Supongamos que $|g| = 2^{k'} m'$ con $0 \leq k' \leq k$ y m' un divisor positivo de m. Por su misma definición, l_g es un producto de $2^{k-k'} m/m'$ ciclos disjuntos de longitud $2^{k'} m'$. Dado que estos ciclos son permutaciones impares si y sólo si $k' > 0$, y que $2^{k-k'} m/m'$ es impar si y sólo si $k' = k$, el signo de l_g es -1 si y sólo si $k' = k \geq 1$. □

COROLARIO 2.6. *Si $|G| = 2^k m$, con m impar y $k > 0$, y G tiene un elemento g tal que 2^k divide a $|g|$, entonces G tiene un subgrupo de índice 2.*

DEMOSTRACIÓN. Por el teorema de Cayley y la Proposición 2.5, podemos suponer sin pérdida de generalidad que G es un subgrupo de S_G no incluído en A_G. En este caso el resultado se sigue inmediatamente de la Proposición 3.7 del Capítulo 2. □

COROLARIO 2.7. *Si $|G| = 2m$, con m impar, entonces G tiene un subgrupo de índice 2.*

DEMOSTRACIÓN. Por el Corolario 2.6 y por la Observación 6.7 del Capítulo 1 □

COROLARIO 2.8. *Si G es un grupo simple de orden par mayor que 2 y $|G| = 2^k m$ con m impar, entonces $k > 1$ y G no tiene ningún elemento g cuyo orden es múltiplo de 2^k.*

DEMOSTRACIÓN. Por el Corolario 2.6, si G tuviera un elemento cuyo orden es múltiplo de 2^k, entonces tendría un subgrupo de índice 2 y, por lo tanto, normal. Como $|G| > 2$ dicho subgrupo no sería trivial, lo que contradeciría la hipótesis de que G es simple. Por la Observación 6.7 del Capítulo 1, necesariamente $k > 1$. □

Volvamos a la situación considerada en el Ejemplo 2.1. Supongamos que L tiene índice finito. Recordemos que el morfismo

$$\begin{array}{l} G \longrightarrow \mathrm{S}_{G/L} \\ g \longmapsto l_g \end{array},$$

asociado a la acción de G sobre G/L vía traslaciones a izquierda, induce un morfismo inyectivo de G/N en $\mathrm{S}_{G/L}$, donde $N := \bigcap_{g\in G} gLg^{-1}$ es me máximo subgrupo normal de G contenido en L. Por consiguiente el índice de N en G es menor que infinito y divide a $|\,\mathrm{S}_{G/L}\,| = |G : L|!$. Como además $|G : L|$ divide a $|G : N|$, vale el siguiente resultado:

TEOREMA 2.9. *Si L es un subgrupo de índice $n < \infty$ de un grupo G, entonces el índice del máximo subgrupo normal $N := \bigcap_{g\in G} gLg^{-1}$, de G contenido en L, es nh, donde h es un divisor de $(n-1)!$. Además, N es el núcleo del morfismo de G en $\mathrm{S}_{G/L}$ que manda g en l_g.*

El Teorema 2.9 generaliza al teorema de Cayley y refina a la Observación 18.22 del Capítulo 1. También generaliza la Proposición 10.7 del Capítulo 1, porque si $n = 2$, entonces $h = 1$ y $N = L$.

COROLARIO 2.10. *Si un grupo G tiene un subgrupo de índice finito $n > 1$ que no contiene a ningún subgrupo normal de G distinto de 1, entonces $|G| = nh$ con h un divisor de $(n-1)!$. Además hay un morfismo inyectivo de G en S_n.*

DEMOSTRACIÓN. Porque debido a la hipótesis el subgrupo normal N de G mencionado en el Teorema 2.9 necesariamente es 1. □

COROLARIO 2.11. *Si un grupo simple G tiene un subgrupo de índice finito $n > 1$, entonces $|G| = nh$ con h un divisor de $(n-1)!$. Además hay un morfismo inyectivo de G en S_n.*

DEMOSTRACIÓN. Se sigue inmediatamente del corolario anterior. □

Notemos que, debido a la Proposición 3.7 del Capítulo 2, si $n > 2$, entonces la imagen del morfismo inyectivo de G en S_n, mencionado en el corolario anterior, está incluída en A_n.

COROLARIO 2.12. *Los grupos infinitos simples no tienen subgrupos propios de índice finito.*

COROLARIO 2.13. *Supongamos que G es un grupo finito de orden nm y que L es un subgrupo de orden m de G. Entonces el índice del máximo subgrupo normal $N := \bigcap_{g\in G} gLg^{-1}$, de G contenido en L, es nh, donde h es un divisor de $((n-1)! : m)$. Además, N es el núcleo del morfismo de G en $\mathrm{S}_{G/L}$ que manda g en l_g.*

DEMOSTRACIÓN. Por el Teorema 2.9, sabemos que el índice de N en G es nh, con h un divisor de $(n-1)!$. Como $|G : N|$ divide a $|G|$, también m es divisible por h. □

COROLARIO 2.14. *Supongamos que G es un grupo finito y que $|G| = nm$. Si todos los primos que dividen a m son mayores que el máximo primo menor que n, entonces todo subgrupo de índice n de G es normal.*

DEMOSTRACIÓN. Por el Corolario 2.13, sabemos que cada subgrupo L de índice n de G contiene un subgrupo normal N cuyo índice en G es nh, con h un divisor de $((n-1)! : m)$. Para terminar la demostración debemos ver que si ningún primo menor que n divide a m, entonces $((n-1)! : m) = 1$, lo que es evidente. □

COROLARIO 2.15. *Si G es un grupo finito y p es el mínimo primo que divide a $|G|$, entonces todo subgrupo de índice p de G es normal.*

EJERCICIO 2.16. *Pruebe que si $n \neq 4$, entonces S_n no tiene subgrupos de índice t con $2 < t < n$. Pruebe también que esto es falso si $n = 4$.*

EJEMPLO 2.17. *Recordemos que el grupo diedral D_n tiene orden $2n$ y está generado por dos elementos x e y sujetos las relaciones $x^n = y^2 = yxy^{-1}x = 1$. Supongamos que $n > 2$. Como $\langle y\rangle$ tiene orden 2 y (en este caso) no es normal en D_n, la acción de D_n en $D_n/\langle y\rangle$ definida via traslaciones a izquierda es fiel. Por lo tanto hay un morfismo inyectivo de D_n en S_n (lo que ya fue obtenido en el Ejemplo 1.6 del Capítulo 2).*

3. Subconjuntos estables y morfismos

Decimos que un subconjunto Y de un G-espacio X es *estable bajo la acción de G* o simplemente *estable* si $g \cdot y \in Y$ para todo $g \in G$ e $y \in Y$. En este caso Y en si mismo es un G-espacio con la acción inducida y, debido a eso, decimos también que Y es un *G-subespacio* de X.

Un morfismo $\varphi\colon X \to X'$, de un G-espacio X en otro X', es una terna (X, φ, X'), donde φ es una función de X en X' que satisface

$$\varphi(g \cdot x) = g \cdot \varphi(x) \quad \text{para todo } g \in G \text{ y } x \in X.$$

En términos de los morfismos $\widetilde{\rho}\colon G \to S_X$ y $\widetilde{\rho'}\colon G \to S_{X'}$ inducidos por las acciones de G sobre X y X' respectivamente, esta condición queda

$$\varphi \circ \widetilde{\rho}(g) = \widetilde{\rho'}(g) \circ \varphi \quad \text{para todo } g \in G.$$

Por ejemplo, la identidad $\mathrm{id}\colon X \to X$ y, más generalmente, la inclusión canónica $i\colon Y \to X$, de un subconjunto estable Y de un G-espacio X en X, es un morfismo de G-espacios. También lo es la composición $\psi\circ\varphi\colon X \to X''$ de dos morfismos de G-espacios $\varphi\colon X \to X'$ y $\psi\colon X' \to X''$.

Las definiciones de endomorfismo, isomorfismo, G-espacios isomorfos, automorfismo, monomorfismo, epimorfismo, sección y retracción son las idénticas a las dadas para monoides y grupos, y las propiedades básicas son las mismas. Los monomorfismos, epimorfismos, secciones y retracciones son cerrados bajo la composición, toda retracción es sobreyectiva, toda es sección inyectiva, todo morfismo inyectivo es un monomorfismo, y todo morfismo sobreyectivo es un epimorfismo. Un morfismo $\varphi\colon X \to X'$ es un isomorfismo si y sólo si es biyectivo.

Dados G-espacios X y X', designaremos con los símbolos $\mathrm{Hom}_G(X, X')$, $\mathrm{Iso}_G(X, X')$, $\mathrm{End}_G(X)$ y $\mathrm{Aut}_G(X)$ a los conjuntos de morfismos de X en X', isomorfismos de X en X', endomorfismos de X y automorfismos de X, respectivamente. Tal como en el caso de monoides y grupos, $\mathrm{End}_G(X)$ es un monoide (cuyo elemento neutro es la función identidad) vía la composición y $\mathrm{Aut}_G(X)$ es su grupo de unidades.

OBSERVACIÓN 3.1. *Si X es un G-espacio y $\sigma\colon X \to X'$ es una función biyectiva, entonces hay una única acción de G sobre X' que convierte a σ en un isomorfismo de G-espacios. En efecto, si este es el caso, entonces*

$$g \cdot x' = \sigma\big(\sigma^{-1}(g \cdot x')\big) = \sigma\big(g \cdot \sigma^{-1}(x')\big)$$

y es fácil ver que esta iguldad define una tal acción de G sobre X', que diremos es obtenida a partir de la acción de G sobre X' por traslación de estructura.

4. Más ejemplos

Hasta ahora hemos visto un sólo ejemplo de acción de un grupo sobre un conjunto, el dado por la acción, vía traslaciones a izquierda, de un grupo G sobre el conjunto G/L, de las

coclases a izquierda de un subgrupo L. El objetivo de esta breve subsección es proveernos de muchos otros.

EJEMPLO 4.1. *Cada conjunto X es un G-espacio vía la* acción trivial $g \cdot x := x$.

EJEMPLO 4.2. *G actúa sobre si mismo por conjugación. Esto es, $g \cdot h := ghg^{-1}$. Más generalmente, G actúa por conjugación sobre cada uno de sus subgrupos normales N. El núcleo de esta acción es $\mathrm{C}_G(N)$.*

EJEMPLO 4.3. *Si N y K son subgrupos de un grupo G y $K \subseteq \mathrm{N}_G(N)$, entonces K actúa sobre N por conjugación. El núcleo de esta acción es $K \cap \mathrm{C}_G(N)$. Cuando $K = G$ nos reducimos al Ejemplo 4.2.*

EJEMPLO 4.4. *Todo subgrupo H de un grupo G actúa fielmente sobre G por traslaciones a izquierda. En símbolos, $h \cdot g := hg$ para todo $h \in H$ y $g \in G$. Más generalmente el subgrupo H actúa sobre G/L para cada subgrupo L de G vía $h \cdot gL := hgL$. El núcleo de esta acción es $H \cap \bigcap_{g \in G} gLg^{-1}$.*

EJEMPLO 4.5. *G actúa sobre el conjunto $\mathrm{P}(G)$, de partes de G, por conjugación. Esto es, $g \cdot S := gSg^{-1}$. El núcleo de esta acción es $\mathrm{Z}\,G$.*

EJEMPLO 4.6. *El subconjunto $\mathrm{Sub}(G)$ de $\mathrm{P}(G)$ de los subgrupos de G es estable por la acción del ejemplo anterior y, así, G también actúa sobre $\mathrm{Sub}(G)$ por conjugación. El núcleo de esta acción es $\bigcap_{H \in \mathrm{Sub}(G)} \mathrm{N}_G(H)$.*

EJEMPLO 4.7. *La clase de conjugación de un subgrupo L de G es un G-espacio via*

$$g \cdot hLh^{-1} := ghLh^{-1}g^{-1}.$$

El núcleo de esta acción es $\bigcap_{h \in G} \mathrm{N}_G(hLh^{-1})$.

EJEMPLO 4.8. *G actúa fielmente sobre $\mathrm{P}(G)$ vía $g \cdot S := gS$. Esto es, por traslaciones a izquierda.*

EJEMPLO 4.9. *G actúa sobre el conjunto $G\backslash L$ de las coclases a derecha de un subgrupo L de G vía $g \cdot (Lh) := Lhg^{-1}$. El núcleo de esta acción es $\bigcap_{h \in G} hLh^{-1}$.*

EJEMPLO 4.10. *S_n actúa fielmente sobre el anillo $k[X_1, \ldots, X_n]$ de polinomios en n variables con coeficientes en un cuerpo k, via*

$$\sigma \cdot P(X_1, \ldots, X_n) := P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

EJEMPLO 4.11. *S_n actua sobre el producto cartesiano $X \times \cdots \times X$ de n copias de un conjunto arbitrario X, via*

$$\sigma \cdot (x_1, \ldots, x_n) := \big(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}\big).$$

EJEMPLO 4.12. *Cada subgrupo G de $\mathrm{GL}(V)$ actúa fielmente sobre V vía $g \cdot v := g(v)$. Esta es la* acción natural de G sobre V.

EJEMPLO 4.13. *El grupo ortogonal $O(\mathbb{R}^n)$ actúa fielmente sobre la esfera*

$$S^{n-1} := \{x \in \mathbb{R}^n : \|x\| = 1\},$$

via $g \cdot x := g(x)$.

EJEMPLO 4.14. *La* acción natural de S_X sobre X *es la definida por $\sigma \cdot x := \sigma(x)$.*

EJEMPLO 4.15. *Para cada par de grupos G y N hay una acción de G en $\mathrm{Hom}(N, G)$, que está dada por $(g \cdot f)(n) := gf(n)g^{-1}$, para todo $g \in G$, $f \in \mathrm{Hom}(N, G)$ y $n \in N$.*

5. Órbitas, puntos fijos y estabilizadores

Dos elementos x e y de un G-espacio X son *conjugados* si existe $g \in G$ tal que $g \cdot x = y$. Se comprueba fácilmente que la relación $\sim$, definida por $x \sim y$ si x e y son conjugados, es de equivalencia. Por consiguiente determina una partición de X en clases llamadas *clases de conjugación* u *órbitas*. Denotamos con $\mathcal{O}_x$ a la órbita que contiene a x y con $\mathcal{O}X$ o X/G al conjunto de todas las órbitas de X. Por definición

$$\mathcal{O}_x = \{g \cdot x : g \in G\}$$

y $\mathcal{O}_x = \mathcal{O}_y$ si y sólo si x e y son conjugados. Es evidente que si consideramos a X/G provisto de la acción trivial de G, entonces la aplicación canónica $\pi\colon X \to X/G$, definida por $\pi(x) := \mathcal{O}_x$, es un morfismo de G-espacios. Además para cada G-morfismo $f\colon X \to Y$, de X en un conjunto Y provisto de la acción trivial de G, existe un único G-morfismo $\overline{f}\colon X/G \to Y$ tal que $f = \overline{f}\circ\pi$.

Para cada subconjunto H de G denotamos con X^H al conjunto de los puntos de X que son dejados fijos por H. En símbolos

$$X^H := \{x \in X : h \cdot x = x \text{ para todo } h \in H\}.$$

Decimos que $x \in X$ es un *punto fijo* si $g \cdot x = x$ para todo $g \in G$, es decir si $x \in X^G$ o, equivalentemente, si $\mathcal{O}_x = \{x\}$. Claramente un subconjunto de X es un G-subespacio si y sólo si es una unión de órbitas. Supongamos que X' es un conjunto de representantes de las clases de conjugación de X. Es decir, que para cada $x \in X$ la intesección $X' \cap \mathcal{O}_x$ tiene exactamente un elemento. Notemos que X^G, está incluído en X'. Es obvio que

$$|X| = \sum_{x \in X'} |\mathcal{O}_x| = |X^G| + \sum_{x \in X' \setminus X^G} |\mathcal{O}_x|. \tag{29}$$

Decimos que la acción de un grupo G sobre un conjunto X es *transitiva* o que G *opera transitivamente* sobre X si tiene una sóla órbita. Por ejemplo la acción de un grupo G sobre el conjunto G/L de las coclases a izquierda de uno de sus subgrupos L, dada por traslaciones a izquierda, es transitiva. El *estabilizador* o *grupo de isotropía* de un elemento x de X es el conjunto

$$G_x := \{g \in G : g \cdot x = x\}.$$

Es evidente que G_x es un subgrupo de G, que $x \in X^G$ si y sólo si $G_x = G$, y que el núcleo de la acción de G sobre X es la intersección de los estabilizadores de todos los elementos de X.

Ejercicio 5.1. *Pruebe que si G es un grupo abeliano que actúa transitivamente sobre un conjunto X, entonces para cada $x, y \in X$ existe un único $g \in G$ tal que $g \cdot x = y$.*

A continuación calculamos los estabilizadores en algunos de los ejemplos introducidos en la subsección anterior.

Ejemplo 5.2. *Para el caso de la acción de un grupo G sobre el conjunto G/L de las coclases a izquierda de uno de sus subgrupos L dada por traslaciones a izquierda, el estabilizador de cada hL es hLh^{-1}. Esta acción no tiene puntos fijos a menos que L sea G.*

Ejemplo 5.3. *Para el caso de la acción de un grupo G sobre uno de sus subgrupos normales N dada por conjugación, el estabilizador de cada $n \in N$ es $\mathrm{C}_G(n)$. Más generalmente si N y K son subgrupos de G tales que $K \subseteq \mathrm{N}_G(N)$ y K actúa sobre N por conjugación, entonces el estabilizador de cada $n \in N$ es $K \cap \mathrm{C}_G(n)$.*

Ejemplo 5.4. *En el caso de la acción de un grupo G sobre $P(G)$ dada por conjugación, el estabilizador de cada subconjunto S de G es $\mathrm{N}_G(S)$. Un subconjunto S de G es un punto fijo para esta acción si y sólo si $gSg^{-1} = S$ para todo $g \in G$.*

Proposición 5.5. *Si $y = g \cdot x$, entonces $G_y = gG_xg^{-1}$. En particular, si G_x es un subgrupo normal de G, entonces $G_y = G_x$.*

Demostración. Como

$$h \cdot y = y \Leftrightarrow hg \cdot x = g \cdot x \Leftrightarrow g^{-1}hg \cdot x = x,$$

un elemento h de G pertenece a G_y si y sólo si pertenece a gG_xg^{-1}. □

Corolario 5.6. *Si x e y están en la misma órbita, entonces sus estabilizadores son isomorfos.*

Observación 5.7. *Supongamos que X es un G-espacio y tomemos $x \in X$. Por la Proposición 5.5, para cada H conjugado a G_x existe $y \in \mathcal{O}_x$ tal que $G_y = H$. Así, debido a los comentarios que preceden a la Observación 18.22 del Capítulo 1, el grupo $N := \bigcap_{y \in \mathcal{O}_x} G_y$ es el máximo subgrupo normal de G_x.*

Proposición 5.8. *Si $f\colon X \to Y$ es un morfismo de G-espacios, entonces $G_x \subseteq G_{f(x)}$ para todo $x \in X$. Además si f es inyectivo, entonces elementos de órbitas distintas de X van a parar a órbitas distintas de Y y $G_x = G_{f(x)}$ para todo $x \in X$.*

Demostración. Si $g \in G_x$, entonces

$$g \cdot f(x) = f(g \cdot x) = f(x)$$

y, así, $g \in G_{f(x)}$. Supongamos ahora que f es inyectiva y que $f(x)$ y $f(x')$ estan en la misma órbita. Entonces existe $g \in G$ tal que $g \cdot f(x) = f(x')$ y, de la igualdad

$$f(g \cdot x) = g \cdot f(x) = f(x'),$$

se sigue que $g \cdot x = x'$. Por último si f es inyectiva y $g \in G_{f(x)}$, entonces de la igualdad

$$f(g \cdot x) = g \cdot f(x) = f(x),$$

obtenemos inmediatamente que $g \in G_x$. □

Teorema 5.9. *Consideremos dos G-espacios X e Y, un subconjunto X' de representantes de las clases de conjugación de X y una familia $(y_x)_{x \in X'}$ de elementos de Y. Son equivalentes:*

1. *Hay un único morfismo de G-espacios $\Phi\colon X \to Y$, tal que $\Phi(x) = y_x$ para todo $x \in X'$.*
2. *Hay un morfismo de G-espacios $\Phi\colon X \to Y$, tal que $\Phi(x) = y_x$ para todo $x \in X'$.*
3. *$G_x \subseteq G_{y_x}$ para todo $x \in X'$.*

Además Φ es inyectivo si y sólo si todos los y_x's están en órbitas distintas y $G_x = G_{y_x}$ para todo $x \in X'$.

Demostración. Es evidente que 1) implica 2) y debido a la proposición anterior también que 2) implica 3) y que se satisface la parte "sólo si" de la afirmación adicional. Veamos que 3) implica 1). Notemos que si Φ existe, entonces

$$\Phi(g \cdot x) = g \cdot y_x \quad \text{para todo } x \in X',$$

y, por lo tanto, es único. Para terminar la demostración, sólo debemos ver que esta definición de Φ es correcta y que da un morfismo de G-espacios. Lo primero se sigue inmediatamente de que, para todo $x \in X'$,

$$g \cdot x = g' \cdot x \Longrightarrow \text{existe } h \in G_x \text{ tal que } g' = gh \Longrightarrow g' \cdot y_x = g \cdot (h \cdot y_x) = g \cdot y_x,$$

mientras que lo último vale pues, para todo $x \in X$ y $g, g' \in G$,

$$\Phi(g' \cdot (g \cdot x)) = \Phi(g'g \cdot x) = g'g \cdot y_x = g' \cdot (g \cdot y_x) = g' \cdot \Phi(g \cdot x).$$

Resta probar que si todos los y_x's están en órbitas distintas y $G_x = G_{y_x}$ para todo $x \in X'$, entonces $\Phi\colon X \to Y$ es inyectiva. Para ello tomemos $z, z' \in X$ tales que $\Phi(z) = \Phi(z')$ y escribamos $z = g \cdot x$ y $z' = g' \cdot x'$ con $x, x' \in X'$ y $g, g' \in G$. Como $\Phi(z)$ y $\Phi(z')$ están en las órbitas de y_x y de $y_{x'}$ respectivamente, de la igualdad $\Phi(z) = \Phi(z')$ se sigue que $x = x'$. Por lo tanto

$$g \cdot y_x = \Phi(z) = \Phi(z') = g' \cdot y_{x'} = g' \cdot y_x$$

de donde existe $h \in G_{y_x}$ tal que $g' = gh$. Pero entonces

$$z' = g' \cdot x' = gh \cdot x' = gh \cdot x = g \cdot x = z,$$

pues, debido a la hipótesis, $h \in G_x$. □

Observación 5.10. *Un morfismo de G-espacios $f\colon X \to Y$ es* isovariante *si $G_x = G_{f(x)}$ para todo $x \in X$. Debido a la Proposición 5.8 y al Teorema 5.9 son equivalentes:*

1. *$f\colon X \to Y$ es isovariante.*
2. *La restricción de f a cada órbita de X es inyectiva.*
3. *Existe un conjunto de representantes X' de las clases de conjugación de X tal que*

$$G_x = G_{f(x)} \qquad \text{para todo } x \in X'.$$

Observación 5.11. *Consideremos un G-espacio X. Del Teorema 5.9 se sigue inmediatamente que hay una correpondencia biyectiva entre X^H y el conjunto de los morfismos de G-espacios de G/H en X, que a cada $x \in X^H$ le asigna el único morfismo $f\colon G/H \to X$ tal que $f(H) = x$. Notemos además que f es inyectivo si y sólo si $G_x = H$.*

Ejemplo 5.12. *Como*

$$(G/H)^H = \{lH : H \subseteq lHl^{-1}\}$$

hay un morfismo de G-espacios $f\colon G/H \to G/H$ tal que $f(H) = lH$ si y sólo si $H \subseteq lHl^{-1}$. Además este morfimo es inyectivo si y sólo si $H = lHl^{-1}$. Notemos que si H es finito esto es trivial y así, en este caso, $(G/H)^H = \mathrm{N}_G(H)/H$.

Corolario 5.13. *Para cada G-espacio X y cada $x \in X$, hay un isomorfismo de G-espacios $\Phi\colon G/G_x \to \mathcal{O}_x$, tal que $\Phi(gG_x) = g \cdot x$ para cada $g \in G$. En consecuencia $|\mathcal{O}_x| = |G : G_x|$ para cada $x \in X$.*

Por ejemplo para cada elemento h de G y cada subgrupo H de G,

$$|G : \mathrm{C}_G(h)| = |\{ghg^{-1} : g \in G\}| \qquad \text{y} \qquad |G : \mathrm{N}_G(H)| = |\{gHg^{-1} : g \in G\}|.$$

Como aplicación del corolario anterior obtenemos la siguiente

Proposición 5.14. *Si k es un cuerpo finito con q elementos, entonces*

$$|\operatorname{GL}(n,k)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) = q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1).$$

DEMOSTRACIÓN. Procedemos por inducción en n. Es claro que $\mathrm{GL}(1,k) = k^*$ tiene $q-1$ elementos. Supongamos que el resultado vale para n. Designemos con el símbolo ${}^t k^{n+1}$ al espacio de los vectores columna de $n+1$ coordenadas y con e_1 al primer elemento de la base canónica de ${}^t k^{n+1}$. Como la acción natural de $\mathrm{GL}(n+1,k)$ sobre ${}^t k^{n+1} \setminus \{0\}$ es transitiva, por el Corolario 5.13,

$$q^{n+1} - 1 = |k^{n+1} \setminus \{0\}| = \frac{|\mathrm{GL}(n+1,k)|}{|\mathrm{GL}(n+1,k)_{e_1}|}.$$

Es fácil ver que $\mathrm{GL}(n+1,k)_{e_1}$ es el conjunto de las matrices cuya primera columna es e_1 y, usando esto, que $|\mathrm{GL}(n+1,k)_{e_1}| = q^n |\mathrm{GL}(n,k)|$. Así, por hipótesis inductiva

$$|\mathrm{GL}(n+1,k)| = (q^{n+1}-1)q^n |\mathrm{GL}(n,k)| = (q^{n+1}-1)(q^{n+1}-q)\cdots(q^{n+1}-q^n),$$

como queríamos. □

Veamos otra aplicación del Corolario 5.13.

OBSERVACIÓN 5.15. *Fijemos un elemento h de un grupo G. Es obvio que $\langle h\rangle \subseteq \mathrm{C}_G(h)$. Además, por el Corolario 5.13 y el teorema de Lagrange,*

$$|G| = |\{ghg^{-1} : g \in G\}|\,|\mathrm{C}_G(h)|.$$

Por ejemplo, esta fórmula combinada con la (27) *debida a Cauchy, nos dice que*

$$|\mathrm{C}_{\mathrm{S}_n}(\sigma)| = 1^{\alpha_1}\alpha_1! 2^{\alpha_2}\alpha_2! \cdots n^{\alpha_n}\alpha_n! \quad \textit{para cada permutación } \sigma, \tag{30}$$

donde $[\alpha_1, \ldots, \alpha_n]$ es la estructura cíclica de σ. Comparando el orden de σ (que es el mínimo múltiplo común de los órdenes de los ciclos que aparecen en su descomposición cíclica) con (30)*, concluímos que $\mathrm{C}_{\mathrm{S}_n}(\sigma) = \langle\sigma\rangle$ si y sólo si los órdenes de sus ciclos son coprimos dos a dos (en particular, son todos distintos).*

EJERCICIO 5.16. *Supongamos que G es un grupo simple infinito. Pruebe que:*

1. *Si $g \in G$ es distinto de 1, entonces la clase de conjugación de g es un conjunto infinito.*
2. *Si H es un subgrupo no trivial de G, entonces la clase de conjugación de H es un conjunto infinito.*

Por último damos dos aplicaciones del Corolario 5.13 que son algo más teóricas que las anteriores.

PROPOSICIÓN 5.17. *Si un subgrupo de un grupo finito G contiene algún elemento de cada clase de conjugación de G, entonces coincide con G.*

DEMOSTRACIÓN. Tomemos un subgrupo propio L de G y consideremos la acción de G sobre $\mathrm{Sub}(G)$ dada por conjugación. Dado que por el Corolario 5.13

$$\left|\bigcup gLg^{-1}\right| \leq |G : \mathrm{N}_G(L)|(|L|-1)+1 \leq |G:L|(|L|-1)+1 = |G| - |G:L| + 1,$$

existe $h \in G$ tal que $h \notin gLg^{-1}$ para ningún $g \in G$ o, lo que es claramente equivalente, que L no corta a la clase de conjugación de h. □

Por supuesto que en general el teorema de Cayley no es óptimo. Vamos a ver un caso en el que si lo es. Un subgrupo H de un grupo G es minimal si $H \neq 0$ y $L \leq H$ implica $L = 1$ o $L = H$. Es claro que no todo grupo no trivial tiene subgrupos minimales. Por ejemplo $\mathbb{Z}$ no los tiene. Sin embargo es muy fácil ver que todo grupo finito y no trivial contiene subgrupos

minimales. Por último es claro también que si H es un subgrupo minimal de G y $\varphi\colon G \to G$ es un automorfismo, entonces $\varphi(H)$ también es un subgrupo minimal de G. En particular si un grupo tiene un único subgrupo minimal, este necesariamente es característico.

PROPOSICIÓN 5.18. *Si G es un grupo finito que tiene un único subgrupo minimal y X es un G-espacio fiel, entonces $|X| \geq |G|$.*

DEMOSTRACIÓN. Denotemos con H al único subgrupo minimal de G. Afirmamos que existe $x \in X$ tal que $G_x = 1$. En efecto, en caso contrario $H \subseteq G_x$ para todo $x \in X$, lo que se contradice con que el núcleo $\bigcap_{x\in X} G_x$, de la acción de G sobre X que estamos considerando es 1. En consecuencia $|X| \geq |\mathcal{O}_x| = |G|$. □

Notemos que el grupo cuaterniónico H_{2^m} satisface la hipótesis del teorema anterior. Otro ejemplo es $\mathbb{Z}_{p^r}$, donde $p, r \in \mathbb{N}$ y p es primo. En consecuencia si S_n tiene un subgrupo isomorfo a H_{2^m}, entonces $n \geq 2^{m+2}$ y si S_n tiene un subgrupo isomorfo a $\mathbb{Z}_{p^r}$, entonces $n \geq p^r$. Dado que D_{p^r} contiene a un subgrupo isomorfo a $\mathbb{Z}_{p^r}$, se sigue de esto que si S_n tiene un subgrupo isomorfo a D_{p^r}, entonces $n \geq p^r$.

Terminamos esta subsección mostrando que, para cada grupo G, el conjunto de clases de isomorfía de la clase de los G-espacios de n elementos, está en correspondencia con las órbitas de la acción S_n sobre $\mathrm{Hom}(G, \mathrm{S}_n)$ definida en el Ejemplo 4.15.

OBSERVACIÓN 5.19. *Tomemos un grupo G y consideremos a $\mathrm{Hom}(G, \mathrm{S}_n)$ provisto de la acción de S_n obtenida en el Ejemplo 4.15. Para cada $f \in \mathrm{Hom}(G, \mathrm{S}_n)$ denotemos con $\mathbb{I}_n^f$ al conjunto $\mathbb{I}_n$ provisto de la acción de G determinada por f (es decir que $g \cdot i := f(g)(i)$ para cada $g \in G$ e $i \in \mathbb{I}_n$). Tomemos $\sigma \in \mathrm{S}_n$. Como*

$$\sigma \circ f(g) = (\sigma \cdot f)(g) \circ \sigma \quad \text{para todo } g \in G,$$

la función $\sigma\colon \mathbb{I}_n^f \to \mathbb{I}_n^{\sigma\cdot f}$ es un isomorfismo de G-espacios. En consecuencia queda definida una aplicación del conjunto de las órbitas de $\mathrm{Hom}(G, \mathrm{S}_n)$ en el conjunto de las clases de isomorfía de G-espacios de n elementos, que a la órbita que contiene a f le asigna la clase que contiene a $\mathbb{I}_n^f$. Esta aplicación es inyectiva pues si $\sigma\colon \mathbb{I}_n^f \to \mathbb{I}_n^{f'}$ es un isomorfismo de G-espacios, entonces

$$\sigma \circ f(g) = f'(g) \circ \sigma \quad \text{para todo } g \in G$$

y así, $f' = \sigma \cdot f$. Pero también es sobreyectiva pues si X es un G-espacio de n elementos, entonces tomando una biyección $\sigma\colon X \to \mathbb{I}_n$, obtenemos por traslación de estructura, una acción de G sobre $\mathbb{I}_n$ que convierte a σ en un isomorfismo de G-espacios.

5.1. La ecuación de las clases

Combinando el Corolario 5.13 con la fórmula (29), obtenemos que

$$|X| = |X^G| + \sum_{x \in X' \setminus X^G} |G : G_x|, \tag{31}$$

donde X' es un conjunto de representantes de las órbitas de X. Una observación que será útil más adelante es que cuando G es finito, los cardinales $|G : G_x|$, que aparecen en esta fórmula, dividen propiamente a $|G|$. Veamos ahora que nos dice este resultado en alguno de los ejemplos introducidos arriba.

Acción de G sobre si mismo por conjugación: En este caso la fórmula (31) da la llamada *ecuación de las clases*

$$|G| = |\operatorname{Z} G| + \sum_{g \in X' \setminus \operatorname{Z} G} |G : \operatorname{C}_G(g)|,$$

en la cual X' es un conjunto de representantes de las clases de conjugación de G.

Acción de G sobre un subgrupo normal N por conjugación: En este se reduce a la igualdad

$$|N| = |N \cap \operatorname{Z} G| + \sum_{g \in X' \setminus \operatorname{Z} G} |G : \operatorname{C}_G(g)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de G incluídas en N.

Acción de G sobre Sub(G) por conjugación: Dado que en este caso $\operatorname{Sub}(G)^G$ es el subconjunto $\operatorname{SubN}(G)$ de $\operatorname{Sub}(G)$ formado por los subgrupos normales de G y que $G_H = \operatorname{N}_G(H)$ para todo subgrupo H de G, la fórmula (31) deviene

$$|\operatorname{Sub}(G)| = |\operatorname{SubN}(G)| + \sum_{H \in X' \setminus \operatorname{SubN}(G)} |G : \operatorname{N}_G(H)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de $\operatorname{Sub}(G)$.

Acción de G sobre P(G) por conjugación: En este caso la fórmula (31) se transforma en

$$2^{|G|} = |\operatorname{PaN}(G)| + \sum_{S \in X' \setminus \operatorname{PaN}(G)} |G : \operatorname{N}_G(S)|,$$

donde X' es un conjunto de representantes de las órbitas de $\operatorname{P}(G)$ y $\operatorname{PaN}(G)$ es el conjunto de los subconjuntos S de G tales que $gSg^{-1} = S$ para todo $g \in G$.

A continuación usamos la ecuación de las clases para probar que para ningún $n \in \mathbb{N}$ hay una cantidad infinita de grupos finitos no isomorfos dos a dos, con exáctamente n clases de conjugación.

LEMA 5.20. *Fijemos $n \in \mathbb{N}$ y $q \in \mathbb{Q}$. Existe sólo una cantidad finita de n-uplas $(i_1, \ldots, i_n)$ de números naturales, tales que $q = \sum_{j=1}^{n} 1/i_j$.*

DEMOSTRACIÓN. Procedemos por inducción en n. El caso $n = 1$ es trivial. Supongamos que el lema es cierto para uplas de longitud $n-1$. Para probar que lo es para uplas de longitud n es suficiente ver que hay sólo un número finito de n-uplas $(i_1, \ldots, i_n)$ de números naturales tales que $i_1 \leq \cdots \leq i_n$ y $q = \sum_{j=1}^{n} 1/i_j$. Pero esto es cierto, porque en cada una de estas n-uplas $i_1 \leq n/q$ y, por la hipótesis inductiva, para cada número natural $k \leq n/q$ sólo hay una cantidad finita de $(n-1)$-uplas $(i_2, \ldots, i_n)$ que satisfacen $q - 1/k = \sum_{j=2}^{n} 1/i_j$. □

TEOREMA 5.21. *Para cada $n \geq 1$, sólo hay una cantidad finita de grupos finitos, no isomorfos dos a dos, que tienen exáctamente n clases de conjugación.*

DEMOSTRACIÓN. Si G es un grupo finito con n clases de conjugación, entonces la ecuación de las clases nos dice que

$$|G| = \sum_{j=1}^{n} |G : C_G(g_j)|,$$

donde $\{g_1, \ldots, g_n\}$ es un conjunto de representantes de las clases de conjugación de G. Por consiguiente

$$1 = \sum_{j=1}^{n} \frac{1}{|C_G(g_j)|}.$$

Por una parte, el máximo valor que toman los números $|C_G(g_j)|$ es $|G|$, y ocurre cuando $g \in \mathrm{Z}\, G$. Por otra parte, por el Lema 5.20, dicho valor está acotado por un $M > 0$. En consecuencia $|G| \leq M$, y para concluir la demostración basta notar que sólo hay finitos grupos no isomorfos de orden menor o igual que M. □

5.2. k-transitividad

Consideremos un G-espacio X y un entero positivo k. Decimos que la acción de G sobre X es *k-transitiva* o que *G opera k-transitivamente* sobre X, si para cada par $\{x_1, \ldots, x_k\}$ e $\{y_1, \ldots, y_k\}$ de subconjuntos de k elementos de X, existe $g \in G$ tal que $g \cdot x_1 = y_1, \ldots, g \cdot x_k = y_k$.

Ejemplo 5.22. *La acción natural de S_n sobre $\mathbb{I}_n$ es n-transitiva. Afirmamos que la acción de A_n sobre $\mathbb{I}_n$ inducida por ella es $n-2$ transitiva. En efecto, para cada par $\{x_1, \ldots, x_{n-2}\}$ e $\{y_1, \ldots, y_{n-2}\}$ de subconjuntos de $n-2$ elementos de $\mathbb{I}_n$, existe $\sigma \in \mathrm{S}_n$ tal que $\sigma(x_i) = y_i$ para todo i. Si $\sigma \in \mathrm{A}_n$ ya está. Si no, tomando $z_1, z_2 \in X \setminus \{y_1, \ldots, y_{n-2}\}$ y considerando $\sigma' := (z_1, z_2) \circ \sigma$ obtenemos una permutación par σ' que también satisface $\sigma'(x_i) = y_i$.*

Proposición 5.23. *Supongamos que $k \geq 2$ y que X es un G-espacio. Son equivalentes:*

1. *G opera k-transitivamente sobre X.*
2. *G opera transitivamente sobre X y la acción de G_x sobre $X \setminus \{x\}$ es $(k-1)$-transitiva, para cada $x \in X$.*

Demostración. 1) ⇒ 2) Es evidente que G opera transitivamente sobre X. Tomemos $x \in X$. Por hipótesis, para cada par $\{x_1, \ldots, x_{k-1}\}$ e $\{y_1, \ldots, y_{k-1}\}$ de subconjuntos de $k-1$ elementos de $X \setminus \{x\}$, existe $g \in G$ tal que $g \cdot x = x$ y $g \cdot x_1 = y_1, \ldots, g \cdot x_{k-1} = y_{k-1}$. Esto muestra que G_x opera $(k-1)$-transitivamente sobre $X \setminus \{x\}$.

2) ⇒ 1) Tomemos subconjuntos $\{x_1, \ldots, x_k\}$ e $\{y_1, \ldots, y_k\}$ de k elementos de X. Como G opera transitivamente sobre X y G_{x_1} opera $(k-1)$-transitivamente sobre $X \setminus \{x_1\}$ existen $g \in G$ y $h \in G_{x_1}$ tales que $g \cdot y_1 = x_1$ y $h \cdot x_2 = g \cdot y_2, \ldots, h \cdot x_{k-1} = g \cdot y_{k-1}$. Pero entonces $(g^{-1}h) \cdot x_1 = y_1, \ldots, (g^{-1}h) \cdot x_k = y_k$. □

5.3. Contando órbitas

Recordemos que para cada G-espacio X el símbolo $\mathcal{O}X$ denota al conjunto de órbitas de la acción y que para cada elemento g de G designamos con X^g al conjunto $\{x \in X : g \cdot x = x\}$ formado por los puntos de X que son dejados fijos por g. El siguiente resultado es conocido como lema de Burnside, pero es debido a Frobenius.

Teorema 5.24. *Para cada G-espacio X, los cardinales de los conjuntos X^g y $\mathcal{O}X$ están relacionados por la siguiente igualdad:*

$$|\mathcal{O}X||G| = \sum_{g \in G} |X^g|.$$

DEMOSTRACIÓN. En $\sum_{g\in G}|X^g|$ cada $x \in X$ es contado $|G_x|$ veces (pues G_x consiste de todos los $g \in G$ tales que $x \in X^g$). Puesto que $|G_x| = |G_y|$ siempre que x e y están en la misma órbita, y que la órbita de x tiene $|G : G_x|$ elementos, en la suma de arriba los elementos de $\mathcal{O}_x$ aportan en total el valor $|G| = |G : G_x||G_x|$. Recorriendo todas las órbitas de X obtenemos que $|\mathcal{O}X||G| = \sum_{g\in G}|X^g|$, como queremos. □

EJEMPLO 5.25. *La cantidad de clases de conjugación de un grupo finito G es igual a*

$$\frac{1}{|G|}\sum_{g\in G}|\,\mathrm{C}_G(g)|,$$

En efecto, para la acción de G sobre si mismo vía conjugación,

$$G^g = \{h \in G : ghg^{-1} = h\} = \{h \in G : hgh^{-1} = g\} = \mathrm{C}_G(g).$$

COROLARIO 5.26. *Si G es un grupo finito y X es un G-espacio transitivo con más de un elemento, entonces existe $g \in G$ tal que $X^g = \emptyset$.*

DEMOSTRACIÓN. Como X es transitivo, tiene una sóla órbita. En consecuencia, por el Teorema 5.24,

$$|G| = \sum_{g\in G}|X^g|$$

y, como $|X^1| = |X| > 1$, debe existir $g \in G$ tal que $X^g = \emptyset$. □

6. Teoremas de Sylow

Fijemos un número primo p. Un grupo finito es un *p-grupo* si su orden es una potencia de p. Supongamos que G es un grupo de orden $n = p^\alpha m$ con $\alpha > 0$ y m coprimo con p. Por definición un *p-subgrupo de Sylow* de G es un subgrupo de G de orden p^α. Cuando p esté claro o no nos interese hablaremos también de *subgrupos de Sylow*. En esta sección vamos a probar un teorema muy importante, que asegura, entre otras cosas, que el conjunto de los p-subgrupos de Sylow de G no es vacío. El teorema tiene tres items conocidos como primer, segundo y tercer teorema de Sylow, respectivamente. Esta es la razón del plural en el título. Antes de enunciar el resultado principal necesitamos establecer un par de lemas.

LEMA 6.1 (Teorema de Cauchy). *Si el orden de un grupo finito G es divisible por un primo p entonces G contiene un elemento de orden p.*

DEMOSTRACIÓN. Consideremos el subconjunto X de G^p formado por todas las p-uplas $(g_1, \ldots, g_p)$ tales que $g_1 \cdots g_p = 1$. El grupo cíclico $\mathbb{Z}_p$ actúa sobre X vía

$$i \cdot (g_1, \ldots, g_p) = (g_{1+i}, \ldots, g_p, g_1, \ldots, g_i).$$

Los puntos fijos de X son las p-uplas constantes $(g, \ldots, g)$ tales que $g^p = 1$. Como p divide a $|X| = |G|^{p-1}$ y cada órbita que no es un punto fijo tiene cardinal p, de la igualdad (29) se sigue que la cantidad de puntos fijos de X es un múltiplo de p. En consecuencia, existe $g \neq 1$ en G tal que $g^p = 1$. □

La noción de p-grupos se puede extender a grupos infinitos. La caracterización dada en el siguiente corolario indica la manera correcta de hacerlo.

COROLARIO 6.2. *Un grupo finito G es un p-grupo si y sólo si el orden de cada uno de sus elementos es una potencia de p.*

En la demostración del teorema de Sylow usaremos el teorema de Cauchy en el caso en que G es abeliano. Bajo esta hipótesis es posible dar una prueba alternativa del último por inducción en $|G|/p$, y obtener luego el caso general como un corolario inmediato del primero.

Demostración alternativa del teorema de Cauchy, para G abeliano. El resultado es obvio cuando $|G|/p = 1$. Para el paso inductivo tomemos $g \in G$ tal que $|g| > 1$. Si p divide a $|g|$, entonces $g^{|g|/p}$ tiene orden p. Si no, p divide a $|G/\langle g\rangle|$ y, por hipótesis inductiva, existe $h \in G$, tal que su clase en $G/\langle g\rangle$ tiene orden p. Pero entonces el orden de h es múltiplo de p y $h^{|h|/p}$ tiene orden p.

Lema 6.3. *Supongamos que P es un p-subgrupo de Sylow de G y que H es un p-subgrupo de G. Si H normaliza a P, entonces H está incluído en P.*

Demostración. Por hipótesis HP es un subgrupo de $\mathrm{N}_G(P)$ y P es un subgrupo normal de HP. Así por el tercer teorema del isomorfismo $H \cap P \lhd H$ y $HP/P \simeq H/H \cap P$, de lo cual se sigue que

$$|HP| = |HP : P||P| = |H : H \cap P||P|$$

es una potencia de p. Así, como P es un p-subgrupo maximal de G, necesariamente $H \leq P$. □

Demostración alternativa del Lema 6.3. De la Proposición 8.2 del Capítulo 1 o de igualdad (7), se sigue que $|HP|$ es una potencia de p. Por otro lado, debido a la hipótesis, HP es un subgrupo de P. Así, como P es un p-subgrupo maximal de G, necesariamente $H \leq P$.

Teorema 6.4 (Sylow). *Si G es un grupo finito y p es un primo que divide a $|G|$, entonces*

1. *La cantidad de p-subgrupos de Sylow de G es congruente a 1 módulo p.*
2. *Todos los p-subgrupos de Sylow de G son conjugados.*
3. *Todo p-subgrupo H de G está incluído en un p-subgrupo de Sylow de G. Además, la cantidad de p-subgrupos de Sylow de G que contienen a H es congruente a 1 módulo p.*

Demostración. Primero probemos que el conjunto de los p-subgrupos de Sylow de G no es vacío. Procedemos por inducción en $|G|/p$. Cuando $|G|/p = 1$, esto es trivial. Supongamos que $|G|/p = n > 1$ y que el resultado es cierto cuando $|G|/p < n$. Si G tiene un subgrupo propio H cuyo índice es coprimo con p, entonces todo p-subgrupo de Sylow de H (por hipótesis inductiva al menos hay uno) lo es también de G. Podemos suponer entonces que ningún subgrupo propio de G tiene índice coprimo con p. De la ecuación de las clases

$$|G| = |\operatorname{Z} G| + \sum_{g \in X' \setminus \operatorname{Z} G} |G : \mathrm{C}_G(g)|,$$

se sigue que p divide a $|\operatorname{Z} G|$. En consecuencia, por el Lema 6.1, el centro de G tiene un elemento g de orden p. Como $n > 1$ y g es central, $\langle g\rangle$ es un subgrupo normal y propio de G. Además p divide a $|G/\langle g\rangle| = |G|/p$, porque si no el índice de $\langle g\rangle$ sería coprimo con p. Tomemos un p-subgrupo de Sylow P' de $G/\langle g\rangle$ y consideremos su preimagen P por la proyección canónica $\pi\colon G \to G/\langle g\rangle$. La igualdad

$$|P| = |g||P'| = p|P'|$$

muestra que P es un p-subgrupo de Sylow de G. Fijemos un tal P y llamemos X a su clase de conjugación. Cada p-subgrupo H de G actúa por conjugación sobre X. Por el Lema 6.3,

$$X^H = \{gPg^{-1} : H \subseteq \mathrm{N}_G(gPg^{-1})\} = \{gPg^{-1} : H \subseteq gPg^{-1}\}.$$

Por otra parte

$$|X^H| \equiv |X| \pmod{p},$$

puesto que $X \setminus X^H$ es una unión disjunta de órbitas no triviales y, por el Corolario 5.13, el cardinal de cada órbita no trivial de X es una potencia positiva de p. Así,

$$|\{gPg^{-1} : H \subseteq gPg^{-1}\}| \equiv |X| \pmod{p}.$$

Como $\{gPg^{-1} : P \subseteq gPg^{-1}\} = \{P\}$, tomando $H = P$ en esta igualdad, concluímos que $|X| \equiv 1 \pmod{p}$ y, en consecuencia, que

$$|\{gPg^{-1} : H \subseteq gPg^{-1}\}| \equiv 1 \pmod{p}.$$

Aplicando esta fórmula con H un p-subgrupo de Sylow se obtiene el item 2). Considerando ahora H arbitrario se verifica que vale el item 3). Finalmente, el item 1) se sigue del 3) tomando $H = 1$. □

Para cada grupo finito G, designamos con el símbolo $\mathrm{Syl}_p G$ al conjunto de los p-subgrupos de Sylow de G.

Corolario 6.5. *Supongamos que G es un grupo finito y que p es un primo que divide al orden de G. La cantidad de p-subgrupos de Sylow de G es $|G : \mathrm{N}_G(P)|$, donde $P \in \mathrm{Syl}_p G$ es arbitrario.*

Demostración. Dado que la acción de G sobre $\mathrm{Syl}_p G$ por conjugación es transitiva,

$$|\mathrm{Syl}_p G| = |G : G_P| = |G : \mathrm{N}_G(P)|,$$

como afirmamos. □

Corolario 6.6. *Si G es un grupo finito de orden $p^r m$ con p primo y m coprimo con p, entonces $|\mathrm{Syl}_p G|$ divide a m.*

Demostración. Es una consecuencia inmediata del Corolario 6.5. □

Corolario 6.7. *Supongamos que P es un p-subgrupo de Sylow de un grupo finito G. Son equivalentes:*

1. *P es un subgrupo completamante normal de G.*
2. *P es un subgrupo normal de G.*
3. *P es el único p-subgrupo de Sylow de G.*

Demostración. 1) $\Rightarrow$ 2) Es trivial.

2) $\Rightarrow$ 3) Por el item 2) del Teorema 6.4.

3) $\Rightarrow$ 1) Si G tiene sólo un p-subgrupo de Sylow P, entonces P es completamente normal en G, porque la imagen de P por un endomorfismo de G es un p-subgrupo de G que, por el item 3) del Teorema 6.4, está incluído en P. □

Nota 6.8. *Supongamos que G es un grupo finito y que p es un primo que divide a $|G|$. Por los items 2) y 3) del teorema de Sylow, si H es un p-subgrupo normal de G, entonces H está incluído el la interseccion de todos los p-subgrupos de G. Por otro lado, del item 2) del teorema de Sylow se sigue también que la intersección de todos los p-subgrupos de Sylow de G es un p-subgrupo normal de G.*

PROPOSICIÓN 6.9. *Si $(P_i)_{i\in I}$ es una familia de subgrupos de Sylow de un grupo finito G, que contiene exáctamente un p-subgrupo de Sylow para cada primo p que divide a $|G|$, entonces G está generado por $\bigcup_{i\in I} P_i$.*

DEMOSTRACIÓN. Consideremos el subgrupo G' de G generado por $\bigcup_{i\in I} P_i$. Como $P_i \leq G'$, el orden de P_i divide a G' y, como los $|P_i|$'s son coprimos dos a dos, $|G| = \prod_{i\in I} |P_i|$ también divide a G'. Por lo tanto $G' = G$. □

OBSERVACIÓN 6.10. *Consideremos un subgrupo H de un grupo finito G y fijemos un divisor primo p de $|H|$. Por el item 3) del Teorema 6.4, todo p-subgrupo de Sylow P_H de H está incluído en un p-subgrupo de Sylow P de G y, además, $P_H = P \cap H$. En consecuencia,*

$$|\operatorname{Syl}_p H| \leq |\operatorname{Syl}_p G|.$$

Supongamos que P' es otro p-subgrupo de Sylow de G. Por el item 2) del mismo teorema, sabemos que existe $g \in G$ tal que $P' = gPg^{-1}$, de lo cual se sigue que

$$gP_Hg^{-1} = P' \cap gHg^{-1}.$$

Por consiguiente, si H es normal, entonces $P \cap H \in \operatorname{Syl}_p H$ para cada $P \in \operatorname{Syl}_p G$ (en particular, cada p-subgrupo normal de G está incluído en todos los p-subgrupos de Sylow de G). Además $PH/H \in \operatorname{Syl}_p(G/H)$, porque

$$|PH/H| = |P/(P \cap H)|$$

es una potencia de p y

$$|G/H : PH/H| = |G : PH|$$

es coprimo con p. Usando que

$$[g]\frac{PH}{H}[g]^{-1} = \frac{gPHg^{-1}}{H} = \frac{gPg^{-1}gHg^{-1}}{H} = \frac{gPg^{-1}H}{H} \qquad \text{para todo } g \in G,$$

y que todos los elementos de $\operatorname{Syl}_p(G/H)$ son conjugados, es fácil ver ahora que todos los subgrupos de Sylow de G/H son de esta forma.

PROPOSICIÓN 6.11. *Si H es un subgrupo normal de un grupo finito G y p es un primo que divide a $|H|$, entonces $|\operatorname{Syl}_p H|$ divide a $|\operatorname{Syl}_p G|$. Además*

$$\frac{|\operatorname{Syl}_p G|}{|\operatorname{Syl}_p H|} = \frac{|\operatorname{N}_G(P_H)|}{|\operatorname{N}_G(P)|} = \frac{|G : H||\operatorname{N}_H(P_H)|}{|\operatorname{N}_G(P)|},$$

donde P_H y P son p-subgrupos de Sylow arbitrarios de H y G, respectivamente.

DEMOSTRACIÓN. G actúa sobre $\operatorname{Syl}_p H$ por conjugación, porque

$$gP_Hg^{-1} \subseteq gHg^{-1} = H \qquad \text{para todo } P_H \in \operatorname{Syl}_p H \text{ y } g \in G.$$

Además, esta acción es transitiva debido a que lo es su restricción a H y, dado que $\operatorname{N}_G(P_H)$ es el estabilizador de P_H para la acción de G,

$$|\operatorname{Syl}_p H| = |G : \operatorname{N}_G(P_H)|.$$

Tomemos $P \in \operatorname{Syl}_p G$ tal que $P \cap H = P_H$. Como para todo $g \in \operatorname{N}_G(P)$,

$$gP_Hg^{-1} = g(P \cap H)g^{-1} = gPg^{-1} \cap gHg^{-1} = gPg^{-1} \cap H = P \cap H = P_H$$

el grupo $\operatorname{N}_G(P)$ está incluído en $\operatorname{N}_G(P_H)$. En consecuencia,

$$|H : \operatorname{N}_H(P_H)| = |\operatorname{Syl}_p H| = |G : \operatorname{N}_G(P_H)| \quad \text{divide a} \quad |G : \operatorname{N}_G(P)| = |\operatorname{Syl}_p G|.$$

Finalmente

$$\frac{|\,\mathrm{N}_G(P_H)|}{|\,\mathrm{N}_G(P)|} = \frac{|G:\mathrm{N}_G(P)|}{|G:\mathrm{N}_G(P_H)|} = \frac{|\,\mathrm{Syl}_p\, G|}{|\,\mathrm{Syl}_p\, H|} = \frac{|G:\mathrm{N}_G(P)|}{|H:\mathrm{N}_H(P_H)|} = \frac{|G:H||\,\mathrm{N}_H(P_H)|}{|\,\mathrm{N}_G(P)|},$$

como afirmamos. □

PROPOSICIÓN 6.12. *Si H es un subgrupo normal de un grupo finito G y p es un primo que divide a $|G/H|$, entonces $|\,\mathrm{Syl}_p(G/H)|$ divide a $|\,\mathrm{Syl}_p\, G|$.*

DEMOSTRACIÓN. Claramente G actúa sobre $\{PH/H : P \in \mathrm{Syl}_p\, G\}$ por conjugación y esta acción es transitiva. Puesto que $\mathrm{N}_G(P)$ está incluído en el estabilizador $G_{\frac{PH}{H}}$ de PH/H y que $|\,\mathrm{Syl}_p(G/H)| = |G:G_{\frac{PH}{H}}|$, el cardinal de $\mathrm{Syl}_p(G/H)$ divide a $|G:\mathrm{N}_G(P)| = |\,\mathrm{Syl}_p\, G|$. □

6.1. Algunos ejemplos

El objetivo de esta subsección es determinar los subgrupos de Sylow de algunos grupos finitos.

EJEMPLO 6.13. *Es fácil ver que $\langle(1,2)\rangle$, $\langle(1,3)\rangle$ y $\langle(2,3)\rangle$ son los 2-subgrupos de sylow de S_3 y que $\langle(1,2,3)\rangle$ es su único 3-subgrupo de Sylow.*

EJEMPLO 6.14. *Consideremos el grupo simétrico S_4. Como se trata de un grupo de orden $4! = 2^3 \times 3$, sus 2-subgrupos de Sylow tienen orden 8 y sus 3-subgrupos de Sylow, orden 3. Dado que los únicos elementos de orden 3 de S_4 son sus ocho 3-ciclos, los últimos son los grupos cíclicos*

$$\langle(1,2,3)\rangle, \quad \langle(1,2,4)\rangle, \quad \langle(1,3,4)\rangle \quad y \quad \langle(2,3,4)\rangle.$$

Por otra parte, como

$$H := \{\mathrm{id}, (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3)\}$$

es invariante, está incluído en todos los 2-subgrupos de Sylow de S_4. Por lo tanto, estos son los subgrupos $P_\sigma := \langle\sigma, H\rangle$, con $\sigma \in \mathrm{S}_4 \setminus H$ un elemento cuyo orden es una potencia de 2. Por ejemplo, podemos tomar como σ a un 4-ciclo. Más aún, por el Teorema 1.2 del Capítulo 2 y el item 2) del teorema de Sylow, sabemos que todos los 2-subgrupos de Sylow de S_4 tienen esta forma. Puesto que $\langle\sigma\rangle = \langle\sigma^3\rangle$, los únicos candidatos son $P_{(1,2,3,4)}$, $P_{(1,2,4,3)}$ y $P_{(1,3,2,4)}$. Un cálculo directo muestra que

$$P_{(1,2,3,4)} := \{\mathrm{id}, (1,3), (2,4), (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3), (1,2,3,4), (1,4,3,2)\},$$
$$P_{(1,2,4,3)} := \{\mathrm{id}, (1,4), (2,3), (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3), (1,2,4,3), (1,3,4,2)\}$$

y

$$P_{(1,3,2,4)} := \{\mathrm{id}, (1,2), (3,4), (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3), (1,3,2,4), (1,4,2,3)\}.$$

Finalmente, como $P_{(1,2,3,4)}$ está generado por las permutaciones

$$\sigma := (1,2,3,4) \quad y \quad \tau := (1,4)\circ(2,3),$$

y $\sigma^4 = \tau^2 = \tau\circ\sigma\circ\tau^{-1}\circ\sigma = \mathrm{id}$, los grupos $P_{(1,2,3,4)}$, $P_{(1,2,4,3)}$ y $P_{(1,3,2,4)}$ son isomorfos a D_4.

EJEMPLO 6.15. *Parte de los argumentos usados en el ejemplo anterior muestran que*

$$\langle(1,2,3)\rangle, \quad \langle(1,2,4)\rangle, \quad \langle(1,3,4)\rangle \quad y \quad \langle(2,3,4)\rangle$$

son los 3-subgrupos de Sylow de A_4, y que $H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ es su único 2-subgrupo de Sylow.

EJEMPLO 6.16. *Consideremos el grupo diedral D_n. Recordemos que D_n está generado por dos elementos x e y sujetos a las relaciones*

$$x^n = 1, \quad y^2 = 1 \quad e \quad yxy^{-1}x = 1,$$

y que

$$D_n = \{1, \ldots, x^{n-1}, y, \ldots, x^{n-1}y\}.$$

Recordemos también que

- *Los elementos $x^i y$ tienen orden 2.*
- *Los elementos x^i tienen orden $n/(n : i)$.*
- *El subgrupo $\langle x^i \rangle$ de D_n es invariante para todo i.*

Escribamos $n = 2^m t$ con t impar, de manera que $|D_n| = 2^{m+1}t$. Afirmamos que:

1. *Todos los 2-subgrupos de Sylow de D_n son isomorfos a D_{2^m}, y hay t de ellos (aquí debemos interpretar a D_1 como el grupo cíclico de orden 2).*
2. *Si p es un primo impar que divide a t, entonces D_n tiene un único p-subgrupo de Sylow, el cual es cíclico.*

El item 2) se sigue inmediatamente de que si $t = p^u v$ con v coprimo con p, entonces $\langle x^{2^m v} \rangle$ tiene orden p^u y es invariante. Consideremos ahora el item 1). Como $\langle x^t \rangle \triangleleft D_n$ y $|x^t| = 2^m$, todos los 2-subgrupos de Sylow de D_n incluyen a $\langle x^t \rangle$. En consecuencia, dado que el orden de ningún $x^i \in D_n \setminus \langle x^t \rangle$ es una potencia de 2, los posibles 2-subgrupos de Sylow de D_n, son los subgrupos $K_i := \langle x^i y, x^t \rangle = \langle x^t \rangle \langle x^i y \rangle$, donde la última igualdad vale porque $\langle x^t \rangle$ es normal. De hecho, como

$$|\langle x^t \rangle \langle x^i y \rangle| = \frac{|\langle x^t \rangle||\langle x^i y \rangle|}{|\langle x^t \rangle \cap \langle x^i y \rangle|} = \frac{2^m \times 2}{1} = 2^{m+1},$$

todos los K_i son, efectivamente, 2-subgrupos de Sylow de D_n. Puesto que

$$K_i = \langle x^i y, x^t \rangle = \{x^{tj+i} y, x^{tj} : 0 \leq j < 2^m\},$$

es claro que $K_i = K_{i'}$ si y sólo si $i' \equiv i \pmod{t}$. Así, los 2-subgrupos de Sylow de D_n son exactamente $K_0, \ldots, K_{t-1}$. Para ver que K_i es isomorfo a D_n es suficiente notar que tiene orden 2^{m+1} y que los elementos $x^i y$ y x^t generan K_i y satisfacen

$$(x^t)^{2^m} = 1, \quad (x^i y)^2 = 1 \quad y \quad (x^i y)x^t(x^i y)^{-1}x^t = 1.$$

EJEMPLO 6.17. *Recordemos que el grupo cuaterniónico generalizado H_n está generado por dos elementos x e y sujetos a las relaciones*

$$x^n y^{-2} = 1 \quad e \quad yxy^{-1}x = 1,$$

y que

$$H_n = \{1, \ldots, x^{2n-1}, y, \ldots, x^{2n-1}y\}.$$

Recordemos también que

- *Los elementos $x^i y$ tienen orden 4.*
- *Los elementos x^i tienen orden $2n/(2n : i)$.*
- *El subgrupo $\langle x^i \rangle$ de H_n es invariante para todo i.*

Escribamos $n = 2^m t$ con t impar, de manera que $|H_n| = 2^{m+2}t$. Afirmamos que:

1. *Todos los 2-subgrupos de Sylow de H_n son isomorfos a H_{2^m}, y hay t de ellos (aquí debemos interpretar a H_1 como el grupo cíclico de orden 4).*

2. *Si p es un primo impar que divide a t, entonces H_n tiene un único p-subgrupo de Sylow, el cual es cíclico.*

El item 2) se sigue inmediatamente de que si $t = p^u v$ con v coprimo con p, entonces $\langle x^{2^{m+1}v}\rangle$ tiene orden p^u y es invariante. Consideremos ahora el item 1). El subgrupo $\langle x^t\rangle$ de H_n está incluído en todos los 2-subgrupos de Sylow de H_n, porque es invariante y tiene 2^{m+1} elementos. En consecuencia, como el orden de ningún $x^i \in H_n \setminus \langle x^t\rangle$ es una potencia de 2, los posibles 2-subgrupos de Sylow de H_n son algunos de los subgrupos $L_i := \langle x^i y, x^t\rangle = \langle x^t\rangle\langle x^i y\rangle$, donde la última igualdad vale porque $\langle x^t\rangle$ es invariante. Notemos ahora que

$$(x^i y)^2 = x^i y x^i y^{-1} y^2 = y^2 = x^n$$

y, por lo tanto, $\langle x^i y\rangle \cap \langle x^t\rangle = \{1, x^n\}$. Así,

$$|\langle x^t\rangle\langle x^i y\rangle| = \frac{|\langle x^t\rangle||\langle x^i y\rangle|}{|\langle x^t\rangle \cap \langle x^i y\rangle|} = \frac{2^{m+1}\times 4}{2} = 2^{m+2},$$

lo que muestra que todos los L_i son 2-subgrupos de Sylow. Puesto que

$$L_i = \langle x^i y, x^t\rangle = \{x^{tj+i} y, x^{tj} : 0 \le j < 2^{m+1}\},$$

es claro que $L_i = L_{i'}$ si y sólo si $i' \equiv i \pmod t$. Así, los 2-subgrupos de Sylow de H_n son exactamente $L_0, \dots, L_{t-1}$. Para ver que L_i es isomorfo a H_{2^m} es suficiente notar que tiene orden 2^{m+2} y que $x^i y$ y x^t generan L_i y satisfacen

$$(x^t)^{2^m}(x^i y)^{-2} = 1 \quad y \quad (x^i y)x^t(x^i y)^{-1}x^t = 1.$$

Ejemplo 6.18. *Consideremos un grupo simétrico S_p, con p primo. Como $|\mathrm{S}_p| = p!$ y p es coprimo con $(p-1)!$, cada p-subgrupo de Sylow de S_p es cíclico de orden p y así está generado por un p-cíclo. Como la cantidad de los p-cíclos de S_p es $(p-1)!$ y cada subgrupo cíclico de orden p de S_p tiene $p-1$ de estos p-cíclos, la cantidad de p-subgrupos de Sylow de S_p es*

$$(p-2)! = \frac{(p-1)!}{p-1}.$$

En consecuencia, por el item (1) del teorema de Sylow

$$(p-2)! \equiv 1 \pmod p,$$

que es lo que dice el famoso teorema de Wilson.

Ejemplo 6.19. *Supongamos que k es un cuerpo de p^m elementos con p primo (más adelante veremos que el cardinal de un cuerpo finito siempre es una potencia de un primo). Por la Proposición 5.14 sabemos que, cualquiera sea n, el orden de $\mathrm{GL}(n,k)$ es*

$$p^{mn(n-1)/2}(p^{mn}-1)(p^{m(n-1)}-1)\cdots(p^m-1).$$

En consecuencia, como p es coprimo con $(p^{mn}-1)(p^{m(n-1)}-1)\cdots(p^m-1)$, los p-subgrupos de Sylow de $GL(n,k)$ tienen $p^{mn(n-1)/2}$ elementos. Puesto que este es el orden del subgrupo $\mathrm{UT}(n,k)$ de $\mathrm{GL}(n,k)$, formado por las matrices triangulares superiores que tienen 1 en la diagonal principal, $\mathrm{UT}(n,k)$ es un p-subgrupo de Sylow de $\mathrm{GL}(n,k)$.

Teorema 6.20 (Frattini). *Si H es un subgrupo normal de un grupo finito G y P es un p-subgrupo de Sylow de H, entonces $G = H\,\mathrm{N}_G(P)$. En particular, P es un subgrupo normal de H si y sólo si es un subgrupo normal de G.*

DEMOSTRACIÓN. Tomemos $g \in G$. Como H es normal, $gPg^{-1} \subseteq gHg^{-1} = H$. En consecuencia, por el item 2) del teorema de Sylow, existe $h \in H$ tal que $hgPg^{-1}h^{-1} = P$. Así, $g = h^{-1}hg \in H\,\mathrm{N}_G(P)$. □

COROLARIO 6.21. *Si un subgrupo H de un grupo finito G contiene al normalizador de un subgrupo de Sylow P de G, entonces $\mathrm{N}_G(H) = H$.*

DEMOSTRACIÓN. Debido al Teorema 6.20, como H es normal en $\mathrm{N}_G(H)$,

$$\mathrm{N}_G(H) = H\,\mathrm{N}_{\mathrm{N}_G(H)}(P) \subseteq H\,\mathrm{N}_G(P) = H,$$

como queremos. □

6.2. Algunas aplicaciones

En esta subsección establecemos algunos resultados que son consecuencia más o menos directa del teorema de Cauchy, los Teoremas de Sylow y sus corolarios. El primero es la clasificación de los grupos finitos cuyo orden es producto de dos primos distintos. La prueba que damos usa de manera escencial el teorema de Cauchy.

TEOREMA 6.22 (Caracterización de grupos de orden pq). *Supongamos que G es un grupo de orden pq con p y q primos y $q < p$.*

- *Si G es abeliano, entonces $G \simeq \mathbb{Z}_{pq}$.*
- *Si G no es abeliano, entonces q divide a $p-1$, el conjunto*

$$R = \{r \in \mathbb{N} : 1 < r < p \text{ y } r^q \equiv 1 \pmod{p}\}$$

no es vacío y G está generado por elementos g y h, de órdenes p y q respectivamente, que satisfacen $hgh^{-1} = g^{r_0}$, donde r_0 es el mínimo elemento de R. En particular, G es producto semidirecto interno de los subgrupos $\langle g\rangle$ y $\langle h\rangle$.

DEMOSTRACIÓN. Por el teorema de Cauchy, existen $g, k \in G$ con $|\langle g\rangle| = p$ y $|\langle k\rangle| = q$. Además, por el Corolario 2.15, el primero es normal. Si $\langle k\rangle$ también lo es, entonces

$$[g,k] = gkg^{-1}k^{-1} \in \langle g\rangle \cap \langle k\rangle = 1$$

y así $G = \langle g\rangle \times \langle k\rangle \simeq \mathbb{Z}_{pq}$. Supongamos ahora que $\langle k\rangle$ no es normal. Como $\langle g\rangle$ si lo es, existe $0 \le r < p$ tal que $kgk^{-1} = g^r$. Un argumento inductivo muestra ahora que $k^i g k^{-i} = g^{r^i}$ para todo $i > 1$, por lo que

$$g^{r^q} = k^q g k^{-q} = g,$$

lo cual implica que $r^q \equiv 1 \pmod{p}$. Por otra parte, dado que la igualdad $kgk^{-1} = 1$ es imposible y que G no es conmutativo, debe ser $r > 1$. Por lo tanto, como q es primo, q es el orden de r en $\mathbb{Z}_p^*$. En consecuencia, por el teorema de Lagrange, q divide a $|\mathbb{Z}_p^*| = p-1$. Como la ecuación $X^q = 1$ no puede tener más de q raíces en $\mathbb{Z}_p^*$, y cada potencia de r es una raíz, existe $\alpha < q$ tal que $r^\alpha \equiv r_0 \pmod{p}$, donde r_0 es el mínimo de los enteros s tales que

$$1 < s < p \qquad \text{y} \qquad s^q \equiv 1 \pmod{p}.$$

Tomemos $h = k^\alpha \neq 1$. Puesto que $k = h^\beta$, donde $\beta \in \mathbb{Z}_q$ es el inverso multiplicativo de α, el grupo G está generado por g y h. Finalmente, como

$$h^q = (k^\alpha)^q = (k^q)^\alpha = 1 \quad \text{y} \quad hgh^{-1} = k^\alpha g k^{-\alpha} = g^{r^\alpha} = g^{r_0},$$

los elementos g y h satisfacen las relaciones requeridas en el enunciado. □

Supongamos que p y q son primos y que q divide a $p-1$. Por el teorema de Cauchy $\mathbb{Z}_p^*$ tiene un elemento r de orden q. Por el Ejemplo 16.9 del Capítulo 1, sabemos que para cada uno de estos r hay un grupo de orden pq generado por elementos g y h, de órdenes p y q respectivamente, que satisfacen $hgh^{-1} = g^r$.

En el resto de esta subsección denotaremos con n_p a la cantidad de p-subgrupos de Sylow de un grupo finito G.

PROPOSICIÓN 6.23. *Ningún grupo de orden p^2q, donde p y q son dos números primos distintos, es simple. Más precisamente, todo grupo G de este orden tiene un subgrupo normal de orden p^2 o un subgrupo normal de orden q.*

DEMOSTRACIÓN. Por el Corolario 6.6, forzosamente $n_q = 1$, $n_q = p$ o $n_q = p^2$. En el primer caso el único q-subgrupo de Sylow de G es normal debido al Corolario 6.7 . Por el item 1) del teorema de Sylow, en el segundo $p \equiv 1 \pmod q$, por lo que $p > q$. Puesto que, nuevamente por el Corolario 6.6 y el item 1) del teorema de Sylow, $n_p \mid q$ y $n_p \equiv 1 \pmod p$, esto implica que $n_p = 1$, y así G tiene un único p-subgrupo de Sylow, el cual es normal, nuevamente por el Corolario 6.7. Por último en el tercer caso el grupo G tiene $p^2(q-1)$ elementos de orden q y los restantes p^2 elementos de G sólo pueden formar un p-subgrupo de Sylow de G, el cual es normal por la misma razón que antes. □

NOTA 6.24. *Supongamos que H sartisface la hipótesis de la proposición anterior y tomemos subgrupos P y Q de Sylow de H de ordenes p^2 y q respectivamente. Como $|P \cap Q|$ divide a p^2 y a q, necesariamente $P \cap Q = 1$ y así $|PQ| = p^2q$ (por ejemplo debido a la Proposición 8.2 del Capítulo 1). En consecuencia H es el producto semidirecto interno de P y Q. Por último, si P y Q son normales, entonces este es un producto directo.*

PROPOSICIÓN 6.25. *Ningún grupo de orden $2pq$, donde $p < q$ son dos números primos impares, es simple. Más precisamente, si G es un grupo de ese orden, entonces G tiene un subgrupo normal de orden p o un subgrupo normal de orden q.*

DEMOSTRACIÓN. Por el item 1) del teorema de Sylow, existen enteros no negativos h_p y h_q tales que $n_p = h_p p + 1$ y $n_q = h_q q + 1$. Denotemos con S a la unión de todos los p-subgrupos de Sylow de G y todos los q-subgrupos de Sylow de G. Si el resultado es falso, entonces por el Corolario 6.7 necesariamente $h_p, h_q \geq 1$ y, en consecuencia,

$$\begin{aligned} |(G \setminus S) \cup 1| &= 2pq - \big((h_p p + 1)(p-1) + (h_q q + 1)(q-1)\big) \\ &\leq 2pq - \big((p+1)(p-1) + (q+1)(q-1)\big) \\ &= 2pq - (p^2 - 1 + q^2 - 1) \\ &= -(q-p)^2 + 2 \leq -2, \end{aligned}$$

lo que es absurdo. □

NOTA 6.26. *Por el Corolario 2.8 sabemos que si un grupo G tiene orden $2m$ com m impar, entonces G tiene un subgrupo de índice 2 y, por lo tanto, normal. Si $m > 1$, entonces este grupo no sería trivial y, por lo tanto, G no sería simple. Esto da una demostración alternativa de que ningún grupo de orden $2pq$, donde $p < q$ son dos números primos impares, es simple.*

Aplicaciones a grupos de orden pequeño En este parágrafo aplicamos los Teoremas de Sylow para determinar salvo isomorfismos todos los grupos simples de un orden fijo dado.

En todos los casos considerados el orden es menor que 100 y, salvo en uno, lo que se prueba es la no existencia de grupos simples del orden requerido.

No existen subgrupos simples G de orden 36: Tomemos un 3-subgrupo de Sylow P de G. Por el Corolario 2.13 sabemos que P contiene un subgrupo P', que es normal en G y cuyo índice en G es $4h$, con h un divisor de $(3! : 3^2) = 3$. En particular, P' es un subgrupo no trivial de G.

No existen subgrupos simples G de orden 48: Tomemos un 2-subgrupo de Sylow P de G. Por el Corolario 2.13, sabemos que P contiene un subgrupo normal P', cuyo índice en G es $3h$, con h un divisor de $(2! : 2^4) = 2$. En particular, P' es un subgrupo no trivial de G.

No existen grupos simples G de orden 56: En efecto, como $n_7 \equiv 1$ (mód 7) y $n_7 \mid 8$, debe ser $n_7 = 1$ u $n_7 = 8$. En el primer caso G tiene un único 7-subgrupo de Sylow que, justamente por eso, es normal, y, en el segundo, G tiene $8 \times 6 = 48$ elementos de orden 7 y los restantes 8 sólo pueden formar un 2-subgrupo de Sylow de G, el cual es normal por la misma razón.

No existen subgrupos simples G de orden 80: Tomemos un 2-subgrupo de Sylow P de G. Por el Corolario 2.13, sabemos que P contiene un subgrupo normal P', cuyo índice en G es $5h$, con h un divisor de $(4! : 2^4) = 8$. En particular, P' es un subgrupo no trivial de G. También se puede proceder de la siguiente manera: Como $n_5 \equiv 1$ (mód 5) y $n_5 \mid 2^4$ debe ser $n_5 = 1$ o $n_5 = 16$. En el primer caso G tiene un único 5-subgrupo de Sylow que, por lo tanto, es normal, y, en el segundo, G tiene $16 \times 4 = 64$ elementos de orden 5 y los restantes 16 elementos sólo pueden formar un 2-subgrupo de Sylow de G, el cual necesariamente es normal.

No existen grupos simples G de orden 84: En efecto, como $n_7 \equiv 1$ (mód 7) y $n_7 \mid 12$, forzosamente $n_7 = 1$. Así, G tiene un único 7-subgrupo de Sylow que, por lo tanto, es normal.

No existen subgrupos simples G de orden 96: Tomemos un 2-subgrupo de Sylow P de G. Por el Corolario 2.13, sabemos que P contiene un subgrupo normal P', cuyo índice en G es $3h$, con h un divisor de $(2! : 2^5) = 2$. En particular, P' es un subgrupo no trivial de G.

Todo grupo simple de orden 60 es isomorfo a $\mathbf{A_5}$: Por la Proposición 3.7 del Capítulo 2 y el Corolario 2.11 para probar esto será suficiente ver que si G es un grupo simple de orden 60, entonces G tiene un subgrupo H de índice 5. Por el item 1) del teorema de Sylow y el Corolario 6.6, sabemos que $n_2 \in \{1, 3, 5, 15\}$ y $n_5 \in \{1, 6\}$. Por el Corolario 6.7, como G es simple, no puede ser $n_2 = 1$ ni $n_5 = 1$. En particular G tiene 24 elementos de orden 5. Además, por el Corolario 6.5, sabemos que si $n_2 = 3$, entonces G tiene un subgrupo de índice 3. Pero esto es imposible, porque por el Teorema 2.9, en tal caso G tendría un subgrupo normal propio. Así que tampoco puede ser $n_2 = 3$. Si $n_2 = 5$, entonces por el Corolario 6.5, podemos tomar $H = \mathrm{N}_G(P)$ dónde P es un 2-subgrupo de Sylow arbitrario. Supongamos por último que $n_2 = 15$. Si cada par de 2-subgrupos de Sylow de G tuviera intersección trivial, G tendría $15 \times 3 = 45$ elementos de orden par, que sumados a los 24 de orden 5, da 69, lo que es absurdo. Así que existen dos 2-subgrupos de Sylow P_1 y P_2 tales que $K = P_1 \cap P_2$ no es trivial. Claramente K es un subgrupo normal de P_1 y P_2 y, por lo tanto, de $\langle P_1, P_2 \rangle$. En consecuencia, como G es simple, $\langle P_1, P_2 \rangle \neq G$. Como $4 = |P_1|$ divide propiamente a $|\langle P_1, P_2 \rangle|$ y

$|\langle P_1, P_2\rangle|$ divide propiamente a $|G|$, forzosamente $|\langle P_1, P_2\rangle| = 12$ o $|\langle P_1, P_2\rangle| = 20$. Pero lo último es imposible, por el Teorema 2.9. Así pues, el índice de $\langle P_1, P_2\rangle$ en G es 5 y podemos tomar $H = \langle P_1, P_2\rangle$.

7. p-Grupos finitos

En esta sección p denota a un primo positivo y, en ella, establecemos algunas propiedades básicas de los p-grupos finitos.

TEOREMA 7.1. *Si G es un p-grupo finito, $H \triangleleft G$ y $H \neq 1$, entonces $H \cap \mathrm{Z}\, G \neq 1$. En particular, $\mathrm{Z}\, G$ no es trivial.*

DEMOSTRACIÓN. Consideremos la ecuación

$$|H| = |H \cap \mathrm{Z}\, G| + \sum_{h \in X' \setminus (H \cap \mathrm{Z}\, G)} |G : \mathrm{C}_G(h)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de G que están incluídas en H (vease el segundo ejemplo debajo de la igualdad (31)). Dado que tanto $|H|$ como cada $|G : \mathrm{C}_G(h)|$ son divisibles por p, también lo es $|H \cap \mathrm{Z}\, G|$, de manera de que $H \cap \mathrm{Z}\, G$ no es trivial. □

COROLARIO 7.2. *Todo subgrupo normal de orden p de un p-grupo G está incluído en el centro de G.*

COROLARIO 7.3. *Si $|G| = p^n$, entonces toda cadena*

$$1 = G_0 \subseteq G_{i_1} \subseteq G_{i_2} \subseteq \cdots \subseteq G_{i_r} \subseteq G_n = G,$$

de subgrupos normales de G con $0 < i_1 < i_2 < \cdots < i_r < n$ y $|G_{i_j}| = p^{i_j}$, se puede completar a una cadena

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

de subgrupos normales de G con $|G_j| = p^j$. En particular G tiene un subgrupo normal de orden p^j para cada $j \leq n$.

DEMOSTRACIÓN. Para grupos de orden p el resultado es trivial. Supongamos que $n > 1$ y que es cierto para p-grupos de orden menor que p^n. Por el Teorema 7.1 existe $g \in \mathrm{Z}(G) \cap G_{i_1}$ tal que $G_1 := \langle g\rangle$ es un subgrupo normal de orden p de G incluído en G_{i_1}. Por lo tanto podemos suponer sin pérdida de generalidad que $i_1 = 1$. Consideremos la proyección canónica $\pi\colon G \to G/G_1$. Por hipótesis inductiva la cadena

$$1 = \overline{G}_0 \subseteq \overline{G}_{i_2-1} \subseteq \overline{G}_{i_3-1} \subseteq \cdots \subseteq \overline{G}_{i_r-1} \subseteq \overline{G}_{n-1} = G/G_1,$$

donde $\overline{G}_{i_j-1}$ denota a $\pi(G_{i_j})$, se puede extender a una cadena

$$1 = \overline{G}_0 \subseteq \overline{G}_1 \subseteq \overline{G}_2 \subseteq \cdots \subseteq \overline{G}_{n-1} \subseteq \overline{G}_{n-1},$$

de subgrupos normales de $\overline{G}_{n-1}$, tal que $|\overline{G}_j| = p^j$ para $1 \leq j \leq n-1$. Es claro que la cadena

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

obtenida tomando $G_0 = 1$ y $G_j = \pi^{-1}(\overline{G}_{j-1})$ para $1 \leq j \leq n$, satisface las condiciones requeridas en el enunciado. □

COROLARIO 7.4. *Todo grupo G de orden p^2 es abeliano. Además son equivalentes:*

1. *G no es cíclico.*
2. *G tiene $p+1$ subgrupos de orden p.*
3. *G tiene al menos dos subgrupos de orden p.*
4. *G es isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Demostración. Supongamos que G no es abeliano, entonces por el Teorema 7.1 los grupos $\mathrm{Z}\,G$ y $G/\mathrm{Z}\,G$ tienen orden p y, por eso mismo son cíclicos, lo que contradice la Proposición 18.9 del Capítulo 1. Ahora consideremos las equivalencias. Si G no es cíclico, entonces cada uno de los p^2-1 elementos no nulos de G genera un subgrupo de orden p. Como estos subgrupos se intersecan trivialmente, G tiene $p+1=(p^2-1)/(p-1)$ subgrupos de este orden. En consecuencia 1) $\Rightarrow$ 2). Es evidente que 2) $\Rightarrow$ 3) y 4) $\Rightarrow$ 1). Resta comprobar que 3) $\Rightarrow$ 4). Para ello, debido a la Proposición 15.14 del Capítulo 1, será suficiente ver que G es el producto directo interno de dos cualesquiera de sus subgrupos de orden p. Pero como la intersección de dos de estos subgrupos es claramente 1, esto se sigue de la Proposición 8.2 del Capítulo 1 y el Teorema 15.1 del Capítulo 1. □

Corolario 7.5. *Si G es un grupo no conmutativo de orden p^3, entonces el centro de G coincide con el subgrupo conmutador, tiene orden p, y es el único subgrupo invariante de G de ese orden. Además, $G/\mathrm{Z}\,G$ es abeliano y no es cíclico.*

Demostración. Por el Teorema 7.1 sabemos que $\mathrm{Z}\,G \neq 1$ y, como G no es abeliano, $\mathrm{Z}\,G \neq G$. Además, por la Proposición 18.9 del Capítulo1, el cociente $G/\mathrm{Z}\,G$ no es cíclico. Por lo tanto $|G/\mathrm{Z}\,G| = p^2$ y $|\,\mathrm{Z}\,G| = p$. Por otra parte, dado que por el corolario anterior $G/\mathrm{Z}\,G$ es abeliano,

$$[G,G] \subseteq \mathrm{Z}\,G.$$

Pero la inclusión no puede ser propia, porque eso significaría que G es abeliano. Finalmente, por el Corolario 7.2, el único subgrupo normal de orden p de G es $\mathrm{Z}\,G$. □

Teorema 7.6. *Si H es un subgrupo propio de un p-grupo finito G, entonces $H \subsetneq \mathrm{N}_G(H)$.*

Demostración. Si H es normal, entonces $H \subsetneq G = \mathrm{N}_G(H)$. Supongamos que H no es normal. Bajo esta hipótesis, el cardinal $|G : N_G(H)|$, del conjunto X de los subgrupos de G conjugados a H, es una potencia de p mayor que 1. El grupo H actúa sobre X por conjugación y, como H es un p-grupo, el cardinal de cada una de las órbitas de X bajo esta acción es una potencia de p. En consecuencia, como H es un punto fijo, X tiene al menos otros $p-1$ puntos fijos. Tomemos uno de ellos gHg^{-1}, distinto de H. Entonces $hgHg^{-1}h^{-1} = gHg^{-1}$ para cada $h \in H$, por lo que $g^{-1}Hg \subseteq \mathrm{N}_G(H)$. Esto termina la prueba porque $g^{-1}Hg \neq H$. □

Corolario 7.7. *Si H es un subgrupo propio maximal de un p-grupo finito G, entonces H es normal y su índice es p.*

Demostración. Por el teorema anterior $H \triangleleft G$. Además, por el Corolario 13.15 del Capítulo 1, el cociente G/H no tiene subgrupos no triviales y, en consecuencia, debido al Corolario 7.3, su cardinal es p. □

Observación 7.8. *Supongamos que H es un subgrupo propio de un p-grupo finito G. Por el Teorema 7.6, en la cadena de subgrupos*

$$H \triangleleft \mathrm{N}_G^1(H) \triangleleft \mathrm{N}_G^2(H) \triangleleft \cdots \triangleleft \mathrm{N}_G^{i-1}(H)) \triangleleft \mathrm{N}_G^i(H) = G,$$

donde $\mathrm{N}_G^{j+1}(H) = \mathrm{N}_G(\mathrm{N}_G^j(H))$ *para todo* $j < i$*, cada grupo es un subgrupo propio del siguiente. Como* G *es un p-grupo, los órdenes de los grupos que constituyen la cadena anterior forman una sucesión estrictamente creciente*

$$p^{\alpha_0} < p^{\alpha_1} < \cdots < p^{\alpha_i},$$

de potencias de p*. Por el Corolario 7.3, para cada* $j < i$ *hay una cadena*

$$\mathrm{N}_G^j(H) = G_{\alpha_j} \subseteq G_{\alpha_j+1} \subseteq \cdots \subseteq G_{\alpha_{j+1}-1} \subseteq G_{\alpha_{j+1}} = \mathrm{N}_G^{j+1}(H),$$

en la cual G_{α_j+l} *es un subgrupo normal de orden* p^{α_j+l} *de* $\mathrm{N}_G^{j+1}(H)$*. En particular* H *está incluído en un subgrupo de índice* p *de* G*.*

Teorema 7.9. *Consideremos un subgrupo arbitrario* H *de un grupo finito* G*. Si* $|H|$ *divide a* p^m *y* p^m *divide al orden de* G*, entonces la cantidad de p-subgrupos de* G *de orden* p^m *que incluyen a* H *es congruente a* 1 *módulo* p*.*

Demostración. Podemos suponer que $|H| < p^m$ ya que en otro caso el resultado es trivial. Escribamos $|G| = p^m r$. Haremos la demostración por inducción en el máximo entero no negativo n tal que p^n divide a r. Cuando $n = 0$ el enunciado se reduce al item 3) del Teorema 6.4. Supongamos que $n > 0$ y que el teorema vale para subgrupos de G de orden p^{m+1}. Designemos con

$$P_1, \ldots, P_u \qquad \text{y} \qquad Q_1, \ldots, Q_v$$

a los subgrupos de G, de orden p^{m+1} y p^m respectivamente, que contienen a H. Por hipótesis inductiva la cantidad a_j de los P_i's que contienen a un Q_j fijo, es congruente a 1 módulo p. Para concluir la demostración será suficiente mostrar que la cantidad b_i de los Q_j's que están contenidos en un P_i fijado, también es congruente a 1 módulo p, ya que entonces de la igualdad

$$\sum_{i=1}^{u} b_i = \sum_{j=1}^{v} a_j,$$

válida pues las dos sumas cuentan a cada P_i con multiplicidad igual a la cantidad de Q_j's que contiene, se seguirá que $u \equiv v \pmod{p}$. Con esto en mente fijemos P_i y supongamos que

$$Q_{j_1}, \ldots, Q_{j_{v'}}$$

son los Q_j's contenidos en P_i. Debemos mostrar que $v' \equiv 1 \pmod{p}$. Por el Corolario 7.3 aplicado al grupo P_i y a la cadena trivial $1 \subseteq P_i$ sabemos que $v' \geq 1$. Si $v' = 1$, entonces es obvio que $v' \equiv 1 \pmod{p}$. Analizemos que ocurre cuando $v' > 1$. Por el Corolario 7.7, cada Q_{j_l} es un subgrupo normal de P_i. Por consiguiente $Q_{j_1} Q_{j_2} = P_i$. Por la Proposición 8.2 del Capítulo 1, esto implica que $D_1 := Q_{j_1} \cap Q_{j_2}$ tiene orden p^{m-1}. Además $D_1 \lhd P_i$ porque es la intersección de dos subgrupos normales de P_i. Por el Corolario 7.4, el cociente P_i/D_1 es abeliano y tiene $p+1$ subgrupos de orden p. En consecuencia, en el conjunto

$$\{Q_{j_1}, \ldots, Q_{j_{v'}}\}$$

hay $p+1$ elementos que incluyen a D_1. Si $v' = p+1$ esto termina la demostración. Supongamos que $v' > p+1$ y tomemos $Q_{j_{l_3}}$ tal que D_1 no esté incluído en $Q_{j_{l_3}}$. Escribamos $D_2 := Q_{j_1} \cap Q_{j_{l_3}}$. Razonando como antes, vemos que $p+1$ de los elementos del conjunto

$$\{Q_{j_1}, \ldots, Q_{j_{v'}}\},$$

incluyen a D_2. De estos, Q_{j_1} es el único que contiene a la vez a D_1 y a D_2, ya que si hubiera otro, digamos Q_{j_l}, entonces $Q_{j_1} \cap Q_{j_l}$ contendría a D_1 y a D_2, lo que es absurdo porque

$$|D_1| = |D_2| = |Q_{j_1} \cap Q_{j_l}| = p^{m-1}$$

y $D_1 \neq D_2$. Así, en $\{Q_{j_1}, \ldots, Q_{j_{v'}}\}$ hay $2p+1$ elementos que incluyen a D_1 o a D_2. Si $v' = 2p+1$ la demostración se termina aquí. Supongamos que $v' > 2p+1$, tomemos $Q_{j_{l_4}}$ tal que ni D_1 ni D_2 estén incluídos en $Q_{j_{l_4}}$ y escribamos $D_3 := Q_{j_1} \cap Q_{j_{l_4}}$. En $\{Q_{j_1}, \ldots, Q_{j_{v'}}\}$ hay $p+1$ elementos que contienen a D_3. Nuevamente Q_{j_1} es el único que contiene a D_1 y a D_3, y también es el único que contiene a D_2 y a D_3. Así, hay $3p+1$ elementos en $\{Q_{j_1}, \ldots, Q_{j_{v'}}\}$ que contienen a D_1, D_2 o D_3. Si $v' = 3p+1$ esto termina la demostración, y si no podemos continuar con este procedimiento hasta que todos los elementos de $\{Q_{j_1}, \ldots, Q_{j_{v'}}\}$ estén listados. □

Corolario 7.10. *Si p^m divide al orden de un grupo finito G, entonces la cantidad de subgrupos de G de orden p^m es congruente a 1 módulo p.*

Demostración. Tómese $H := 1$ en el teorema anterior. □

Observación 7.11. *Supongamos que N es un subgrupo normal de un p-grupo finito G. Fijemos $m < n$ tales que $p^m \leq |N|$ y $p^n \leq |G|$ y designemos con X al conjunto de los subgrupos de orden p^n de G que intersecan a N en un subgrupo de orden p^m (X puede ser vacío). Como N es normal, G actúa sobre X por conjugación. Los puntos fijos de X bajo esta acción son los subgrupos normales de G que pertenecen a X. Además $|X^G| \equiv |X| \pmod p$, puesto que $X \setminus X^G$ es una unión disjunta de órbitas no triviales, y por el Corolario 5.13 el cardinal de cada una de esta órbitas es una potencia positiva de p. En consecuencia,*

$$|\{P \in X : P \text{ es un subgrupo normal de } G\}| \equiv |X| \pmod p.$$

Por ejemplo, por el Teorema 7.9, si N un subgrupo normal de un p-grupo finito G y

$$|N| \leq p^n \leq |G|,$$

entonces la cantidad de subgrupos normales de G de orden p^n que contienen a N es congruente a 1 módulo p y, por el Teorema 7.1, la cantidad de subgrupos de orden p^n de un p-grupo finito G cuya intersección con $\mathrm{Z}\,G$ es 1, es un múltiplo de p.

Lema 7.12. *El grupo*

$$G_1 := \langle g, h | g^{p^2}, h^p, hgh^{-1}g^{-p-1} \rangle$$

tiene p^3 elementos.

Demostración. Es claro que el subgrupo $\langle g \rangle$ de G_1 es normal, $|g| \leq p^2$ y $|G_1/\langle g \rangle| \leq p$. Por lo tanto, $|G_1| \leq p^3$. Para probar que vale la desigualdad opuesta será suficiente exhibir un morfimo sobreyectivo de G_1 en un grupo de orden p^3. Tomemos grupos cíclicos $C_{p^2} = \langle x \rangle$ y $C_p = \langle y \rangle$ de orden p^2 y p, respectivamente. Como $(1+p)^p \equiv 1 \pmod{p^2}$ la aplicación

$$\begin{array}{ccc} C_{p^2} & \xrightarrow{\psi} & C_{p^2} \\ x^i & \longmapsto & x^{i(p+1)} \end{array},$$

es un automorfismo de orden p y, por consiguiente, la correspondencia

$$\begin{array}{ccc} C_p & \xrightarrow{\varsigma} & \mathrm{Aut}(C_{p^2}) \\ y^j & \longmapsto & \psi^j \end{array},$$

es un morfismo de grupos. Consideremos el producto semidirecto $C_{p^2} \rtimes_\varsigma C_p$ y escribamos $\hat{x} := (x, 1)$ e $\hat{y} := (1, y)$. Puesto que

$$\hat{x}^{p^2} = \hat{y}^p = 1 \qquad \text{e} \qquad \hat{y}\hat{x}\hat{y}^{-1} = \hat{x}^{p+1},$$

hay un morfismo $\xi\colon G_1 \to C_{p^2} \rtimes_\varsigma C_p$ tal que $\xi(g) = \hat{x}$ y $\xi(h) = \hat{y}$. Como ξ es sobreyectivo y $|C_{p^2} \rtimes_\varsigma C_p| = p^3$, esto termina la demostración. □

Lema 7.13. *El grupo*

$$G_2 := \langle g, h, k | g^p, h^p, k^p, hgh^{-1}g^{-1}, kgk^{-1}g^{-1}, khk^{-1}h^{-1}g\rangle$$

tiene p^3 elementos.

Demostración. Notemos que el subgrupo $\langle g\rangle$ de G_2 es normal, $|g| \leq p$ y $|G_2/\langle g\rangle| = p^2$. Por lo tanto, $|G_2| \leq p^3$. Tal como hicimos en el lema anterior, para probar que vale la desigualdad opuesta construiremos un morfismo sobreyectivo de G_2 en un grupo de orden p^3. Un cálculo sencillo muestra que la aplicación

$$\begin{array}{c} C_p \times C_p \xrightarrow{\ \psi\ } C_p \times C_p \ , \\ (y^i, y^j) \longmapsto (y^{i-j}, y^j) \end{array}$$

donde $C_p = \langle y\rangle$ es un grupo cíclico con p elementos, es un automorfismo de orden p, por lo que la correspondencia

$$\begin{array}{c} C_p \xrightarrow{\ \varsigma\ } \mathrm{Aut}(C_p \times C_p) \\ y^k \longmapsto \psi^k \end{array}$$

es un morfismo de grupos. Consideremos el producto semidirecto $(C_p \times C_p) \rtimes_\varsigma C_p$ y escribamos $\widehat{y}_1 = (y, 0, 0)$, $\widehat{y}_2 = (0, y, 0)$ y $\widehat{y}_3 = (0, 0, y)$. Puesto que

$$\hat{y}_1^p = \hat{y}_2^p = \hat{y}_3^p = 1, \quad \hat{y}_2\hat{y}_1 = \hat{y}_1\hat{y}_2, \quad \hat{y}_3\hat{y}_1 = \hat{y}_1\hat{y}_3 \quad \text{y} \quad \hat{y}_3\hat{y}_2 = \hat{y}_1^{-1}\hat{y}_2\hat{y}_3,$$

hay un morfismo $\xi\colon G_2 \to (C_p \times C_p) \rtimes_\varsigma C_p$ tal que $\xi(g) = \hat{y}_1$, $\xi(h) = \hat{y}_2$ y $\xi(k) = \hat{y}_3$. Como ξ es sobreyectivo y $|(C_p \times C_p) \rtimes_\varsigma C_p| = p^3$, esto termina la demostración. □

Nota 7.14. *En las demostraciones de los Lemas 7.12 y 7.13 se probó más que lo establecido en los enunciados. Específicamente, en la del primero se probó que G_1 es producto semidirecto interno de los subgrupos $\langle g\rangle$, de orden p^2, y $\langle h\rangle$, de orden p; mientras que, en la del segundo se probó que G_2 es producto semidirecto interno de los subgrupos $\langle g, h\rangle$, de orden p^2, y $\langle k\rangle$, de orden p.*

Teorema 7.15 (Caracterización de los grupos de orden p^3). *Para cada grupo G de orden p^3, vale que:*

1. *Si G es abeliano, entonces G es isomorfo a $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ o $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$.*
2. *Si G no es abeliano y $p = 2$, entonces G es isomorfo al grupo diedral D_4 o al grupo cuaterniónico H_2.*
3. *Si G no es abeliano y $p > 2$, entonces G es isomorfo al grupo G_1 presentado en el Lema 7.12, o al grupo G_2 presentado en el Lema 7.13.*

Demostración. Sabemos que G es cíclico si y sólo si tiene elementos de orden p^3. Supongamos que no lo es, pero que tiene un elemento g de orden p^2. Tomemos $h \in G \setminus \langle g\rangle$. Es evidente que $G = \langle g, h\rangle$. Además, por el Corolario 2.15 el subgrupo de G generado por g es

normal. En consecuencia $h^p \in \langle g\rangle$ y existe $1 \le r < p^2$ tal que $hgh^{-1} = g^r$. Consideramos por separado los casos $r = 1$ (i. e. G conmutativo) y $r > 1$

r = 1: Escribamos $h^p = g^j$ con $0 \le j < p^2$. Debido a que $1 = h^{p^2} = g^{pj}$, existe $0 \le t < p$ tal que $j = pt$. Reemplazando h por hg^{-t} podemos suponer que $h^p = 1$, lo cual implica que $\langle g\rangle \cap \langle h\rangle = 1$. Pero entonces, por el Teorema 15.1 del Capítuo 1 y la Proposición 15.14 de Capítulo 1,

$$G \simeq \langle g\rangle \times \langle h\rangle \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_p.$$

r > 1: Un argumento inductivo prueba que $h^i g h^{-i} = g^{r^i}$ para todo $i \ge 1$. En particular $g = h^p g h^{-p} = g^{r^p}$, por lo que $r^p \equiv 1 \pmod{p^2}$. Puesto que $(1+p)^p \equiv 1 \pmod{p^2}$ y $\mathbb{Z}_{p^2}^\times$ tiene un único subgrupo de orden p (pues es cíclico de orden $(p-1)p$), existe $0 < \alpha < p$ tal que $1 + p \equiv r^\alpha \pmod{p^2}$. Notemos que $h^\alpha \in G \setminus \langle g\rangle$ porque p no divide a α. Cambiando h por h^α podemos suponer que $r = 1 + p$, ya que

$$h^\alpha g h^{-\alpha} = g^{r^\alpha} = g^{1+p}.$$

Como en el caso $r = 1$, existe $0 \le t < p$ tal que $h^p = g^{tp}$. Ahora dividimos la demostración en dos partes, considerando por separado los subcasos $p = 2$ y $p > 2$.

p = 2: Las únicas posibilidades para h^2 son 1 o g^2. Si $h^2 = 1$, entonces G está generado por dos elementos g y h que satisfacen

$$g^4 = h^2 = 1 \quad \text{y} \quad hgh^{-1} = g^3$$

y, por lo tanto, $G \simeq D_4$, mientras que si $h^2 = g^2$, entonces G está generado por dos elementos g y h que satisfacen

$$g^4 = 1, \quad h^2 = g^2 \quad \text{y} \quad hgh^{-1} = g^3$$

y, por lo tanto, $G \simeq H_2$.

p > 2: Haciendo inducción primero en j y luego en i se verifica que $h^i g^j = g^{j(1+p)^i} h^i$. Usando esto es fácil comprobar por inducción en l que

$$(g^{-t(1+p)}h)^l = g^{-t(1+p)(1+\cdots+(1+p)^{l-1})} h^l = g^{-t(1+p)\frac{(1+p)^l-1}{p}} h^l.$$

En consecuencia

$$(g^{-t(1+p)}h)^p = g^{-t(1+p)\frac{(1+p)^p-1}{p}} h^p = g^{-t(1+p)p} h^p = g^{-tp} h^p = 1,$$

donde en la segunda igualdad hemos usado que $g^{p^2} = 1$ y que, debido a que $p > 2$, sabemos que $(1+p)^p \equiv 1 + p^2 \pmod{p^3}$. Como

$$(g^{-t(1+p)}h)g(g^{-t(1+p)}h)^{-1} = g^{-t(1+p)} h g h^{-1} g^{t(1+p)} = g^{-t(1+p)} g^{1+p} g^{t(1+p)} = g^{1+p},$$

reemplazando h por $g^{-t(1+p)}h$, vemos que G está generado por dos elementos g y h que satisfacen

$$g^{p^2} = h^p = 1 \quad \text{e} \quad hgh^{-1} = g^{1+p}$$

y, por lo tanto, $G \simeq G_1$.

Resta ver que sucede cuando todos los elementos no nulos de G tienen orden p. Nuevamente consideramos por separado los casos G conmutativo y G no conmutativo.

G es conmutativo: Tomemos $g \in G \setminus \{1\}$ arbitrario y $h, k \in G$ tales que sus clases en $G/\langle g\rangle$ generan $G/\langle g\rangle$. Como $\langle h, k\rangle\langle g\rangle = G$ y $\langle h\rangle \cap \langle k\rangle = 1$ se sigue de la Proposición 8.2 del Capítulo 1 y el Teorema 15.1 del Capítulo 1, que G es producto directo interno de los subgrupos $\langle g\rangle$, $\langle h\rangle$ y $\langle k\rangle$, y, en consecuencia, isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$.

G no es conmutativo: Por el Ejercicio 4.9 del Capítulo 1 y los Corolarios 7.4 y 7.5 sabemos que $p > 2$, que $\mathrm{Z}\,G = [G, G]$ es un subgrupo invariante de orden p de G, y que $G/\mathrm{Z}\,G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Tomemos $h, k \in G$ tales que sus clases en $G/\mathrm{Z}\,G$ generen $G/\mathrm{Z}\,G$. Entonces el conmutador

$$g = [h, k] = hkh^{-1}k^{-1} \in \mathrm{Z}\,G$$

es distinto de 1, porque de lo contrario $G = \langle h, k, \mathrm{Z}\,G\rangle$ sería conmutativo. Por consiguiente G está generado por los elementos g, h y k, los cuales satisfacen las relaciones

$$g^p = h^p = k^p = hgh^{-1}g^{-1} = kgk^{-1}g^{-1} = khk^{-1}h^{-1}g = 1,$$

y en consecuencia es isomorfo a G_2.

No habiendo más casos para considerar, la prueba está terminada. □

7.1. Grupos de orden 12

En esta pequeña subsección clasificamos los quepos de orden 12. Esto junto con los resultados que hemos obtenido anteriormente da una clasificación completa de los grpou de orden menor que 16. Ponemos este resultado al final de la sección de p-grupos finitos porque usamos en su prueba el Corolario 7.4.

PROPOSICIÓN 7.16. *Hay* 5 *grupos no isomorfos de orden* 12*, dos de ellos son los grupos abelianos* $\mathbb{Z}_4 \times \mathbb{Z}_3$ *y* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$*, otros dos son el grupo alternado* A_4 *y el grupo diedral* D_6 *y hay finalmente otro grupo que tiene la presentación* $\langle g, k | k^6, g^2k^{-3}, gkg^{-1}k\rangle$*.*

DEMOSTRACIÓN. Consideremos un grupo G de orden 12. Por el item 1) del teorema de Sylow y el Corolario 6.6, sabemos que $n_2 \in \{1, 3\}$ y $n_3 \in \{1, 4\}$, mientras que de la Proposición 6.23 se sigue que necesariamente $n_2 = 1$ o $n_3 = 1$. Si $n_1 = n_3 = 1$, entonces debido al la Nota 6.24, sabemos que G es el producto directo interno de sus subgrupos de sylow de orden 3 y 4 y, por lo tanto, G es abeliano. Por el Corolario 7.4, en este caso

$$G \simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \qquad \text{o} \qquad G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Supongamos ahora que G no es abeliano y que $n_3 = 4$. Tomemos un 3-subgrupo de Sylow Q de G. Como Q no es normal y Q es cíclico de orden 3 se sigue del Corolario 2.10, que hay un morfismo inyectivo de G en S_4. Así, por la Proposición 5.7 del Capítulo 2, en este caso, G es isomorfo a A_4. Supongamos ahora que $n_2 = 3$ y denotemos con P_1, P_2 y P_3 a los 2-subgrupo de Sylow de G y con Q al único 3-subgrupo de Sylow de G. Por el corolario 6.7 sabemos que Q es un subgrupo normal de G y que P_1, P_2 y P_3 no lo son. Denotemos con H al máximo subgrupo de P_1 que es normal en G. Afirmamos que H tiene orden 2. Ya vimos que $H \subsetneq P_1$. Afirmamos que H tampoco es 1. En efecto, en este caso, por Corolario 2.10, el grupo G sería isomorfo a un subgrupo de S_4, lo cual, debido a la Proposición 5.7 del Capítulo 2 y el Ejemplo 6.14, es imposible. Además, por la Nota 6.8, la intersección de los P_i's coincide con H y, por el Corolario 15.2 del Capítulo 1, los subgrupos H y Q de G están en producto directo. Tomemos generadores h de H y q de Q. Es evidente que $k := hq$ genera HQ y tiene orden 6. Dado que H y Q son subgrupos normales de G, también HQ lo es (esto también ocurre

porque HQ tiene índice 2 en G). Además $P_1 \nsubseteq HQ$ pues $P_1Q = G$. Tomemos $g \in P_1 \setminus HQ$ arbitrario. Entonces

$$G = HQ\langle g\rangle = \{1, k, k^2, k^3, k^4, k^5, g, kg, k^2g, k^3g, k^4g, k^5g\},$$

donde la última igualdad se sigue de que 1, k, k^2, k^3, k^4, k^5, g, kg, k^2g, k^3g, k^4g y k^5g son todos distintos. Como $g^2 \in P_1 \cap HQ$ (pues HQ tiene índice 2) y tiene orden 1 o 2, y $gkg^{-1} \in HQ$ tiene orden 6 y es diferente de k (pues G no es conmutativo), necesariamente

$$g^2 \in \{1, k^3\} \qquad \text{y} \qquad gkg^{-1} = k^{-1}.$$

Por lo tanto

$$G = \langle g, k | k^6, g^2, gkg^{-1}k\rangle \qquad \text{o} \qquad G = \langle g, k | k^6, g^2k^{-3}, gkg^{-1}k\rangle. \tag{32}$$

Notemos que el primero de estos grupos es isomorfo al grupo diedral D_6 y que ninguno de ellos es isomorfo a A_4 (por el item 1) de la Proposición 5.7 y por que en ellos k genera un subgrupo de orden 6). Finalmente los grupos que aparecen en (32) no pueden ser isomorfos porque tienen 2-subgrupos de Sylow no isomorfos. En efecto como vimos en el Ejemplo 6.16 los del primero son isomorfos a $D_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$, mientras que en el segundo son cíclicos de orden 4 (pues de $g^2 = k^3$ se sigue que g tiene orden 4). □

NOTA 7.17. *Tal vez el lector no esté convencido de la existencia del segundo de los grupos que aparenen en* (32)*. Si es así tiene razón en no estarlo ya que no hemos dado ninguna construcción explícita del mismo. Hay una técnica para construír este grupo (y muchos otros) que consiste en una generalización del producto semidirecto externo llamado producto cruzado. También se puede probar por cálculo directo que el conjunto*

$$\{1, k, k^2, k^3, k^4, k^5, g, kg, k^2g, k^3g, k^4g, k^5g\},$$

provisto de la operación dada por

$$k^ik^j = k^{i+j}, \quad k^ik^jg = k^{i+j}g, \quad k^igk^j = k^{i-j}g \quad y \quad k^igk^jg = k^{i-j+3}$$

donde $0 \le i, j < 6$ *y las operaciones en los exponentes son realizadas en* $\mathbb{Z}_6$*, es un grupo.*

Capítulo 4

Grupos resolubles y nilpotentes

Una *serie normal* de *longitud* m de un grupo G es una sucesión de subgrupos

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m,$$

de G, tales que $G_0 = 1$, $G_m = G$ y $G_i \triangleleft G_{i+1}$ para todo $i < m$. Los *grupos factores* son los cocientes G_{i+1}/G_i. Notemos que la longitud es la cantidad de grupos factores o, lo que es igual, la cantidad de inclusiones. Consideremos dos series normales

$$G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_m \qquad \text{y} \qquad H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft N_n$$

de G. Decimos que la primera *refina* a la segunda si existen índices $1 \leq i_1 < \cdots < i_n \leq m$ tales que $G_{i_j} = H_j$ para todo j, y que ambas son *equivalentes* si $m = n$ y existe una permutación $\sigma \in \mathrm{S}_m$ tal que $\frac{G_i}{G_{i-1}} \simeq \frac{G_{\sigma(i)}}{G_{\sigma(i)-1}}$, para todo i entre 1 y m (esto es, si tienen los mismos grupos factores y cada uno aparece la misma cantidad de veces en ambas).

Una *serie de composición* de un grupo G es una serie normal de G cuyos factores son simples. Es evidente que cada grupo finito tiene una serie de composición.

Lema 0.1 (Lema de la Mariposa). *Si $H_1 \triangleleft H_2$ y $G_1 \triangleleft G_2$ son subgrupos de un grupo G, entonces*

$$H_1(H_2 \cap G_1) \triangleleft H_1(H_2 \cap G_2), \quad (H_1 \cap G_2)(H_2 \cap G_1) \triangleleft H_2 \cap G_2, \quad G_1(H_1 \cap G_2) \triangleleft G_1(H_2 \cap G_2),$$

y hay isomorfismos canónicos

$$\frac{H_1(H_2 \cap G_2)}{H_1(H_2 \cap G_1)} \simeq \frac{H_2 \cap G_2}{(H_1 \cap G_2)(H_2 \cap G_1)} \simeq \frac{G_1(H_2 \cap G_2)}{G_1(H_1 \cap G_2)}.$$

Demostración. Escribamos

$$K = H_1(H_2 \cap G_1) \quad \text{y} \quad N = H_2 \cap G_2.$$

Como $H_1 \triangleleft H_2$, sabemos que K es un subgrupo de G. Además, $N \subseteq \mathrm{N}_G(K)$ y, por consiguiente, KN es un subgrupo de G y $K \triangleleft KN$. En consecuencia $(N \cap K) \triangleleft N$ y $N/(N \cap K)$

es canónicamente isomorfo a KN/K. Como $KN = H_1(H_2 \cap G_2)$ y, por el item 1) de la Proposición 8.1 del Capítulo 1,

$$N \cap K = (H_1 \cap G_2)(H_2 \cap G_1),$$

concluímos que

$$(H_1 \cap G_2)(H_2 \cap G_1) \lhd H_2 \cap G_2, \quad H_1(H_2 \cap G_1) \lhd H_1(H_2 \cap G_2)$$

y que el primer isomorfismo existe. El resto sale por simetría. □

TEOREMA 0.2 (Schreier). *Dos series normales de un grupo G siempre se pueden refinar a series equivalentes.*

DEMOSTRACIÓN. Consideremos dos series normales

$$G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_m \qquad \text{y} \qquad H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_n$$

de G. Escribamos

$$G_{ij} = G_{j-1}(H_i \cap G_j) \qquad \text{y} \qquad H_{ij} = H_{i-1}(H_i \cap G_j),$$

dónde en cada caso los subíndices recorren todos los valores para los cuales la expresión a la derecha del signo igual tiene sentido. Intercalando los G_{ij} en la primer serie y los H_{ij} en la segunda, obtenemos cadenas

$$G_0 = G_{01} \subseteq G_{11} \subseteq \cdots \subseteq G_{n1} = G_1 = G_{02} \subseteq \cdots \subseteq G_{nm} = G_m$$

y

$$H_0 = H_{10} \subseteq H_{11} \subseteq \cdots \subseteq H_{1m} = H_1 = H_{20} \subseteq \cdots \subseteq H_{nm} = H_n,$$

donde no necesariamente las inclusiones son propias. Por el lema de la Mariposa cada uno de los subgrupos que aparecen en estas cadenas es normal en el que le sigue y

$$\frac{G_{ij}}{G_{i-1,j}} \simeq \frac{H_{ij}}{H_{i,j-1}} \quad \text{para } 1 \leq i \leq n \text{ y } 1 \leq j \leq m.$$

El resultado es consecuencia inmediata de esto. □

TEOREMA 0.3 (Jordan-Hölder). *Si G tiene una serie de composición, entonces toda serie normal y estrictamente creciente de G se puede refinar a una serie de composición. Además todas las series de composición de G son equivalentes y, en particular, tienen la misma longitud.*

DEMOSTRACIÓN. Es un corolario inmediato del teorema de Schreier. □

A los grupos factores de una serie de composición de G se los denomina *factores de composición* de G.

Definimos la *longitud* $\ell(G)$ de un grupo G, por

$$\ell(G) := \begin{cases} 0 & \text{si } G = 1, \\ n & \text{si } G \text{ tiene una serie de composición de longitud } n, \\ \infty & \text{en otro caso.} \end{cases}$$

Por el teorema de Jordan Hölder, esta definición no es ambigua.

TEOREMA 0.4. *Si N es un subgrupo normal de G, entonces G tiene una serie de composición si y sólo si N y G/N la tienen. Además, $\ell(G) = \ell(N) + \ell(G/N)$.*

DEMOSTRACIÓN. Evidentemente podemos suponer que N es un subgrupo no trivial de G. Es claro que si G tiene una serie de composición, entonces refinando la serie normal $1 \lhd N \lhd G$ a una serie de composición

$$1 = N_0 \lhd \cdots \lhd N_i = N \lhd \cdots \lhd N_m = G, \tag{33}$$

obtenemos series de composición

$$1 = N_0 \lhd \cdots \lhd N_i = N \qquad \text{y} \qquad 1 = \frac{N_i}{N} \lhd \cdots \lhd \frac{N_m}{N} = \frac{G}{N}, \tag{34}$$

de N y G/N, respectivamente. Notemos que además

$$\ell(G) = m = i + (m - i) = \ell(N) + \ell(G/N).$$

Recíprocamente, si G tiene un subgrupo normal N tal que N y G/N tienen series de composición como (34), combinándolas se obtiene una serie de composición como (33). □

TEOREMA 0.5 (Teorema de la dimensión). *Supongamos que H_1 y H_2 son subgrupos de un grupo G y que H_1 normaliza a H_2 o H_2 normaliza a H_1. Entonces $\ell(H_1)$ y $\ell(H_2)$ son finitos si y sólo si $\ell(H_1H_2)$ y $\ell(H_1 \cap H_2)$ lo son y, además,*

$$\ell(H_1H_2) + \ell(H_1 \cap H_2) = \ell(H_1) + \ell(H_2).$$

DEMOSTRACIÓN. Por simetría podemos suponer que H_1 normaliza a H_2. En este caso basta aplicar el teorema anterior a los subgrupos y grupos cocientes que aparecen en las sucesiones exactas cortas

$$1 \longrightarrow H_1 \cap H_2 \longrightarrow H_1 \longrightarrow \frac{H_1}{H_1 \cap H_2} \longrightarrow 1$$

y

$$1 \longrightarrow H_2 \longrightarrow H_1H_2 \longrightarrow \frac{H_1H_2}{H_2} \longrightarrow 1\ ,$$

y usar que $\frac{H_1}{H_1 \cap H_2} \simeq \frac{H_1H_2}{H_2}$. □

Del teorema de Jorden-Hölder se sigue la parte de la unicidad del Teorema fundamental de la aritmética. En efecto si $n = p_1 \dots p_n$ es una factorización de un número natural n y $\langle g \rangle$ es un grupo cíclico de orden n, entonces

$$1 \lhd \langle g^{p_2 \cdots p_n} \rangle \lhd \langle g^{p_3 \cdots p_n} \rangle \lhd \cdots \lhd \langle g^{p_{n-1}p_n} \rangle \lhd \langle g^{p_n} \rangle \lhd \langle g \rangle$$

es una serie de composición de $\langle g \rangle$. Como los grupos factores de esta serie tienen ordenes $p_1, \dots, p_n$, estos números dependen sólo de n.

1. Grupos resolubles

Una *serie resoluble* de un grupo G es una serie normal

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_m = G$$

tal que sus grupos factores son conmutativos. Un grupo G es *resoluble* si tiene una serie resoluble. Es evidente que todo grupo abeliano es resoluble.

PROPOSICIÓN 1.1. *Un grupo resoluble tiene una serie de composición si y sólo si es finito.*

DEMOSTRACIÓN. Por el teorema de Schreier los grupos factores de una serie de composición de un grupo resoluble son grupos abelianos simples, los cuales son los grupos cíclicos finitos de orden primo. En consecuencia, todo grupo resoluble con una serie de composición es finito. La afirmación recíproca es obvia. □

El siguiente es un ejemplo no trivial de grupo resoluble.

EJEMPLO 1.2. *Consideremos un K-espacio vectorial de dimensión finita V. Fijemos una sucesión de subespacios*

$$V = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_{n-1} \supsetneq V_n = \{0\}$$

tal que $\operatorname{codim}_k V_i = i$. *Escribamos*

$$G = \{f \in \operatorname{Aut}_k(V) : f(V_i) = V_i \text{ para todo } i\}.$$

Es evidente que G es un grupo vía la composición. Vamos a probar que es resoluble. Con este objetivo definimos una sucesión $(H_i)_{0\le i\le n}$ de subgrupos de G, por

$$H_i = \{f \in G : (f - \mathrm{id})(V_j) \subseteq V_{i+j} \text{ para todo } j \le n - i \ \}.$$

Por ejemplo $H_0 = G$ y $H_n = \mathrm{id}$. Para ver que los H_i son en verdad subgrupos de G basta observar que:

- $\mathrm{id} \in H_i$ *para todo* i,
- *Si $f \in H_i$, entonces $f^{-1} \in H_i$ para todo $f \in G$ porque*

$$(f^{-1} - \mathrm{id})(V_j) = f^{-1}(\mathrm{id} - f)(V_j) \subseteq f^{-1}(V_{i+1}) = V_{i+1}$$

  para todo $j \le n - i$,
- *Si $f, g \in H_i$, entonces $f \circ g \in H_i$, porque*

$$\begin{aligned}(f \circ g - \mathrm{id})(V_j) &= (f \circ g - g + g - \mathrm{id})(V_j)\\ &\subseteq (f - \mathrm{id}) \circ g(V_j) + (g - \mathrm{id})(V_j)\\ &\subseteq V_{i+j}\end{aligned}$$

  para todo $j \le n - i$.

Afirmamos que $[H_j, H_k] \subseteq H_{j+k}$ para todos los $j, k \le n$ con $0 \le j + k \le n$. En efecto, para cada $f \in H_j$, $g \in H_k$ y $x \in V_i$, existen $u_{ij} \in V_{i+j}$, $v_{ik} \in V_{i+k}$ y $w_{ijk}, w'_{ijk} \in V_{i+j+k}$ tales que

$$f(x) = x + u_{ij}, \quad g(x) = x + v_{ik}, \quad f(v_{ik}) = v_{ik} + w'_{ijk} \quad y \quad g(u_{ij}) = u_{ij} + w_{ijk}.$$

Entonces

$$g(f(x)) = x + v_{ik} + u_{ij} + w_{ijk} \qquad y \qquad f(g(x)) = x + u_{ij} + v_{ik} + w'_{ijk}.$$

En consecuencia $g(f(x)) = f(g(x)) \pmod{V_{i+j+k}}$ y, por lo tanto,

$$g^{-1} \circ f^{-1} \circ g \circ f(x) \pmod{V_{i+j+k}}.$$

En particular

1. *$[H_0, H_i] \subseteq H_i$ para $0 \le i \le n$, por lo que cada H_i es normal en $H_0 = G$.*
2. *$[H_i, H_i] \subseteq H_{2i} \subseteq H_{i+1}$ para $1 \le i < n$, por lo que H_i/H_{i+1} es abeliano para $1 \le i < n$.*

Para terminar la demostración debemos ver que H_0/H_1 es abeliano, para lo cual es suficiente probar que $[H_0, H_0] \subseteq H_1$. Tomemos $f, g \in H_0$ y $x \in V_i \setminus V_{i+1}$. Como $V_i = Kx \oplus V_{i+1}$, $f(V_i) \subseteq V_i$ y $G(V_i) \subseteq V_i$, existen $\alpha, \beta \in K$ tales que

$$f(x) \in \alpha \cdot x + V_{i+1} \qquad y \qquad g(x) \in \beta \cdot x + V_{i+1}.$$

Dado que además $f(V_{i+1}) \subseteq V_{i+1}$ y $G(V_{i+1}) \subseteq V_{i+1}$,

$$g \circ f \circ g^{-1} \circ f^{-1}(x) \in \alpha\beta\alpha^{-1}\beta^{-1} \cdot x + V_{i+1} = x + V_{i+1}$$

y, por consiguiente, $[g, f] \in H_1$

TEOREMA 1.3. *Cada subgrupo H de un grupo resoluble G es resoluble.*

DEMOSTRACIÓN. Tomemos una serie resoluble

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

de G, y consideremos la serie

$$1 = H_0 \subseteq H \cap G_1 \subseteq \cdots \subseteq H \cap G_n = H.$$

Para probar el teorema es suficiente observar que $H \cap G_i \lhd H \cap G_{i+1}$ y

$$\frac{H \cap G_{i+1}}{H \cap G_i} = \frac{H \cap G_{i+1}}{(H \cap G_{i+1}) \cap G_i} \simeq \frac{G_i(H \cap G_{i+1})}{G_i} \subseteq \frac{G_{i+1}}{G_i},$$

para todo i. □

TEOREMA 1.4. *El grupo de permutaciones S_n no es resoluble para ningún $n \geq 5$.*

DEMOSTRACIÓN. Como el grupo alternado A_n es simple y no conmutativo, no es resoluble. En consecuencia, por el Teorema 1.3, tampoco lo es S_n. □

TEOREMA 1.5. *Dada una sucesión exacta corta de grupos*

$$1 \longrightarrow H \xrightarrow{\iota} G \xrightarrow{\pi} L \longrightarrow 1\ ,$$

el grupo G es resoluble si y sólo si H y L lo son.

DEMOSTRACIÓN. Supongamos que G es resoluble. Por el teorema anterior sabemos que H es resoluble. Para comprobar que L también lo es basta observar que si

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

es una serie resoluble de G, entonces $\pi(G_i) \lhd \pi(G_{i+1})$ y

$$\frac{\pi(G_{i+1})}{\pi(G_i)} \simeq \frac{\iota(H)G_{i+1}}{\iota(H)G_i} = \frac{\iota(H)G_iG_{i+1}}{\iota(H)G_i} \simeq \frac{G_{i+1}}{\iota(H)G_i \cap G_{i+1}} \simeq \frac{G_{i+1}/G_i}{(\iota(H)G_i \cap G_{i+1})/G_i}$$

es conmutativo, para todo $i < n$. Recíprocamente, si

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = H$$

es una serie resoluble de H y

$$1 = L_0 \lhd L_1 \lhd \cdots \lhd L_m = L$$

es una serie resoluble de L, entonces

$$1 = \iota(H_0) \lhd \iota(H_1) \lhd \cdots \lhd \iota(H_n) = H = \pi^{-1}(L_0) \lhd \pi^{-1}(L_1) \lhd \cdots \lhd \pi^{-1}(L_m) = G$$

es una serie resoluble de G. □

COROLARIO 1.6. *Si H y K son grupos resolubles, entonces también lo es cada producto semidirecto de H con K. En particular los grupos diedrales son resolubles.*

Decimos que una clase $\mathcal{C}$ de grupos es *cerrada bajo extensiones* si para cada sucesión exacta corta

$$1 \longrightarrow H \xrightarrow{\iota} G \xrightarrow{\pi} L \longrightarrow 1 \ ,$$

con $H, L \in \mathcal{C}$, el grupo G pertenece a $\mathcal{C}$. Se comprueba sin dificultad que toda clase $\mathcal{C}$ cerrada bajo extensiones es cerrada bajo isomorfismos. En otras palabras si $G \in \mathcal{C}$ y $H \simeq G$, entonces $H \in \mathcal{C}$. El Teorema 1.5 dice en particular que la clase de los grupos resolubles es cerrada bajo extensiones [1]. Enseguida veremos que es la más pequeña de estas clases que contiene a todos los grupos abelianos. Para probar esto introducimos primero una noción importante, que da una medida de cuanto se aleja un grupo resoluble de ser abeliano, y que permite hacer demostraciones por inducción. La *clase de resolubilidad* de un grupo resoluble G es el mínimo n tal que G tiene una serie resoluble

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

de longitud n, pero no tiene ninguna serie resoluble de longitud menor. Por ejemplo, un grupo G es abeliano si y sólo si su clase de resolubilidad es menor o igual que 1 (el único grupo con clase de resolubilidad 0 es el trivial).

TEOREMA 1.7. *Si una clase $\mathcal{C}$ de grupos es cerrada bajo extensiones y contiene a todos los grupos abelianos, entonces contiene a todos los grupos resolubles.*

DEMOSTRACIÓN. Tomemos un grupo resoluble G. Si G tiene clase de resolubilidad menor o igual que 1, entonces es abeliano y, por lo tanto, pertenece a $\mathcal{C}$. Supongamos que G tiene clase de resolubilidad $n > 1$ y que $\mathcal{C}$ contine a todos los grupos con clase de resolubilidad menor que n. Consideremos una serie resoluble

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

de G. Por hipótesis inductiva G_{n-1} y G/G_{n-1} pertenecen a $\mathcal{C}$, pero entonces, como la sucesión

$$1 \longrightarrow G_{n-1} \xrightarrow{\iota} G \xrightarrow{\pi} G/G_{n-1} \longrightarrow 1 \ ,$$

donde ι es la inclusión canónica y π es proyección al cociente, es exacta, también $G \in \mathcal{C}$. □

TEOREMA 1.8. *Supongamos que H y L son subgrupos de un grupo G y que H normaliza a L. Entonces H y L son resolubles si y sólo si HL y $H \cap L$ lo son.*

DEMOSTRACIÓN. Basta aplicar el Teorema 1.5 a las sucesiones exactas

$$1 \longrightarrow H \cap L \longrightarrow H \longrightarrow \frac{H}{H \cap L} \longrightarrow 1$$

y

$$1 \longrightarrow L \longrightarrow HL \longrightarrow \frac{HL}{L} \longrightarrow 1,$$

y usar que $H/(H \cap L) \simeq HL/L$. □

[1] Lo que dice exáctamente, es que es cerrada bajo las operaciones de tomar subgrupos, cociente y sucesiones exactas cortas.

OBSERVACIÓN 1.9. *Por el Teorema 1.8, todo grupo finito G tiene un máximo subgrupo normal y resoluble N. Además, por el Teorema 1.5, ningún subgrupo no trivial de G/N es normal y resoluble.*

La *serie derivada* de un grupo G es la serie de subgrupos

$$G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots,$$

definida recursivamente por $G^{(0)} = G$ y $G^{(n+1)} = [G^{(n)}, G^{(n)}]$ para todo $n \geq 0$. Por la Proposición 18.18 del Capítulo 1, cada uno de los grupos derivados $G^{(n)}$ no sólo es un subgrupo normal del anterior, sino que es un subgrupo completamente normal de G. Notemos además que todos los cocientes $G^{(n)}/G^{(n+1)}$ son abelianos.

EJEMPLO 1.10. *Por el Teorema 5.1 del Capítulo 2 y la Observación 5.2 del Capítulo 2, las series derivadas de S_2, S_3, S_4 y S_n con $n \geq 5$ son*

$$\mathrm{S}_2 \triangleright 1, \quad \mathrm{S}_3 \triangleright \mathrm{A}_3 \triangleright 1, \quad \mathrm{S}_4 \triangleright \mathrm{A}_4 \triangleright H \triangleright 1 \quad y \quad \mathrm{S}_n \triangleright \mathrm{A}_n \triangleright \mathrm{A}_n \triangleright \cdots \text{ si } n \geq 5,$$

donde $H = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3), \mathrm{id}\}$.

EJEMPLO 1.11. *Recordemos que D_n es el grupo generado por dos elementos x, y sujetos a las relaciones $x^n = 1$, $y^2 = 1$ e $yxy^{-1}x = 1$, y que H_n es el grupo generado por dos elementos x, y sujetos a las relaciones $x^n y^{-2} = 1$ y $yxy^{-1}x = 1$. Por el Ejemplo 18.17 del Capítulo 1, las series derivadas de D_n (para $n > 2$) y H_n son*

$$D_n \triangleright \langle x^2 \rangle \triangleright 1 \qquad y \qquad H_n \triangleright \langle x^2 \rangle \triangleright 1,$$

respectivamente.

PROPOSICIÓN 1.12. *Si los grupos factores de una sucesión*

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots$$

son abelianos, entonces $G^{(n)} \subseteq G_n$ para todo n.

DEMOSTRACIÓN. Por inducción en n. El caso $n = 0$ es trivial. Supongamos que el resultado es cierto para n, de manera de que $G^{(n)} \subseteq G_i$. Como G_n/G_{n+1} es comutativo $[G_n, G_n] \subseteq G_{n+1}$ y, en consecuencia, $G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i] \subseteq G_{i+1}$. □

TEOREMA 1.13. *Un grupo G es resoluble si y sólo si $G^{(n)} = 1$ para algún $n \geq 0$.*

DEMOSTRACIÓN. Si $G^{(n)} = 1$, entonces la serie derivada de G es una serie resoluble. Recíprocamente, si G tiene una serie resoluble

$$G = G_0 \triangleright G_1 v \triangleright \cdots \triangleright G_n = 1,$$

entonces $G^{(n)} = 1$, por la Proposición 1.12 anterior. □

Es evidente que la clase de resolubilidad de un grupo resoluble es el mínimo n tal que $G^{(n)} = 1$. Los cálculos hechos en los Ejemplos 1.10 y 1.11 muestran que la clase de resolubilidad de los grupos S_2, A_3, S_3, A_4 y S_4 es 1, 1, 2, 2 y 3 respectivamente (los primeros dos son abelianos) y la de los grupos diedral D_n y cuaterniónico generalizado H_n es 2.

OBSERVACIÓN 1.14. *Usando el Teorema 1.13 es posible dar demostraciones alternativas de los Teoremas 1.3 y 1.5. Para el primero basta observar que si H es un subgrupo de G, entonces $H^{(n)} \subseteq G^{(n)}$ para todo $i \geq 0$. Además es fácil probar por inducción que si $\pi\colon G \to L$ es un epimorfismo de grupos, entonces $L^{(n)} = \pi(G^{(n)})$ para todo $n \geq 0$. La primera parte del Teorema 1.5 es consecuencia inmediata de esto. Para probar la segunda notemos que si*

$H^{(m)} = 1$, $L^{(n)} = 1$ y G es una extensión de H por L, entonces $G^{(n)} \subseteq H$ debido a que $\pi(G^{(n)}) = L^{(n)} = 1$ y, por lo tanto, $G^{(n+m)} = (G^{(n)})^{(m)} \subseteq H^{(m)} = 1$.

En realidad las demostraciones de los Teoremas 1.3 y 1.5 dadas en la observación anterior prueban que valen las siguientes versiones más precisas de los resultados establecidos en los enunciados de los mismos: todo subgrupo y todo cociente de un grupo resoluble de clase n es resoluble de clase menor o igual que n y si G es una extensión de un grupo resoluble H por otro L, entonces G es resoluble de clase menor o igual que la suma de las clases de H y L.

TEOREMA 1.15. *Para todo grupo G son equivalentes:*

1. *G es resoluble de clase menor o igual que n.*
2. *$G^{(n)} = 1$.*
3. *G tiene un subgrupo normal y abeliano H tal que G/H es resoluble de clase menor o igual que $n - 1$.*

DEMOSTRACIÓN. 1) $\Leftrightarrow$ 2) Es trivial.

2) $\Rightarrow$ 3) Es claro que se puede tomar $H = G^{(n-1)}$.

3) $\Rightarrow$ 1) Por el comentario que precede a este teorema, y porque la clase de resolubilidad de H es menor o igual que 1. □

EJERCICIO 1.16. *Pruebe que si G tiene un subgrupo $H \neq 1$ que satisface $H^{(1)} = H$, entonces G no es resoluble. Pruebe también que si G es finito y no resoluble, entonces G tiene un subgrupo completamente normal $H \neq 1$ que satisface $H^{(1)} = H$.*

Grupos hiperresolubles Una serie *superresoluble* de un grupo G es una cadena

$$1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_m = G$$

de subgrupos normales de G tal que los grupos factores son cíclicos. Un grupo G es *superresoluble* si tiene una serie superresoluble. Es evidente que si un grupo G es superresoluble, entonces G tiene un subgrupo cíclico normal no nulo. Como toda serie superresoluble es resoluble, todo grupo superresoluble es resoluble. La recíproca no vale. Por ejemplo, S_4 es resoluble, pero no es superresoluble, porque ninguno de sus subgrupos cíclicos no triviales es normal, como se comprueba fácilmente.

TEOREMA 1.17. *La clase de los grupos superresolubles tiene las siguientes propiedades:*

1. *Cada subgrupo H de un grupo superresoluble G es superresoluble.*
2. *Si $\pi\colon G \to L$ es un epimorfismo y G es superresoluble, entonces L también lo es.*
3. *Supongamos que*

$$1 \longrightarrow H \xrightarrow{\iota} G \xrightarrow{\pi} L \longrightarrow 1$$

es una sucesión exacta corta y que H es un subgrupo característico de G. Si H y L son superresolubles, entonces G también lo es.

DEMOSTRACIÓN. 1) Tomemos una serie superresoluble

$$1 = G_0 \subseteq \cdots \subseteq G_n = G$$

de G y consideremos la serie

$$1 = H_0 \subseteq H \cap G_1 \subseteq \cdots \subseteq H \cap G_n = H.$$

Para concluir que vale el item 1) es suficiente observar que $H \cap G_i \lhd H \cap G = H$ y

$$\frac{H \cap G_{i+1}}{H \cap G_i} = \frac{H \cap G_{i+1}}{(H \cap G_{i+1}) \cap G_i} \simeq \frac{G_i(H \cap G_{i+1})}{G_i} \subseteq \frac{G_{i+1}}{G_i},$$

para todo i.

Basta observar que para cada serie superresoluble

$$1 = G_0 \subseteq \cdots \subseteq G_n = G$$

de G, la cadena

$$1 = \pi(G_0) \subseteq \pi(G_1) \subseteq \cdots \subseteq \pi(G_n) = L$$

es una serie superresoluble de L porque $\pi(G_i) \lhd L$ y

$$\frac{\pi(G_{i+1})}{\pi(G_i)} \simeq \frac{HG_{i+1}}{HG_i} = \frac{HG_iG_{i+1}}{HG_i} \simeq \frac{G_{i+1}}{HG_i \cap G_{i+1}} \simeq \frac{G_{i+1}/G_i}{(HG_i \cap G_{i+1})/G_i},$$

donde H denota a el núcleo de π, para todo $i < n$.

3) por la Observación 18.14 del Capítulo 1, si

$$1 = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = H$$

es una serie superresoluble de H y

$$1 = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = L$$

es una serie superresoluble de L, entonces

$$1 = \iota(H_0) \subseteq \cdots \subseteq \iota(H_n) = H = \pi^{-1}(L_0) \subseteq \pi^{-1}(L_1) \subseteq \cdots \subseteq \pi^{-1}(L_m) = G$$

es una serie superresoluble de G. □

2. Grupos nilpotentes

La *serie central descendente* de un grupo G es la serie de subgrupos

$$G^0 \supseteq G^1 \supseteq G^2 \supseteq \cdots,$$

definida recursivamente por $G^0 = G$ y $G^{n+1} = [G, G^n]$ para todo $n \geq 0$. Por la Proposición 18.18 del Capítulo 1, G^n es un subgrupo completamente normal de G, para cada $n \geq 0$. Notemos además que por la Observación 18.19 del Capítulo 1,

$$\frac{G^i}{G^{i+1}} \subseteq \mathrm{Z}\left(\frac{G}{G^{i+1}}\right) \qquad \text{para todo } i \geq 0.$$

Decimos que G es nilpotente si existe $n \geq 0$ tal que $G^n = 1$. Al mínimo n que satisface esta igualdad se lo llama la *clase de nilpotencia de* G. Por ejemplo G es abeliano si y sólo su clase de nilpotencia es menor o igual que 1 (el único grupo que tiene clase de nilpotencia 0 es el trivial). Un argumento inductivo muestra que $G^{(i)} \subseteq G^i$ para todo $i \geq 0$, de modo que todo grupo nilpotente es resoluble y su clase de resolubilidad es menor o igual que su clase de nilpotencia.

Proposición 2.1. *La clase de grupos nilpotentes es cerrada bajo las operaciones de tomar subgrupos, cocientes y productos directos finitos.*

DEMOSTRACIÓN. Consideremos un grupo G, un subgrupo H de G y un par de grupos K y L. Denotemos con $\pi\colon G \to G/H$ a la proyección canónica. Es fácil probar por inducción en i que $H^i \leq G^i$, $(K \times L)^i = K^i \times H^i$ y $\pi(G)^i = \pi(G^i)$ para todo i. Las afirmaciones hechas en el enunciado son consecuencia inmediata de estas propiedades. □

De la demostración se sigue que las clases de nilpotencia de un subgrupo y de un cociente de un grupo son menores o igual que la del grupo, y que la clase de nilpotencia de en producto de dos grupos nilpotentes es el máximo de las clases de nilpotencia de sus factores.

Una sucesión descendente

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots$$

de subgrupos de un grupo G es *central* si $G_i/G_{i+1} \subseteq \mathrm{Z}(G/G_{i+1})$ para todo i.

PROPOSICIÓN 2.2. *Si*

$$G = G_1 \triangleright G_2 \triangleright G_3 \triangleright \cdots$$

es una sucesión central de subgrupos de G, entonces $G^i \subseteq G_i$ para todo i.

DEMOSTRACIÓN. Lo probaremos por inducción en i. Para $i = 0$ es trivial. Supongamos que es cierto para un $i \geq 0$, y veamos que lo es para $i + 1$. Por la Observación 18.19 del Capítulo 1, como $G_i/G_{i+1} \subseteq \mathrm{Z}(G/G_{i+1})$, el subgrupo $[G, G_i]$ de G está incluído en G_{i+1} y, en consecuencia,

$$G^{i+1} = [G, G^i] \subseteq [G, G_i] \subseteq G_{i+1}.$$

como queremos. □

TEOREMA 2.3. *Para cada grupo G son equivalentes:*

1. *G es nilpotente de clase menor o igual que n.*
2. *Existe una serie normal*

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

   que es central.
3. *G tiene un subgrupo $N \subseteq \mathrm{Z}\,G$ tal que G/N es nilpotente de clase menor o igual que $n - 1$.*
4. *G tiene un subgrupo K que contiene a $[G, G]$ y que es nilpotente de clase menor o igual que $n - 1$.*

DEMOSTRACIÓN. 1) $\Leftrightarrow$ 2) Como es evidente que 1) $\Rightarrow$ 2), basta probar que 2) $\Rightarrow$ 1), lo que se sigue de inmediato de la Proposición 2.2.

1) $\Rightarrow$ 3) Es fácil ver que se puede tomar $N = G_{n-1}$.

3) $\Rightarrow$ 1) Consideremos la proyección canónica $\pi\colon G \to G/N$. Usando que $\varphi[H, L] = [\varphi H, \varphi L]$ para cada par de subgrupos H, L de G y cada morfismo $\varphi\colon G \to G'$, es fácil probar por inducción que

$$\left(\frac{G}{N}\right)^i = (\pi G)^i = \pi(G^i) = \frac{G^i N}{N}$$

para todo i. Como, por hipótesis, $(G/N)^{n-1} = 1$, esto implica que $G^{n-1}N = N$. Pero entonces $G^{n-1} \subseteq \mathrm{Z}\,N$ y, por lo tanto, $G^n = 1$.

1) $\Rightarrow$ 4) Es evidente ver que se puede tomar $K = [G, G]$.

4) $\Rightarrow$ 1) Por el comentario que sigue a la Proposición 2.1, sabemos que $G^2 \subseteq K$ es nilpotente de clase menor o igual que $n-1$. Por lo tanto G es nilpotente de clase menor o igual que n. □

Nuestro siguiente objetivo es probar que $[G^i, G^j] \subseteq G^{i+j}$ para todo $i, j \geq 1$. Para ello daremos dos versiones de un lema conocido como lema de los tres subgrupos. Ambas sirven para nuestro proposito.

LEMA 2.4 (Lema de los tres subgrupos). *Supongamos que K, H, L y G' son subgrupos de un grupo G.*

1. *Si K, H y L son normales en G y G' incluye a $[K,[H,L]][H,[L,K]]$, entonces también incluye a $[L,[K,H]]$.*
2. *Si G' es normal en G e incluye a $[K,[H,L]][H,[L,K]]$, entonces también incluye a $[L,[K,H]]$.*

DEMOSTRACIÓN. El item 1) se sigue inmediatamente de la identidad de Hall

$$[lkl^{-1},[h,l]][hlh^{-1},[k,h]][khk^{-1},[l,k]] = 1,$$

que se demuestra por cálculo directo y el 2) de identidad de Jacobi

$$h[k,[h^{-1},l]]h^{-1}l[h,[l^{-1},k]]l^{-1}k[l,[k^{-1},h]]k^{-1} = 1,$$

que también se demuestra por cálculo directo. □

PROPOSICIÓN 2.5. *$[G^i, G^j] \subseteq G^{i+j+1}$ para todo $i, j \geq 0$.*

DEMOSTRACIÓN. Lo probamos por inducción en i. Cuando $i = 0$ el resultado es cierto por la misma definición de G^i y G^{i+1}. Supongamos que lo es para un i fijo y todo j. Entonces

$$[G,[G^i,G^j]] \subseteq [G,G^{i+j+1}] = G^{i+j+2} \quad \text{y} \quad [G^i,[G^j,G]] = [G^i,G^{j+1}] \subseteq G^{i+j+2}.$$

En consecuencia, por el Lema de los tres subgrupos

$$[G^{i+1},G^j] = [[G,G^i],G^j] = [G^j,[G,G^i]] \subseteq G^{i+j+2},$$

como deseamos □

COROLARIO 2.6. *$G^{(i)} \subseteq G^{2^i-1}$ para todo $i \geq 0$.*

DEMOSTRACIÓN. Para $i = 0$ esto es trivial. Supongamos que es cierto para un $i \geq 0$ fijo. Entonces por la Proposición 2.5,

$$G^{(i+1)} = [G^{(i)},G^{(i)}] \subseteq [G^{2^i-1},G^{2^i-1}] \subseteq G^{2^{i+1}-1},$$

como deseamos. □

La *serie central ascendente* de un grupo G es la serie de subgrupos

$$\mathrm{Z}_0\, G \subseteq \mathrm{Z}_1\, G \subseteq \mathrm{Z}_2\, G \subseteq \cdots,$$

definida recursivamente por $\mathrm{Z}_0\, G = 1$ y

$$\mathrm{Z}_{n+1}\, G = \pi^{-1}\left(\mathrm{Z}\left(\frac{G}{\mathrm{Z}_n\, G}\right)\right),$$

donde $\pi\colon G \to G/G_n$ es la proyección canónica, para todo $n \geq 0$.

Una sucesión ascendente

$$G = G_0 \lhd G_1 \lhd G_2 \lhd \cdots$$

de subgrupos de un grupo G es *central* si $G_i/G_{i+1} \subseteq \mathrm{Z}(G/G_{i+1})$ para todo i. Por ejemplo, la serie central ascendente de G es central.

PROPOSICIÓN 2.7. *Si*

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \dots$$

es una sucesión central de subgrupos de G, entonces $G_i \subseteq \mathrm{Z}_i\, G$ para todo i.

DEMOSTRACIÓN. Para $i = 0$ esto es trivial. Supongamos que es cierto para i. Como $G_{i+1}/G_i \subseteq \mathrm{Z}(G/G_i)$ y $G_i \subseteq \mathrm{Z}_i\, G$ se sigue que

$$\frac{G_{i+1}\,\mathrm{Z}_i\, G}{\mathrm{Z}_i\, G} \subseteq Z\left(\frac{G}{\mathrm{Z}_i\, G}\right) = \frac{\mathrm{Z}_{i+1}\, G}{\mathrm{Z}_i\, G},$$

por lo que $G_{i+1} \subseteq G_{i+1}\,\mathrm{Z}_i\, G \subseteq \mathrm{Z}_{i+1}\, G$. □

TEOREMA 2.8. *Para cada grupo G,*

$$G^n = 1 \quad \textit{si y sólo si} \quad \mathrm{Z}_n\, G = G.$$

Además, en este caso $G^i \subseteq Z_{n-i}G$ para todo $i \leq n$.

DEMOSTRACIÓN. Supongamos primero que $\mathrm{Z}_n\, G = G$. Por la Proposición 2.2, sabemos que

$$G^i \subseteq Z_{n-i}G \qquad \text{para } 0 \leq i \leq n.$$

En particular $G^n \subseteq Z_0G = 1$. Supongamos ahora que $G^n = 1$. Entonces, por la Proposición 2.7,

$$G^i \subseteq Z_{n-i}G \qquad \text{para } 0 \leq i \leq n.$$

En particular $G = G^0 \subseteq Z_nG$. □

COROLARIO 2.9. *Un grupo G es nilpotente si y sólo si existe $n \geq 0$ tal que $\mathrm{Z}_n\, G = G$. El mínimo n con esta propiedad es la clase de nilpotencia de G.*

DEMOSTRACIÓN. Es una consecuencia inmediata del Teorema2.8. □

PROPOSICIÓN 2.10. *Si N es un subgrupo normal no nulo de un grupo nilpotente G, entonces $N \cap \mathrm{Z}\, G \neq 1$.*

DEMOSTRACIÓN. Como G es nilpotente el conjunto de los $i \geq 0$ tales que $N \cap G_i \neq 1$ tiene un elemento máximo n_0. Puesto que N es normal,

$$[G, N \cap G^{n_0}] \subseteq N \cap [G, G^{n_0}] = N \cap G^{n_0+1} = 1,$$

o, lo que es igual, $N \cap G^{n_0} \subseteq \mathrm{Z}\, G$. □

PROPOSICIÓN 2.11. *Si N es un subgrupo abeliano y normal maximal de un grupo nilpotente G, entonces $N = \mathrm{C}_G(N)$.*

DEMOSTRACIÓN. Como es conmutativo, $N \subseteq \mathrm{C}_G(N)$. Veamos que también vale la inclusión recíproca. Por los comentarios hechos al comienzo de la Subsección 18.7, sabemos que $\mathrm{C}_G(N) \lhd \mathrm{N}_G(N) = G$, donde la última igualdad es cierta por hipótesis. En consecuencia $\mathrm{C}_G(N)/N$ es un subgrupo normal del grupo nilpotente G/N. Por la Proposición 2.10, si N está incluído propiamente en $\mathrm{C}_G(N)$, entonces existe $g \in \mathrm{C}_G(N) \setminus N$ cuya clase en G/N pertenece a $\mathrm{Z}(G/N)$, pero esto es imposible, porque implica que $\langle N, g\rangle$ es un subgrupo normal y abeliano de G, lo que contradice la maximalidad de N. □

TEOREMA 2.12. *Todo subgrupo propio de un grupo nilpotente está incluído propiamente en su normalizador.*

DEMOSTRACIÓN. Tomemos un subgrupo H de G y consideremos la serie central ascendente

$$1 = \mathrm{Z}_0\, G \subsetneq \mathrm{Z}_1\, G \subsetneq \cdots \subsetneq \mathrm{Z}_n\, G = G,$$

de G. Afirmamos que si i es el máximo índice tal que $\mathrm{Z}_i\, G \subseteq H$, entonces $\mathrm{Z}_{i+1}\, G \subseteq \mathrm{N}_G(H)$. En efecto, como $\mathrm{Z}_{i+1}\, G/\,\mathrm{Z}_i\, G$ es el centro de $G/\,\mathrm{Z}_i\, G$,

$$[ghg^{-1}] = [g][h][g]^{-1} = [h] \quad \text{en } G/\,\mathrm{Z}_i\, G,$$

para todo $h \in H$ y $g \in \mathrm{Z}_{i+1}\, G$. Así $gHg^{-1} \subseteq H$. □

COROLARIO 2.13. *Si G es un grupo nilpotente finito, entonces:*

1. *Para cada subgrupo propio H de G existe una cadena*

$$H = G_1 \lhd G_2 \lhd \cdots \lhd G_m = G$$

de subgrupos de G tales que $|G_{i+1} : G_i|$ es primo para todo $i < m$.

2. *Para cada subgrupo propio H de G, existe un subgrupo normal N de G tal que $H \leq N$ y $|G : N|$ es primo.*
3. *Todo subgrupo maximal de G es normal y tiene índice primo.*

DEMOSTRACIÓN. 1) Cuando $|G : H| = 2$ esto es trivial. Supongamos que es cierto siempre que $|G : H| \leq n$ y que $|G : H| = n + 1$. Si hay un subgrupo propio L de G que contiene propiamente a H, entonces por hipótesis inductiva existen cadenas

$$H = G_1 \lhd G_2 \lhd \cdots \lhd G_i = L \quad \text{y} \quad L = G_i \lhd G_2 \lhd \cdots \lhd G_m = G$$

tales que $|G_{i+1} : G_i|$ es primo para $1 \leq i < m$, usando lo cual el resultado se sigue inmediatamente. En caso contrario, por el Teorema 2.12 sabemos que H es un subgrupo normal de G. Entonces, por el teorema de Jordan Hölder, la serie normal

$$1 \lhd H \lhd G$$

se puede refinar a una serie de composición, y el resultado de sigue de que G es resoluble y de que cada factor de composición de un grupo resoluble finito es isomorfo a un grupo simple $\mathbb{Z}_p$, con p primo.

2) Es consecuencia inmediata del item 1).

3) Es consecuencia inmediata del item 2).

□

LEMA 2.14. *Todo p-grupo finito es nilpotente.*

DEMOSTRACIÓN. Supongamos que P es un grupo de orden p^r y que el resultado vale para grupos de orden p^k con $k < r$. Entonces la serie central ascendente de $P/\,\mathrm{Z}\, P$ es

$$\frac{\mathrm{Z}_1\, P}{\mathrm{Z}_1\, P} \subsetneq \frac{\mathrm{Z}_2\, P}{\mathrm{Z}_1\, P} \subsetneq \cdots \subsetneq \frac{\mathrm{Z}_n\, P}{\mathrm{Z}_1\, P} = \frac{P}{\mathrm{Z}_1\, P}$$

y, en consecuencia,

$$1 = \mathrm{Z}_0\, P \subsetneq \mathrm{Z}_1\, P \subsetneq \cdots \subsetneq \mathrm{Z}_n\, P = P$$

es la serie central ascendente de P. □

TEOREMA 2.15. *Para cada grupo finito G son equivalentes:*

1. *G es un producto directo de p-grupos.*
2. *G es nilpotente.*

3. *Todo subgrupo propio de G está incluído propiamente en su normalizador.*
4. *Todo subgrupo maximal de G es normal.*
5. *Todos los subgrupos de Sylow de G son normales.*
6. *G es el producto directo de sus subgrupos de Sylow.*
7. *Dos elementos de G de ordenes coprimos entre si conmutan.*
8. *Si P es un p-subgrupo de Sylow de G y $q \neq p$ es un primo que divide a $|G|$, entonces existe un q-subgrupo de Sylow de G que normaliza a P.*

DEMOSTRACIÓN. 1) $\Rightarrow$ 2) Por el Lema 2.14 y la Proposición 2.1.

2) $\Rightarrow$ 3) Por el Teorema 2.12.

3) $\Rightarrow$ 4) Es trivial.

4) $\Rightarrow$ 5) Si un subgrupo de Sylow P de G no fuera normal, entonces $\mathrm{N}_G(P)$ estaría incluído en un subgrupo maximal H de G. Por el Corolario 6.21 del Capítulo 3 esto implica que $H = N_G(H)$, lo que contradice la hipótesis.

5) $\Rightarrow$ 6) Es una consecuencia inmediata del Corolario 15.15 del Capítulo 1.

6) $\Rightarrow$ 1) Es trivial.

1) $\Rightarrow$ 7) Es trivial.

7) $\Rightarrow$ 8) Es trivial.

8) $\Rightarrow$ 1) Tomemos un subgrupo de Sylow P de G. Es claro que $P \subseteq \mathrm{N}_G(P)$ y por hipótesis para cada primo $q \neq p$ que divide a G hay un q-subgrupo de Sylow de G incluído en $\mathrm{N}_G(P)$. En consecuencia, por la Proposición 6.9, necesariamente $\mathrm{N}_G(P) = G$. □

Es obvio que un grupo es conmutativo si y sólo si lo son todos sus subgrupos generados por dos elementos. La proposición que sigue da una caracterización de este tipo de los grupos nilpotentes finitos.

PROPOSICIÓN 2.16. *Un grupo finito es nilpotente si y sólo si todos sus subgrupos generados por dos elementos lo son.*

DEMOSTRACIÓN. Por la Proposición 2.1, si un grupo finito es nilpotente, entonces también lo son todos sus subgrupos generados por dos elementos. La recíproca es un corolario inmediato de la equivalencia entre los items 2) y 7) del Teorema 2.15. □

TEOREMA 2.17. *Cada grupo finito G contiene un máximo subgrupo normal nilpotente $\mathcal{F}(G)$. Además $\mathcal{F}(G)$ es un subgrupo característico de G.*

DEMOSTRACIÓN. Vamos a verificar que la primera afirmación es verdadera mostrando que si N y H son subgrupos normales y nilpotentes de G, entonces también lo es NH. Por la Observación 10.6 del Capítulo 1, sabemos que $NH \lhd G$. Con el objetivo de probar que NH es nilpotente, consideremos el conjunto $\{p_1, \ldots, p_n\}$ de los primos positivos que dividen a $|N||H|$, y escribamos

$$P_i = \begin{cases} \text{El único } p_i\text{-subgrupo de Sylow de } N & \text{si } p_i \text{ divide a } |N|, \\ 1 & \text{si } p_i \text{ no divide a } |N| \end{cases}$$

y

$$Q_i = \begin{cases} \text{El único } p_i\text{-subgrupo de Sylow de } H & \text{si } p_i \text{ divide a } |H|, \\ 1 & \text{si } p_i \text{ no divide a } |H| \end{cases}$$

(una consecuencia del item 5) del Teorema 2.15 y el Corolario 6.7 del Capítulo 3 es que tanto N como H tienen un único p-subgrupo de Sylow para cada uno de sus divisores primos p). Por el Teorema 6.20 del Capítulo 3, los P_i's y los Q_i's son subgrupos normales de G. En consecuencia

$$NH = P_1 \dots P_n Q_1 \dots Q_n = P_1 Q_1 \dots P_n Q_n.$$

Como $|P_i Q_i|$ es una potencia de p_i, cada $|P_i Q_i|$ es coprimo con $|P_j Q_j|$ para $j \neq i$. Además, nuevamente por la Observación 10.6 del Capítulo 1, los $P_i Q_i$'s son subgrupos normales de G y, por lo tanto, también de NH. En consecuencia, por Corolario 15.15 del Capítulo 1,

$$NH \simeq P_1 Q_1 \times \cdots \times P_n Q_n,$$

por lo que NH es nilpotente, debido a la equivalencia entre los items 1) y 2) del Teorema 2.15.

La segunda afirmación se sigue inmediatamente de que, por la Proposición 2.1, el subgrupo normal $\varphi(\mathcal{F}(G))$ de G es nilpotente para cada automorfismo φ de G. □

El grupo $\mathcal{F}(G)$, cuya existencia acabamos de demostrar es llamado el *subgrupo de Fitting* de G.

Parte 2

Anillos y módulos

Capítulo 5

Teoría elemental de anillos

1. Anillos

Un *anillo* A es un conjunto provisto de dos operaciones binarias, llamadas *suma* o *adición* y *producto* o *multiplicación*, tales que

1. A es un grupo abeliano vía la suma,
2. A es un monoide vía el producto,
3. El producto es distributivo a izquierda y a derecha con respecto a la suma.

Como es usual, denotaremos con $a+b$ a la suma de dos elementos $a, b \in A$, con ab al producto, con 0 al elemento neutro de A respecto de la suma, con $-a$ al opuesto aditivo de un elemento a y con 1 a la unidad o neutro respecto del producto. Con estas notaciones el último item de la definición anterior se escribe

$$a(b+c) = ab + ac \qquad \text{y} \qquad (b+c)a = ba + ca.$$

Puede ocurrir que $1 = 0$, pero en este caso, como veremos enseguida, A es el *anillo nulo* $\{0\}$, al que denotaremos 0. Son bien conocidos e importantes los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ de los números enteros, racionales, reales y complejos. También son muy importantes los anillos de polinomios en una y varias variables sobre estos y los de congruencias $\mathbb{Z}/n\mathbb{Z}$. Un anillo es *conmutativo* si su producto lo es. El anillo $\mathrm{M}_n(A)$, de matrices cuadradas de $n \times n$ con coeficientes en un anillo A (cuando A es una anillo arbitrario la definición es la misma que cuando es un cuerpo), no es conmutativo si $n > 1$ y A no es el anillo nulo. Tampoco lo es el anillo de endomorfismos $\mathrm{End}_k(V)$ de un k-espacio vectorial V, si $\dim_k(V) > 1$. Como el lector atento habrá notado, algunos de los ejemplos mencionados aquí, entre ellos el último, ya fueron considerados en la primera parte de estas notas.

Proposición 1.1. *La multiplicación de A tiene las siguientes propiedades:*

1. *$a0 = 0a = 0$ para todo $a \in A$.*
2. *$(-a)b = a(-b) = -ab$ para todo $a, b \in A$.*

Demostración. 1) Sumando $-a0$ a ambos miembros de la igualdad

$$a0 = a(0+0) = a0 + a0,$$

obtenemos que $0 = a0$. De la misma manera se ve que $0 = 0a$.

2) Basta observar que, por el item anterior,

$$ab + (-a)b = (a + (-a))b = 0b = 0.$$

La otra afirmación es similar. □

Corolario 1.2. *Si* $1 = 0$*, entonces* $A = 0$*.*

Demostración. Por la proposición anterior $a = a1 = a0 = 0$ para cada $a \in A$. □

El *anillo opuesto* de A es el anillo A^{op}, que tiene los mismos conjunto subyacente y suma que A, pero cuya multiplicación $\mu_{A^{\mathrm{op}}} \colon A^{\mathrm{op}} \times A^{\mathrm{op}} \to A^{\mathrm{op}}$ está definida por $\mu_{A^{\mathrm{op}}}(a,b) := ba$. Es evidente que A es conmutativo si y sólo si $A = A^{\mathrm{op}}$.

Un elemento a de A es un *divisor de cero a izquierda* si existe $b \in A \setminus \{0\}$ tal que $ab = 0$, un *divisor de cero a derecha* si existe $b \in A \setminus \{0\}$ tal que $ba = 0$. Finalmente a es un *divisor de cero* si lo es a izquierda o a derecha. Por ejemplo, el operador de derivación

$$\frac{d}{dX} \colon \mathbb{R}[X] \to \mathbb{R}[X]$$

es un divisor de cero a izquierda del anillo $\mathrm{End}_{\mathbb{R}}(\mathbb{R}[X])$, porque componiendolo a derecha con la evaluación en cero

$$\mathrm{ev}_0 \colon \mathbb{R}[X] \to \mathbb{R}[X],$$

se obtiene la función nula. Este operador no es un divisor de cero a derecha porque es sobreyectivo. En cambio ev_0 lo es a ambos lados porque $\mathrm{ev}_0 \circ (\mathrm{id} - \mathrm{ev}_0) = 0$. Notemos que a es divisor de cero a un lado en A si y sólo si lo es al otro en A^{op}y que, salvo en el caso en que A es el anillo nulo, 0 es divisor de cero.

Tal como para magmas, monoides y grupos, muchas propiedades predicables sobre elementos y subconjuntos de A tienen una versión a izquierda y otra a derecha (que es la misma, pero predicada en A^{op}). También en esta parte del apunte a veces daremos sólo una de ellas, dejando como ejercicio la tarea de enunciar la otra.

Recordemos que un elemento $a \in A$ es cancelable a izquierda si $ab = ac \Rightarrow b = c$ y cancelable a derecha si $ba = ca \Rightarrow b = c$. Decimos que a es cancelable si lo es a izquierda y a derecha. Como vimos en la Sección 1 del Capítulo 1, los elementos cancelables a izquierda forman un submonoide multiplicativo de A y si ab es cancelable a izquierda, entonces b también lo es.

Proposición 1.3. *Un elemento* $a \in A$ *es un divisor de cero a izquierda si y sólo si no es cancelable a izquierda.*

Demostración. Si $ab = 0$ para algún $b \in A$ no nulo, entonces $ab = a0$, y así a no es cancelable a izquierda. Recíprocamente, si $ab = ac$ con $b, c \in A$ distintos, entonces a es un divisor de cero a izquierda, pues $a(b-c) = 0$ y $b - c \neq 0$. □

Proposición 1.4. *Para todo anillo* A *las siguientes afirmaciones son equivalentes:*

1. *A no tiene divisores de cero a izquierda no nulos.*
2. *A no tiene divisores de cero a derecha no nulos.*

3. Todo elemento no nulo de A es cancelable a izquierda.

4. Todo elemento no nulo de A es cancelable a derecha.

Demostración. Por la Proposición 1.3 sabemos que 1) es equivalente a 3). Similarmente, 2) es equivalente a 4). Veamos que 1) implica 2). Supongamos que $ab = 0$ y que $b \neq 0$. Entonces a es un divisor de cero a izquierda, por lo que $a = 0$. Esto muestra que vale 2). Por simetría 2) implica 1). □

Un *dominio* o *anillo cancelativo* es un anillo no nulo que tiene las propiedades equivalentes listadas en la proposición anterior.

Ejemplo 1.5. *Los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son dominios conmutativos.*

Ejemplo 1.6. *Fijemos $q \in \mathbb{C}^\times$. El anillo $\mathbb{C}_q[X, Y]$ es el grupo aditivo $\mathbb{C}[X, Y]$, con el producto definido por*

$$(aX^mY^n)(bX^{m'}X^{n'}) := q^{m'n}abX^{m+m'}Y^{n+n'}$$

sobre monomios, y extendido a los polinomios mediante la propiedad distributiva. Es fácil ver que $\mathbb{C}_q[X, Y]$ es en verdad un anillo. Como la estructura aditiva es la estandar, basta verificar que 1 es el neutro (lo que es obvio), que vale la propiedad distributiva (lo que no es muy difícil) y que el producto es asociativo. Este parece el punto más molesto, pero una vez que uno se convence de que es suficiente comprobarlo sobre monomios se vuelve casi trivial. Cuando $q \neq 1$, este anillo es un dominio no conmutativo. La demostración usual en el caso conmutativo, funciona también en el caso general.

Un elemento a de A es *inversible a izquierda* si existe $b \in A$ tal que $ba = 1$ y es *inversible a derecha* si existe $b \in A$ tal que $ab = 1$. En el primer caso decimos que b es una *inversa a izquierda* de a, y en el segundo, que es una *inversa a derecha*. Diremos que a es una *unidad* o que es *inversible*, si lo es a ambos lados. En este caso su inversa es única y la denotamos a^{-1}. El conjunto $A^\times$ de los elementos inversibles de A es un grupo vía el producto, llamado *grupo de unidades* de A. Por los comentarios que preceden a la Proposición 1.1 del Capítulo 1, todo elemento de A que es inversible a izquierda es cancelable a izquierda. Además, por dicha proposición también sabemos que si $a \in A$ es inversible a izquierda y cancelable a derecha o inversible a derecha y cancelable a izquierda, entonces es inversible. Por último, debido a la Proposición 1.2 del Capítulo 1, si A es finito, entonces cada $a \in A$ que es cancelable a izquierda o a derecha, es inversible.

Ejercicio 1.7. *Pruebe que si $a \in A$ es inversible a izquierda pero no a derecha, entonces tiene infinitas inversas a izquierda.*

Sugerencia: Tome $b_0 \in I$, donde I es el conjunto de las inversas a izquierda de a, y pruebe que la aplicación $\theta\colon I \to I$, dada por $\theta(b) := ab + b_0 - 1$, es inyectiva pero no sobreyectiva.

En el siguiente ejercicio se muestra que un anillo puede tener elementos que son inversibles a izquierda pero no a derecha.

Ejercicio 1.8. *Pruebe que si V es un k-espacio vectorial con base numerable, entonces $\mathrm{End}_k(V)$ tiene elementos inversibles a izquierda que son divisores de cero a derecha.*

Ejercicio 1.9. *Pruebe que si V es un k-espacio vectorial de dimensión finita, entonces para cada $\varphi \in \mathrm{End}_k(V)$ son equivalentes:*

1. φ es inversible.

2. φ no es divisor de cero a izquierda.

3. φ no es divisor de cero a derecha.

Un *anillo de división* es un anillo no nulo en el cual todo elemento distinto de cero es inversible. Todo anillo de división es un dominio. Un *cuerpo* es un anillo de división conmutativo. Los anillos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, de los números racionales, reales y complejos, son cuerpos. También lo es $\mathbb{Z}/p\mathbb{Z}$, si p es primo. Después veremos ejemplos de anillos de división no conmutativos. Por el comentario que precede al Ejercicio 1.7, todo dominio finito es un anillo de división. Sin embargo, como veremos más adelante, estos son necesariamente conmutativos.

Un elemento a de un anillo es *nilpotente* si $a^n = 0$ para algún $n \in \mathbb{N}$.

PROPOSICIÓN 1.10. *Para cada par de elementos a y b de un anillo no nulo A, vale lo siguiente:*

1. Si a es nilpotente y b conmuta con a, entonces ab y ba son nilpotentes.

2. Si a y b son nilpotentes y conmutan entre sí, entonces $a+b$ también es nilpotente.

3. Si a es nilpotente, entonces a es un divisor de cero a izquierda y a derecha.

4. Si a es inversible y b es nilpotente, entonces $a-b$ es inversible.

DEMOSTRACIÓN. 1) Si $a^n = 0$, entonces $(ab)^n = a^n b^n = 0 = b^n a^n = (ba)^n$.
2) Si $a^n = b^m = 0$, entonces $(a+b)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} a^i b^{m+n-i-1} = 0$.
3) Podemos suponer que $a \neq 0$. La igualdad $aa^{n-1} = a^{n-1}a = 0$, en la cual n es el mínimo número natural tal que $a^n = 0$, muestra que a es un divisor de cero a izquierda y a derecha.
4) Si $b^n = 0$, entonces $(a-b)(a^{-1} + a^{-2}b + \cdots + a^{-n}b^{n-1}) = 1$. □

NOTA 1.11. *Para cada anillo A denotamos con $A^\times$ al grupo de unidades de A.*

2. Subanillos

Un subconjunto B de un anillo A es un *subanillo* de A si es cerrado para la resta y el producto y $1 \in B$. Entonces B es un anillo en forma natural. Dado que la intersección de una familia de subanillos de A es un subanillo de A, para cada subconjunto S de A existe un mínimo subanillo $\mathbb{Z}\{S\}$ de A que contiene a S, el cual es llamado *el subanillo de A generado por S*. Siguiendo la práctica usual, si $S = \{x_1, \ldots, x_s\}$, escribiremos $\mathbb{Z}\{x_1, \ldots, x_s\}$ en lugar de $\mathbb{Z}\{\{x_1, \ldots, x_s\}\}$. Dejamos a cargo del lector comprobar que $\mathbb{Z}\{S\}$ es el conjunto de las sumas algebraicas finitas de las expresiones de la forma

$$x_1 \cdots x_n \quad \text{con } n \geq 0 \text{ y } x_i \in S,$$

con la convención usual de que el producto vacío da 1. Decimos que S *genera* a A como anillo si $\mathbb{Z}\{S\} = A$. El conjunto de los subanillos de A es un reticulado completo con el orden definido por la inclusión. El mínimo es el subanillo $\mathbb{Z}\{1_A\}$, llamado *anillo primo* de A, el máximo es A, el ínfimo de una familia es la intersección de sus elementos, y el supremo, el subanillo de A generado por la unión de sus elementos. Cuando A es conmutativo se usan las notaciones $\mathbb{Z}[S]$ en lugar de $\mathbb{Z}\{S\}$ y $\mathbb{Z}[x_1, \ldots, x_s]$ en lugar de $\mathbb{Z}\{x_1, \ldots, x_s\}$. Para cada subanillo B de A y cada subconjunto S de A, denotamos con $B\{S\}$ al subanillo de A generado por $B \cup S$. Por supuesto que si $S = \{x_1, \ldots, x_s\}$, escribiremos $B\{x_1, \ldots, x_s\}$ en lugar de $B\{\{x_1, \ldots, x_s\}\}$ y que si A es conmutativo usaremos las notaciones $B[S]$ y $B[x_1, \ldots, x_s]$ en lugar de $B\{S\}$ y $B\{x_1, \ldots, x_s\}$ respectivamente.

EJEMPLO 2.1. *Cada uno de los tres primeros de los anillos* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *y* $\mathbb{C}$ *se identifica canónicamente con un subanillo del siguiente.*

EJEMPLO 2.2. *Los anillos de matrices* $\mathrm{M}_n(\mathbb{Q})$ *y* $\mathrm{M}_n(\mathbb{R})$ *son subanillos de* $\mathrm{M}_n(\mathbb{C})$.

EJEMPLO 2.3. *Una matriz cuadrada*

$$\mathrm{A} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

con coeficientes en un anillo A *es* triangular superior *si* $a_{ij} = 0$ *siempre que* $i > j$, diagonal *si* $a_{ij} = 0$ *siempre que* $i \neq j$ *y* escalar *si es diagonal y* $a_{11} = \cdots = a_{nn}$. *Los conjuntos* $\mathrm{Esc}_n(A)$ *de las matrices escalares,* $\mathrm{D}_n(A)$ *de las matrices diagonales y* $\mathrm{T}_n(A)$ *de las matrices triangulares superiores de* $n \times n$ *con coeficientes en* A, *son subanillos de* $\mathrm{M}_n(A)$.

EJEMPLO 2.4. *El anillo de los* enteros de Gauss *es el subanillo* $\mathbb{Z}[i]$ *de* $\mathbb{C}$. *Es inmediato que* $\mathbb{Z}[i]$ *son los números complejos con parte real e imaginaria enteras.*

EJEMPLO 2.5. *El subanillo* $\mathbb{Z}[\sqrt{3}]$ *de* $\mathbb{R}$ *está formado por los elementos de la forma* $a+b\sqrt{3}$, *con* $a, b \in \mathbb{Z}$. *Es fácil ver que si* $a + b\sqrt{3} = a' + b'\sqrt{3}$, *entonces* $a = a'$ *y* $b = b'$, *de modo que esta escritura es única.*

EJEMPLO 2.6. *Todo anillo* A *es un subanillo de* $A[X_1, \ldots, X_n]$.

2.1. El centro de un anillo

Por definición, el *centro* de una anillo A es el conjunto

$$\mathrm{Z}\,A := \{a \in A : ab = ba \text{ para todo } b \in A\}.$$

Un elemento a de A es *central* si pertenece al centro de A. Es evidente que $\mathrm{Z}\,A$ es un subanillo conmutativo de A. Además, no es difícil probar que si $a \in \mathrm{Z}\,A$ es inversible, entonces $a^{-1} \in \mathrm{Z}\,A$. En efecto,

$$ab = ba \Leftrightarrow b = a^{-1}ba \Leftrightarrow ba^{-1} = a^{-1}b.$$

En particular, si A es un anillo de división, entonces $\mathrm{Z}\,A$ es un cuerpo.

PROPOSICIÓN 2.7. *Para cada anillo* A, *el centro de* $\mathrm{M}_n(A)$, *es el anillo* $\mathrm{Esc}_n(\mathrm{Z}\,A)$, *de las matrices escalares con coeficientes en el centro de* A.

DEMOSTRACIÓN. Como es usual denotamos con E_{rs} a la matriz que tiene un 1 en la coordenada (r, s) y 0 en las demás. Tomemos $\mathrm{B} = (a_{ij}) \in \mathrm{Z}\,\mathrm{M}_n(A)$. Como $\mathrm{E}_{rs}\mathrm{B}$ es la matriz cuya única fila no nula es la r-ésima, que coincide con la s-ésima fila de B y BE_{rs} es la matriz cuya única columna no nula es la s-ésima, que coincide con la r-ésima columna de B, la matriz B es diagonal y $a_{ss} = a_{rr}$ para todo r y s. Así, $\mathrm{Z}\,\mathrm{M}_n(A) \subseteq \mathrm{Esc}_n(\mathrm{Z}\,A)$. Como la inclusión recíproca es trivial, $\mathrm{Z}\,\mathrm{M}_n(A) = \mathrm{Esc}_n(\mathrm{Z}\,A)$. □

Notemos que en la demostración anterior podríamos haber supuesto que $r \leq s$. Por lo tanto el mismo argumento muestra que $\mathrm{Z}\,T_n(A) = \mathrm{Esc}_n(\mathrm{Z}\,A)$.

Consideremos ahora un subconjunto T de un anillo A. El *centralizador de* T *en* A es

$$\mathrm{Z}_T\,A := \{a : ab = ba \text{ para todo } b \in T\}.$$

De la definición se sigue inmediatamente que $\mathrm{Z}_A\, A$ es el centro de A. Argumentando del mismo modo que para $\mathrm{Z}\, A$, se comprueba que $\mathrm{Z}_T\, A$ es un subanillo de A cualquiera sea T, y, que si $a \in \mathrm{Z}_T\, A$ es inversible, entonces $a^{-1} \in \mathrm{Z}_T\, A$. En particular, si A anillo de división, entonces $\mathrm{Z}_T\, A$ también lo es. Evidentemente un subanillo B de A es commutativo si y sólo si $B \subseteq \mathrm{Z}_B\, A$. Además, en este caso, $B\{a\}$ es conmutativo para cada $a \in \mathrm{Z}_B\, A$. En consecuencia, si B es un subanillo conmutativo maximal de A, entonces $B = \mathrm{Z}_B\, A$. También vale la recíproca, puesto que si $B = \mathrm{Z}_B\, A$ y C es un subanillo conmutativo de A que incluye a B, entonces $C \subseteq \mathrm{Z}_B\, A = B$.

Supongamos ahora que A es un anillo de división. Entonces es natural considerar el conjunto de los subanillos de división de A, el cual claramente es cerrado bajo intersecciones. En consecuencia, para cada subconjunto S de A existe un mínimo subanillo de división $\mathbb{Z}(S)$ de A que contiene a S, el cual es llamado *el subanillo de división de A generado por S*. De la misma manera que para subanillos, cuando $\mathbb{Z}(S) = A$ decimos que *S genera a A como anillo de división*. El conjunto de los subanillos de división de A también es un reticulado completo con el orden definido por la inclusión. El mínimo es el cuerpo $\mathbb{Z}(1_A)$, llamado *el cuerpo primo de A*, el máximo es A, el ínfimo de una familia es la intersección de sus elementos y el supremo, el subanillo de división de A generado por la unión de sus elementos. Para cada subanillo de división B de A y cada subconjunto S de A denotamos con $B(S)$ al mínimo subanillo de división de A que contiene a B y a S. Este sería el lugar apropiado para dar ejemplos de subanillos de división, y en particular de subcuerpos, pero de hecho sólo daremos ejemplos de estos últimos. Esto se debe simplemente a que en realidad todavía no hemos dado ningún ejemplo de anillo de división no conmutativo. Más adelante, cuando introduzcamos los cuaterniones, solucionaremos esta falencia.

Ejemplo 2.8. *Dos de los subanillos del Ejemplo 2.1 son subcuerpos.*

Terminamos esta subsección probando un famoso teorema de Wedderburn que dice que todo anillo de división finito es conmutativo. En la demostración, además de la ecuación de las clases usaremos propiedades básicas de los polinomios ciclotómicos. Por definición para cada $n \in \mathbb{N}$ el n-ésimo polinomio ciclotómico es

$$\phi_n(X) := \prod_{w \in \Omega_n} (X - w),$$

donde $\Omega_n \subseteq \mathbb{C}$ denota al conjunto de las raíces n-ésimas primitivas de la unidad. Es evidente que

$$X^n - 1 = \prod_{d|n} \phi_d(X).$$

Un argumento inductivo, usando este hecho, muestra que $\phi_n(X)$ es un polinomio mónico con coeficientes en $\mathbb{Z}$.

También usaremos implicitamente el siguiente resultado elemental.

Lema 2.9. *Si $k \subseteq K$ son anillos de división y V es un K-espacio vectorial, entonces*

$$\dim_k(V) = \dim_k(K) \dim_K(V).$$

Demostración. Es suficiente ver que si $(u_i)_{i \in I}$ es una base de K como k-espacio vectorial a izquierda y $(w_j)_{j \in J}$ es una base de V como K-espacio vectorial a izquierda, entonces $(u_i w_j)_{i \in I, j \in J}$ es una base de V como k-espacio vectorial a izquierda. Veamos primero que esta

última es una famila de generadores de V. Para ello tomemos $v \in V$ arbitrario. Por hipótesis existe una familia $(\lambda_j)_{j\in J}$, de elementos de K, con soporte finito, tal que

$$v = \sum_{j\in J} \lambda_j w_j. \tag{35}$$

Dado que, nuevamente por hipótesis, para cada $\lambda_j \neq 0$ existe una familia $(\alpha_{ij})_{i\in I}$, de elementos de K, con soporte finito, tal que

$$\lambda_j = \sum_{i\in I} \alpha_{ij} u_i,$$

reemplazando cada λ_j por la suma que aparece en el lado derecho de esta igualdad y poniendo $\alpha_{ij} = 0$ para todo i y todo j tal que $\lambda_j = 0$, obtenemos que

$$v = \sum_{j\in J} \left(\sum_{i\in I} \alpha_{ij} u_i \right) w_j = \sum_{i\in I, j\in J} \alpha_{ij} u_i w_j.$$

Veamos ahora que la familia $(u_i w_j)_{i\in I, j\in J}$ es linealmente independiente sobre k. Supongamos que $(\alpha_{ij})_{i\in I, j\in J}$ es una familia de elementos de k, con soporte finito, tal que

$$\sum_{j\in J} \left(\sum_{i\in I} \alpha_{ij} u_i \right) w_j = \sum_{i\in I, j\in J} \alpha_{ij} u_i w_j = 0.$$

Como $(w_j)_{j\in J}$ es linealmente independiente sobre K,

$$\sum_{i\in I} \alpha_{ij} u_i = 0 \qquad \text{para todo } j \in J,$$

y así, dado que $(u_i)_{i\in I}$ es linealmente independiente sobre k, cada α_{ij} es cero. □

Teorema 2.10. *Todo anillo de división finito D es un cuerpo.*

Demostración. Denotemos con Z el centro de D y con Z_x al centralizador en D de cada elemento $x \in D$. Sabemos que Z es un cuerpo y que cada Z_x es un anillo de división. Además es evidente que si $q := \#(Z)$, $n_x := \dim_Z(Z_x)$, $m_x := \dim_{Z_x}(D)$ y $n := \dim_Z(D)$, entonces $n = m_x n_x$, $\#(Z_x) = q^{n_x}$ y $\#(D) = q^n = (q^{n_x})^{m_x}$. Es claro también que $Z^\times$ es el centro de $D^\times$ y que $Z_x^\times$ es el centralizador en $D^\times$ de cada elemento $x \in D^\times$. Tomemos un conjunto R de representantes de cada una de las clases de conjugación de $D^\times$ que tienen más de un elemento. La ecuación de las clases de $D^\times$ queda

$$q^n - 1 = \#(D^\times) = \#(Z^\times) + \sum_{x\in R} \frac{\#(D^\times)}{\#(Z_x^\times)} = q - 1 + \sum_{x\in R} \frac{q^n - 1}{q^{n_x} - 1}. \tag{36}$$

Dado que $x \notin Z$ para ningún $x \in R$, sabemos que n_x divide propiamente a n para todo $x \in R$. En consecuencia, tanto $X^n - 1$ como cada uno de los cocientes $\frac{X^n-1}{X^{n_x}-1}$ son polinomios divisibles por $\phi_n(X)$ en $\mathbb{Z}[X]$. De esto se sigue inmediatamente que $\phi_n(q)$ divide en $\mathbb{Z}$, tanto a $q^n - 1$ como a cada uno de los enteros $\frac{q^n-1}{q^{n_x}-1}$. Debido a la igualdad (36) tenemos entonces que $\phi_n(q) \mid q - 1$, lo que implica que

$$\prod_{w\in\Omega_n} |q - w| = |\phi_n(q)| \mid q - 1,$$

donde Ω_n es el conjunto de las raíces n-ésimas primitivas de la unidad. Dado que si $n > 1$, entonces $|q - w| > q - 1$ para cada $w \in \Omega_n$, se deduce de aquí que $n = 1$ y, así, $D = Z$. □

3. Ideales

Un subconjunto $I \neq \emptyset$ de A es un *ideal a izquierda* si es cerrado para la suma y $ax \in I$ para todo $a \in A$ y $x \in I$, y es un *ideal a derecha* si es cerrado para la suma y $xa \in I$ para todo $a \in A$ y $x \in I$ o, equivalentemente, si es un ideal a izquierda de A^{op}. Si I es un ideal a izquierda y a derecha, entonces decimos que es un *ideal bilátero* de A. Frecuentemente nos referiremos a estos últimos simplemente como ideales. Evidentemente 0 y A son ideales de A. Estos son los llamados *ideales triviales*. Un ideal a izquierda, a derecha o bilátero de A es *propio* si es distinto de A. Es claro que la intersección de una familia arbitraria de ideales a izquierda, derecha o biláteros de A es un ideal del mismo tipo. Por ejemplo, para cada subconjunto S de A, la intersección de los ideales a izquierda de A que incluyen a S es el mínimo ideal a izquierda AS de A que contiene a S. Este es llamado el *ideal a izquierda de A generado por S*. Como es usual, para cada $x \in A$, escribimos Ax en lugar de $A\{x\}$. Los *ideales a derecha* y *bilátero* de A *generados por* S (las definiciones son evidentes) serán denotados SA y ASA o $\langle S\rangle$, respectivamente. Por supuesto, escribimos xA en lugar de $\{x\}A$ y AxA en lugar de $A\{x\}A$. Es fácil ver que AS es el conjunto de todas las sumas finitas de elementos de la forma as, con $s \in S$ y $a \in A$. Similarmente, SA consiste de las sumas finitas de elementos de la forma sa, con $s \in S$ y $a \in A$, y ASA, de las sumas finitas de productos asb, con $a, b \in A$ y $s \in S$. En general $\{axb : a, b \in A\}$, donde x es un elemento fijo de A, no es un ideal bilátero de A. Por ejemplo, en $\mathrm{M}_2(\mathbb{Q})$ el conjunto formado por los productos

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} \\ a_{21}b_{11} & a_{21}b_{12} \end{pmatrix}, \tag{37}$$

no es un ideal bilátero, porque $\mathrm{M}_2(\mathbb{Q})$ no tiene ideales biláteros no triviales (vease la Proposición 3.5) y la expresión (37) nunca es la matriz identidad (debido a que $a_{11}b_{11} = a_{21}b_{12} = 1$ implica $a_{11}b_{12} \neq 0$). Un ideal a izquierda I de A es *finitamente generado* si existe un subconjunto finito S de A tal que $I = AS$ y es *principal* o *cíclico* si $I = Ax$ para algún $x \in A$. Dejamos al lector formular las variantes obvias de estas definiciones para los otros dos tipos de ideales. Un ideal a izquierda, derecha o bilátero de un anillo es *maximal* si es propio y no está incluído en ningún otro ideal propio del mismo tipo.

Proposición 3.1. *Un ideal a izquierda, derecha o bilátero propio de un anillo A está incluído en un ideal maximal del mismo tipo de A.*

Demostración. Supongamos por ejemplo que $I \subsetneq A$ es un ideal a izquierda de A y consideremos el conjunto $\mathcal{P}$ de los ideales a izquierda propios de A que contienen a I. Notemos que $\mathcal{P}$ no es vacío pues $I \in \mathcal{P}$. Por el lema de Zermelo podemos tomar una cadena maximal $(I_i)_{i\in I}$ de elementos de $\mathcal{P}$. Es evidente que ningún ideal a izquierda propio, J de A, puede contener estrictamente a $\bigcup I_i$, ya que en ese caso, agregando J a la cadena $(I_i)_{i\in I}$, obtendríamos una cadena estrictamente más grande que $(I_i)_{i\in I}$, de elementos de $\mathcal{P}$. Por lo tanto el teorema quedará probado si podemos ver que $\bigcup I_i$ es propio. Pero esto es claramente así, pues si 1 estuviera en esta unión, entonces estaría en I_i para algún $i \in I$, lo que se contradeciría con que I_i es propio. □

La *suma* de una familia arbitraria de ideales a izquierda $(I_j)_{j\in J}$ de A, es el ideal a izquierda $\sum_{j\in J} I_j$ generado por la unión $\bigcup_{j\in J} I_j$, de los miembros de la familia. Claramente $\sum_{j\in J} I_j$ es el conjunto de todas las sumas $\sum_{j\in J} a_j$, tales que $a_j \in I_j$ y $(a_j)_{j\in J}$ tiene soporte finito. Una familia $(I_j)_{j\in J}$ de ideales a izquierda de A está en *suma directa* si cada elemento de $\sum_{j\in J} I_j$

se escribe de manera única como una suma con soporte finito $\sum_{j\in J} a_j$ de elementos $a_j \in I_j$. En este caso escribimos $\bigoplus_{j\in J} I_j$ en lugar de $\sum_{j\in J} I_j$. Dejamos como ejercicio probar que son equivalentes:

1. $(I_j)_{j\in J}$ está en suma directa.
2. Si $0 = \sum_{j\in J} a_j$, donde $(a_j)_{j\in J}$ es una familia con soporte finito de elementos $a_j \in I_j$, entonces $a_j = 0$ para todo $j \in J$.
3. $I_i \bigcap \sum_{j\in J\setminus\{i\}} I_j = 0$ para cada $i \in J$.

Decimos que un ideal a izquierda I de un anillo A es un sumando directo de otro ideal a izquierda J de A que lo contiene, si existe un ideal a izquierda I' de A tal que $J = I \oplus I'$. Usualmente I' no es único.

Para los ideales a derecha y biláteros se pueden dar definiciones similares y probar resultados análogos. Dejamos los detalles al lector.

Como ocurre con el conjunto de los subanillos, los conjuntos de los ideales a izquierda, a derecha y biláteros de un anillo A son reticulados completos vía el orden dado por la inclusión. En los tres casos el mínimo es el ideal nulo, el máximo es A, el ínfimo de una familia es la intersección de sus elementos y el supremo es la suma. En general estos reticulados no son distributivos, pero siempre son modulares. En otras palabras,

$$I \cap (J + K) = J + I \cap K,$$

para cada terna de ideales a izquierda, derecha o biláteros (pero, por supuesto, todos del mismo tipo) I, J y K de A tales que $J \subseteq I$. En efecto, es inmediato que $I \cap (J + K) \supseteq J + I \cap K$. Para probar que vale la inclusión recíproca, basta observar que si una suma $a = b + c$, de elementos $b \in J$ y $c \in K$, está en I, entonces $c = a - b \in I \cap K$.

Ejemplo 3.2. *Es evidente que cada ideal no nulo I de $\mathbb{Z}$ tiene un mínimo número natural n_0. Afirmamos que $I = \langle n_0\rangle$. En efecto, por el algoritmo de división, para cada $a \in I$ existen $q, r \in \mathbb{Z}$ con $0 \leq r < n_0$ tales que $a = qn_0 + r$. Por la minimalidad de n_0, como $r = a - qn_0 \in I$, debe ser $r = 0$. Esto muestra que todo ideal de $\mathbb{Z}$ es cíclico. Un argumento similar muestra que el anillo $k[X]$, de polinomios con coeficientes en un cuerpo k, tiene la misma propiedad.*

Ejercicio 3.3. *Pruebe que la suma e intersección de ideales en $\mathbb{Z}$ están dadas por*

$$\langle m\rangle + \langle n\rangle = \langle (m; n)\rangle \qquad y \qquad \langle m\rangle \cap \langle n\rangle = \langle [m; n]\rangle,$$

donde $(m; n)$ y $[m; n]$ denotan al máximo divisor común y al mínimo múltiplo común de m y n, respectivamente. Pruebe que esto también es cierto para el anillo $k[X]$, de polinomios con coeficientes en un cuerpo k.

Proposición 3.4. *Para cada anillo no nulo A son equivalentes:*

1. *A es un anillo de división.*
2. *Los únicos ideales a izquierda de A son los triviales.*
3. *Los únicos ideales a derecha de A son los triviales.*

Demostración. Vamos a probar que 1) $\Leftrightarrow$ 2). La equivalencia entre los items 1) y 3) se sigue por un argumento similar (o bien, utilizando que los items 1) y 2) son equivalentes para el anillo A^{op}).

1) $\Rightarrow$ 2) Si I es un ideal a izquierda no nulo de A, entonces I tiene un elemento inversible y, por consiguiente, $I = A$.

2) $\Rightarrow$ 1) Debemos mostrar que todo $a \in A \setminus \{0\}$ es inversible. Pero como $Aa = A$, existe $b \in A$ tal que $ba = 1$. Por la misma razón b es inversible a izquierda y, por lo tanto, a es inversible. □

PROPOSICIÓN 3.5. *Si D es un anillo de división, entonces los únicos ideales biláteros de $\mathrm{M}_n(D)$ son los triviales.*

DEMOSTRACIÓN. Para cada $1 \leq i, j \leq n$, llamemos E_{ij} a la matriz de $n \times n$ cuya único coeficiente no nulo es el (i, j)-ésimo, que vale 1. Basta observar que si un ideal I de $\mathrm{M}_n(D)$ tiene un elemento no nulo

$$\mathrm{A} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix},$$

y $a_{ij} \neq 0$, entonces $\mathrm{id} = \sum_{l=1}^{n} a_{ij}^{-1} \mathrm{E}_{li} \mathrm{A} \mathrm{E}_{jl} \in I$. □

4. Morfismos de anillos

Un *morfismo de anillos* $f\colon A \to B$ es una terna (A, f, B), donde f es una función del conjunto subyacente de A en el de B, que satisface:

$$f(a + b) = f(a) + f(b), \quad f(ab) = f(a)f(b) \quad \text{y} \quad f(1) = 1.$$

El anillo A es el *dominio* de $f\colon A \to B$, y B es el codominio. Por ejemplo, la identidad $\mathrm{id}_A\colon A \to A$ y, más generalmente, la inclusión canónica $i\colon B \to A$, de un subanillo B de A en A, es un morfismo de anillos. También lo es la composición $g \circ f\colon A \to A''$ de dos morfismos $f\colon A \to A'$ y $g\colon A' \to A''$.

Muchas de las propiedades básicas de los morfismos de anillos son análogas a las establecidas para los de monoides y grupos. Las definiciones de endomorfismo, isomorfismo, automorfismo, monomorfismo, epimorfismo, sección y retracción son las mismas. Un argumento sencillo prueba que un morfismo es un isomorfismo si y sólo si es biyectivo. Mantenemos la notación $A \simeq A'$ para señalar que los anillos A y A' son isomorfos. Es fácil ver que los monomorfismos, epimorfismos, secciones y retracciones son cerrados bajo la composición, que toda retracción es sobreyectiva, toda sección, inyectiva, todo morfismo inyectivo, un monomorfismo, y todo morfismo sobreyectivo, un epimorfismo. También que un morfismo $f\colon A \to A'$ es un isomorfismo si y sólo si es una sección y un epimorfismo, y que esto ocurre si y sólo si es una retracción y un monomorfismo. Sigue siendo cierto que todo monomorfismo $f\colon A \to A'$ es inyectivo. En efecto, si $f(a) = f(a')$, entonces $f \circ g = f \circ g'$, donde $g, g'\colon \mathbb{Z}[X] \to A$ son los morfismos definidos por

$$g(P) := P(a) \quad \text{y} \quad g'(P) := P(a') \text{ para todo polinomio } P.$$

Por lo tanto $g = g'$ y entonces $a = a'$. Pero, como lo muestra el primero de los ejemplos dados abajo, es falso que un epimorfismo deba ser sobreyectivo.

Fijemos morfismos $f\colon A \to A'$ y $g\colon A' \to A''$. De la misma manera que en la teoría de monoides y grupos, vale que:

1. Si $g \circ f$ es una sección, un monomorfismo, o un morfismo inyectivo, entonces también lo es f.

2. Si $g \circ f$ es una retracción, un epimorfismo, o un morfismo sobreyectivo, entonces también lo es g.

Los símbolos $\mathrm{Hom}(A, A')$, $\mathrm{Iso}(A, A')$, $\mathrm{End}(A)$ y $\mathrm{Aut}(A)$ denotan respectivamente a los conjuntos de morfismos de A en A', isomorfismos de A en A', endomorfismos de A y automorfismos de A. Es inmediato que $\mathrm{End}(A)$ es un monoide (cuyo elemento neutro es la función identidad) vía la composición y que $\mathrm{Aut}(A)$ es su grupo de unidades.

EJEMPLOS 4.1. *Hay epimorfismos inyectivos que no son sobreyectivos y morfismos sobreyectivos que no son retracciones. En efecto:*

1. *La inclusión canónica $\imath\colon \mathbb{Z} \to \mathbb{Q}$ es un epimorfismo porque si $g, h\colon \mathbb{Q} \to C$ son morfismos de anillos tales que $g \circ i = h \circ i$, entonces*

$$g(m/n) = g(m)g(n)^{-1} = h(m)h(n)^{-1} = h(m/n)$$

para todo $m/n \in \mathbb{Q}$. Por otra parte no existe ningún morfismo $\pi\colon \mathbb{Q} \to \mathbb{Z}$ pues $\pi(1/2)$ debería satisfacer $2\pi(1/2) = \pi(1) = 1$, lo cual es imposible. En particular $\imath$ no es una sección.

2. *La aplicación $\pi\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, definida por $\pi(0) := \pi(2) := 0$ y $\pi(1) := \pi(3) := 1$, es sobreyectiva, pero no es una retracción.*

EJEMPLO 4.2. *Para cada anillo A hay un único morfismo $\imath\colon \mathbb{Z} \to A$. Es fácil ver que la imagen de $\imath$ es el anillo primo $\mathbb{Z}\{1_A\}$ de A. También es fácil ver que*

$$\mathbb{Z}\{1_A\} \simeq \begin{cases} \mathbb{Z} & \text{si } n1_A \neq 0 \text{ para todo } n \in \mathbb{N}, \\ \mathbb{Z}/n\mathbb{Z} & \text{si no, donde } n \in \mathbb{N} \text{ es el mínimo natural tal que } n1_A = 0. \end{cases}$$

En el primer caso decimos que la característica *de A es cero y en el segundo que es n. Es inmediato que un subanillo de un dominio es un dominio. En consecuencia, como $\mathbb{Z}/n\mathbb{Z}$ tiene divisores de cero si n no es primo, la característica de un dominio es necesariamente un número primo o cero.*

EJEMPLO 4.3. *Como $f(1) = 1$, un morfismo $f\colon \mathbb{Z}[i] \to A$, del anillo de enteros de Gauss en un anillo A, queda completamente determinado por la imagen de i. Puesto que $i^2 = -1$, debe ser $f(i)^2 = f(-1) = -1$. Además este es el único requisito que debe satisfacer $f(i)$. De modo que hay una correspondencia biunívoca entre $\mathrm{Hom}(Z[i], A)$ y $\{a \in A : a^2 = -1\}$. Cuando $A = \mathbb{Z}[i]$, este conjunto es $\{i, -i\}$. Como los endomorfismos obtenidos, son los automorfismos identidad y conjugación, $\mathrm{Aut}(\mathbb{Z}[i]) = \mathrm{End}(\mathbb{Z}[i])$ es un grupo cíclico de orden 2.*

EJEMPLO 4.4. *Para cada $n, m \in \mathbb{N}$ la aplicación*

$$\mathrm{M}_{n\times m}(A^{\mathrm{op}}) \to \mathrm{M}_{m\times n}(A),$$

que a cada matriz B le asigna su transpuesta ${}^t\mathrm{B}$, satisface

$${}^t(\mathrm{B} + \mathrm{C}) = {}^t\mathrm{B} + {}^t\mathrm{C} \quad \text{para todo } \mathrm{B}, \mathrm{C} \in \mathrm{M}_{n\times m}(A^{\mathrm{op}})$$

y

$${}^t(\mathrm{BC}) = {}^t\mathrm{C}{}^t\mathrm{B} \qquad \text{para todo } \mathrm{B} \in \mathrm{M}_{n\times m}(A^{\mathrm{op}}) \text{ y } \mathrm{C} \in \mathrm{M}_{m\times l}(A^{\mathrm{op}}).$$

En particular $\mathrm{M}_n(A^{\mathrm{op}}) \simeq \mathrm{M}_n(A)^{\mathrm{op}}$.

EJEMPLO 4.5. *Para cada morfismo de anillos* $f\colon A \to B$ *y cada* $n \in \mathbb{N}$*, la aplicación*

$$M_n(f)\colon M_n(A) \to M_n(B),$$

definida por $M_n(f)\big((a_{ij})\big) := \big(f(a)_{ij}\big)$*, es un morfismo de anillos.*

EJEMPLO 4.6. *La aplicación* $\theta\colon \mathbb{C} \to \mathrm{M}_2(\mathbb{R})$*, dada por*

$$\theta(a+bi) := \begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

es un monomorfismo de anillos. Por lo tanto $\mathbb{C}$ *es isomorfo a un subanillo de* $\mathrm{M}_2(\mathbb{R})$*. Notemos que* $\det(\theta(z)) = |z|^2$ *para todo* $z \in \mathbb{C}$ *y que si* $S^1 := \{z \in \mathbb{C} : |z| = 1\}$*, entonces* $\theta(S^1) = \mathrm{SO}(2)$*, donde* $\mathrm{SO}(2) := \mathrm{SO}(\mathbb{R}^2)$*, es el grupo ortogonal del espacio euclideano usual* $\mathbb{R}^2$*.*

5. Núcleo e imagen

El *núcleo* $\ker f$ de un morfismo de anillos $f\colon A \to B$ es la preimagen de 0 por f. Es evidente que $\ker f$ es un ideal de A e $\operatorname{Im} f$ es un subanillo de B. Más aún, es fácil verificar que:

1. La imagen de un subanillo de A es un subanillo de B.
2. La preimagen de un subanillo de B es un subanillo de A.
3. La imagen de un ideal a izquierda, a derecha o bilátero de A, es un ideal del mismo tipo de $f(A)$.
4. La preimagen de un ideal a izquierda, a derecha o bilátero de B, es un ideal del mismo tipo de A.

Usando las igualdades

$$f^{-1}(f(I)) = I + \ker f \qquad \text{y} \qquad f(f^{-1}(J)) = J \cap \operatorname{Im} f,$$

válidas para cada subgrupo aditivo I de A y cada subconjunto J de B, se comprueba fácilmente que si f es sobreyectivo, entonces:

1. Las correspondencias definidas en los items 1) y 2) inducen por restricción y correstricción un isomorfismo entre el reticulado de los subanillos de A que contienen a $\ker f$ y el de los subanillos de B.
2. Las correspondencias definidas en los items 3) y 4) inducen por restricción y correstricción un isomorfismo entre los reticulados de los ideales a izquierda, a derecha o biláteros de A que contienen a $\ker f$ y el de los ideales del mismo tipo de B.

OBSERVACIÓN 5.1. *Un morfismo de anillos* $f\colon A \to B$*, manda* $a, a' \in A$ *al mismo elemento de* B *si y sólo si* $a - a' \in \ker f$*. En particular,* f *es inyectiva si y sólo si* $\ker f = 0$*.*

6. Cociente de anillos por ideales

Fijados un anillo A y un subgrupo aditivo I de A, consideremos el grupo cociente A/I de A por I. Recordemos que para cada $a \in A$, el símbolo $[a]$ denota a la clase de a en A/I y que la proyección canónica $\pi\colon A \to A/I$ es un morfismo de grupos. Afirmamos que A/I tiene

un producto tal que π es un morfismo de anillos si y sólo si I es un ideal de A. Para que π respete el producto, forzosamente la multiplicación de A/I deberá estár dada por

$$[a][a'] = [aa']. \tag{38}$$

Así, si esta definición es correcta, entonces

$$a, a'' \in A \text{ y } a' \in I \Rightarrow [a][a'][a''] = [a][0][a''] = [a0a''] = [0] = [aa'a''] \Rightarrow aa'a'' \in I,$$

y, por lo tanto, I es un ideal bilátero. Recíprocamente, si este es el caso, entonces para todo $a, a' \in A$ y todo $y, y' \in I$,

$$[a+y][a'+y'] = [(a+y)(a'+y')] = [aa' + ay' + ya' + y'y'] = [aa'] = [a][a'],$$

de modo que la definición (38) es correcta. Las igualdades

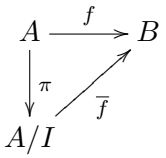
$$([a][a'])[a''] = [aa'][a''] = [(aa')a''] = [a(a'a'')] = [a][a'a''] = [a]([a'][a'']),$$
$$[a]([a']+[a'']) = [a]([a'+a'']) = [a(a'+a'')] = [aa'+aa''] = [aa']+[aa''] = [a][a']+[a][a'']$$

y

$$([a]+[a'])[a''] = ([a+a'])[a''] = [(a+a')a''] = [aa''+a'a''] = [aa'']+[a'a''] = [a][a'']+[a'][a''],$$

muestran que la multiplicación de A/I es asociativa y distribuye con respecto a la suma. Además La identidad de A/I es la clase $[1]$ del 1. Como $\ker \pi = I$, todo ideal de A es el núcleo de un morfismo. Finalmente $\pi\colon A \to A/I$ tiene la siguiente propiedad, llamada *propiedad universal del cociente*:

- Para cada morfismo de anillos $f\colon A \to B$ tal que $I \subseteq \ker f$ existe un único morfismo de anillos $\overline{f}\colon A/I \to B$ tal que el triángulo



  conmuta.

Una forma cómoda de comprobar esto, es recordar que, por la correspondiente propiedad universal del cociente de grupos, si f es un morfismo del grupo aditivo subyacente a A en el subyacente a B, entonces existe un único morfismo de grupos $\overline{f}$ tal que $\overline{f} \circ \pi = f$, y notar que, si f es un morfismo de anillos, entonces

$$\overline{f}([a])\overline{f}([a']) = f(a)f(a') = f(aa') = \overline{f}([a][a']) \quad \text{y} \quad \overline{f}([1]) = f(1) = 1_B.$$

Por la Observación 13.2 del Capítulo 1 sabemos que $\ker \overline{f} = \pi(\ker f)$ e $\operatorname{Im} \overline{f} = \operatorname{Im} f$. En particular, $A/\ker f$ es isomorfo a $\operatorname{Im} f$. Además, como grupo aditivo, $\pi(\ker f) = \ker f/I$.

Observación 6.1. *Una manera equivalente de formular la propiedad universal del cociente es decir que la correspondencia*

$$\begin{aligned} \operatorname{Hom}(A/I, B) &\longrightarrow \operatorname{Hom}(A, B) \\ \overline{f} &\longmapsto \overline{f} \circ \pi \end{aligned}$$

es inyectiva y su imagen es $\{f \in \operatorname{Hom}(A, B) : f(I) = 0\}$.

Observación 6.2. *Por la propiedad universal del cociente, si I y J son ideales de un anillo A tales que $I \subseteq J$, entonces existe un único morfismo $\overline{\pi}_J \colon A/I \to A/J$ tal que el triángulo*

$$\begin{array}{ccc} A & \xrightarrow{\pi_J} & A/J \\ \downarrow{\scriptstyle \pi_I} & \nearrow_{\overline{\pi}_J} & \\ A/I & & \end{array},$$

donde π_I y π_J son las proyecciones canónicas, conmuta. Además $\overline{\pi}_J$ es sobreyectivo, el subgrupo J/I de A/I es un ideal bilátero de A/I y $\ker(\overline{\pi}_J) = \pi_I(J) = J/I$. Por lo tanto $\overline{\pi}_J$ induce un isomorfismo $(A/I)/(J/I) \simeq A/J$.

Observación 6.3. *Supongamos que $f \colon A \to B$ es un morfismo de anillos y que J es un ideal de B. Denotemos con $\tilde{f} \colon A \to B/J$ a la composición de f con la proyección canónica $\pi \colon B \to B/J$. Es evidente que $\operatorname{Im} \tilde{f} = (f(A) + J)/J$ y $\ker \tilde{f} = f^{-1}(J)$. En consecuencia, por la propiedad universal del cociente, $\tilde{f}$ induce un isomorfismo $\overline{f} \colon A/f^{-1}(J) \to (f(A) + J)/J$. En particular, si A es un subanillo de B, entonces $A/(A \cap J) \simeq (A + J)/J$.*

Ejercicio 6.4. *Pruebe que si $f \colon A \to B$ es un morfismo sobreyectivo de anillos e I es un ideal de A, entonces $A/(I + \ker f) \simeq B/f(I)$.*

Observación 6.5. *Consideremos un ideal I de un anillo A. Del isomorfismo que hay entre el reticulado de los ideales de A que contienen a I y el de los ideales de A/I se sigue que I es maximal si y sólo si $A/I \neq 0$ y no tiene ideales no triviales. En particular, debido a la Proposición 3.4, si A es conmutatico, entonces I es maximal si y sólo si A/I es un cuerpo.*

Corolario 6.6. *Para cada anillo conmutativo A, hay un morfismo sobreyectivo de A en un cuerpo.*

Demostración. Para cada ideal maximal I de A, el cociente A/I es un anillo conmutativo sin ideales no triviales. En consecuencia, por la Proposición 3.4, es un cuerpo. Es evidente que podemos tomar como el morfismo en cuestión, la proyección canónica de A en A/I. □

Proposición 6.7. *Consideremos un morfismo de anillos $f \colon A \to B$. Si I y J son ideales de A y B tales que $f(I) \subseteq J$, entonces existe un único morfismo de anillos $\overline{f} \colon A/I \to B/J$ tal que el diagrama*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \pi_I} & & \downarrow{\scriptstyle \pi_J} \\ A/I & \xrightarrow{\overline{f}} & B/J, \end{array}$$

donde $\pi_I \colon A \to A/I$ y $\pi_J \colon B \to B/J$ son las proyecciones canónicas, conmuta. Además, $\operatorname{Im} \overline{f} = (J + \operatorname{Im} f)/J$ y $\ker \overline{f} = f^{-1}(J)/I$.

Demostración. Es una consecuencia inmediata de la propiedad universal de π_I y de que $\operatorname{Im}(\pi_J \circ f) = \pi_J(\operatorname{Im} f)$ y $\ker(\pi_J \circ f) = f^{-1}(J)$. □

Observación 6.8. *La correspondencia introducida en la proposición anterior tiene las siguientes propiedades:*

1. *$\overline{\mathrm{id}_A} \colon A/I \to A/I$ es la aplicación identidad de A/I.*

2. *Si $f\colon A \to B$ y $g\colon B \to C$ son morfismos de anillos, e I, J y K son ideales de A, B y C respectivamente, tales que $f(I) \subseteq J$ y $g(J) \subseteq K$, entonces*
$$g(f(I)) \subseteq K \quad y \quad \overline{g \circ f} = \overline{g} \circ \overline{f}.$$

EJERCICIO 6.9. *Pruebe que si $f\colon A \to B$ es un morfismo de anillos y J es un ideal de B, entonces existe un único morfismo inyectivo $\overline{f}\colon A/I \to B/J$, donde $I = f^{-1}(J)$, tal que el diagrama*
$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \pi_I} & & \downarrow{\scriptstyle \pi_J} \\ A/I & \xrightarrow{\overline{f}} & B/J, \end{array}$$
en el cual $\pi_I\colon A \to A/I$ y $\pi_J\colon B \to B/J$ son las proyecciones canónicas, conmuta. Pruebe además que $\operatorname{Im}\overline{f} = (f(A)+J)/J$.

7. Producto de anillos

El producto directo $\prod_{i\in I} A_i$, de una familia de anillos $(A_i)_{i\in I}$, es un anillo, llamado *producto directo de* $(A_i)_{i\in I}$, vía la suma y multiplicación coordenada a coordenada. Las proyecciones canónicas $\pi_j\colon \prod_{i\in I} A_i \to A_j$ son morfismos de anillos, y las definiciones de suma y producto están forzadas por este requisito. Tal como cuando trabajamos con grupos, si no hay posibilidad de confusión escribiremos $\prod A_i$ en lugar de $\prod_{i\in I} A_i$, y haremos otras simplificaciones similares siempre que, como consecuencia de las mismas, no se pierda claridad en la exposición. Además, escribiremos $A_1 \times \cdots \times A_n$ en lugar de $\prod_{i\in \mathbb{I}_n} A_n$, donde $\mathbb{I}_n$ denota al conjunto de los primeros n números naturales.

El producto directo tiene la siguiente propiedad universal:

- Para cada familia $(f_i\colon A \to A_i)_{i\in I}$ de morfismos de anillos, existe un único morfismo de anillos $\mathbf{f}\colon A \to \prod A_i$ tal que, para cada $j \in I$, el diagrama
$$\begin{array}{ccc} A & & \\ \downarrow{\scriptstyle \mathbf{f}} & \searrow^{f_j} & \\ \prod A_i & \xrightarrow{\pi_j} & A_j \end{array}$$
conmuta. Claramente $\mathbf{f}(a) = (f_i(a))_{i\in I}$ y $\ker \mathbf{f} = \bigcap \ker(f_i)$.

EJERCICIO 7.1. *Muestre que si $A = \prod A_i$, entonces $A^\times = \prod A_i^\times$.*

PROPOSICIÓN 7.2. *Para cada familia de morfismos de anillos $(f_j\colon A_j \to B_j)_{j\in J}$, existe un único morfismo de anillos*
$$\prod f_j\colon \prod A_j \to \prod B_j,$$
tal que los diagramas
$$\begin{array}{ccc} \prod A_j & \xrightarrow{\prod f_j} & \prod B_j \\ \downarrow{\scriptstyle \pi_i} & & \downarrow{\scriptstyle \pi_i} \\ A_i & \xrightarrow{f_i} & B_i \end{array}$$

conmutan.

DEMOSTRACIÓN. Se sigue de la propiedad universal del producto $\prod B_j$. □

Es fácil ver que $\prod f_j$ aplica $(a_j)_{j\in J}$ en $\big(f_j(a_j)\big)_{j\in J}$ y, usando esto, que

$$\ker\Big(\prod f_j\Big) = \prod \ker(f_j) \qquad \text{y} \qquad \operatorname{Im}\Big(\prod f_j\Big) = \prod \operatorname{Im}(f_j).$$

Por ejemplo para cada familia $(A_i)_{i\in I}$ de anillos y cada familia $(I_i)_{i\in I}$ con I_i un ideal bilátero de A_i para cada $i \in I$, las proyecciones canónicas $\pi_i\colon A_i \to A_i/I_i$ inducen un isomorfismo

$$\frac{\prod A_i}{\prod I_i} \longrightarrow \prod \frac{A_i}{I_i}.$$

OBSERVACIÓN 7.3. *La correspondencia introducida en la Proposición 7.2 tiene las siguientes propiedades:*

1. $\prod \mathrm{id}_{A_j} = \mathrm{id}_{\prod A_j}$.
2. *Para cada par* $(f_j\colon A_j \to B_j)_{j\in J}$ *y* $(g_j\colon B_j \to C_j)_{j\in J}$ *de familias de morfismos de anillos,*

$$\prod g_j \circ \prod f_j = \prod (g_j \circ f_j).$$

Para cada $i \in I$ consideremos un ideal a izquierda J_i de A_i. Es evidente que $\prod J_i$ es un ideal a izquierda de $\prod A_i$. Por supuesto que si cada J_i es un ideal a derecha de A_i, entonces $\prod J_i$ es un ideal a izquierda de $\prod A_i$. Supongamos ahora que $J \subseteq \prod A_i$ es un ideal a izquierda, derecha o bilátero de $\prod A_i$ y, para todo $i \in I$, escribamos $J_i := \pi_i(J)$. Evidentemente cada J_i es un ideal de A_i del mismo tipo que J e $J \subseteq \prod J_i$. Afirmamos que

$$\bigoplus I_i \subseteq J \subseteq \prod J_i, \tag{39}$$

donde $\bigoplus I_i$ denota al subconjunto de $\prod J_i$, formado por las uplas que tienen soporte finito. Es claro que para probar que en (39) vale la inclusión de la izquierda, será suficiente ver que, para cada $j \in I$,

$$I_j = \{a_j \in A_j : (a_j\delta_{ij})_{i\in I} \in J\}, \tag{40}$$

donde δ_{ij} denota a la delta de Kronecker definida por $\delta_{ij} = 1$ si $i = j$ y $\delta_{ij} = 0$ si $i \neq j$. Veamos ahora que la igualdad (40) se satisface. Para ello fijemos $j \in I$ y tomemos $a_j \in I_j$. Por la definición de I_j, para cada $i \neq j$, existe $a_i \in A_i$, tales que $(a_i)_{i\in I} \in J$. Denotemos con $\mathbf{e}_j$ al elemento de $\prod A_i$ que tiene 1 en la j-ésima coordenada y cero en las demás. Como

$$(a_j\delta_{ij})_{i\in I} = \mathbf{e}_j(a_i)_{i\in I} = (a_i)_{i\in I}\mathbf{e}_j,$$

en (40) vale la inclusión $\subseteq$. Dado que la otra inclusión es obvia, esto prueba que en (40) vale la igualdad. Notemos que cuando I es finito, entonces (40) dice que $J = \prod J_i$. Así, en este caso, todo ideal de $\prod A_i$ es un producto de ideales.

7.1. El teorema chino del resto

El *producto* de dos ideales I y J de un anillo A es el ideal IJ de A generado por los productos xy, con $x \in I$ e $y \in J$. Claramente IJ es el conjunto de las sumas finitas de elementos de la forma xy con $x \in I$ e $y \in J$. El producto es siempre asociativo, tiene neutro A y es distributivo respecto de la suma. En consecuencia

$$(I + J)(I \cap J) \subseteq IJ + JI \subseteq I \cap J.$$

Dos ideales I y J de A son *coprimos* si $I + J = A$. Claramente, en este caso, $IJ + JI = I \cap J$. Supongamos que I es coprimo con J y K. Entonces existen $x, y \in I$ tales que $1 - x \in J$ y $1 - y \in K$. Multiplicando obtenemos

$$1 - x - y + xy = (1 - x)(1 - y) \in JK.$$

Como $x + y - xy \in I$, esto muestra que I también es coprimo con JK.

Para cada familia $I_1, \ldots, I_n$ de ideales de A, las projecciones canónicas $\pi_i \colon A \to A/I_i$ inducen un morfismo

$$\pi \colon A \to \prod_{j=1}^{n} \frac{A}{I_j}.$$

Se comprueba inmediatamente que $\ker \pi = I_1 \cap \cdots \cap I_n$. En particular, π es inyectivo si y sólo si $I_1 \cap \cdots \cap I_n = 0$. El siguiente resultado da condiciones necesarias y suficientes para que sea sobreyectivo.

Teorema 7.4 (Teorema chino del resto). *El morfismo π es sobreyectivo si y sólo si los ideales $I_1, \ldots, I_n$ son coprimos dos a dos.*

Demostración. Supongamos que π es sobreyectivo. Tomemos $a \in A$ tal que $\pi(a)$ es la n-upla cuyas coordenadas son todas cero, salvo la i-ésima, que vale 1. Por definición esto dice que $1 - a \in I_i$ y $a \in I_j$ para todo $j \neq i$. Así, I_i es coprimo con I_j para todo $j \neq i$. Recíprocamente, si I_i es coprimo con I_j para todo $j \neq i$, entonces I_i es coprimo con $I_1 \cdots \widehat{I_i} \cdots I_n$ y, por lo tanto, existe $a_{(i)} \in I_1 \cap \cdots \cap \widehat{I_i} \cap \cdots \cap I_n$ tal que $1 - a_{(i)} \in I_i$, lo cual implica que

$$\pi\left(\sum_{i=1}^{n} a_i a_{(i)}\right) = \big([a_1], \ldots, [a_n]\big)$$

para cada n-upla $(a_1, \ldots, a_n)$ de elementos de A. □

8. Ideales primos en anillos conmutativos

En esta sección A denota a un anillo conmutativo. Un ideal propio I de A es *primo* si $ab \in I$ implica $a \in I$ o $b \in I$.

Observación 8.1. *Un ideal principal $\langle p \rangle$ de A es primo si y sólo si p no es una unidad de A y $p \mid ab$ implica $p \mid a$ o $p \mid b$. En este caso nos referiremos a p como un* elemento primo *de A.*

Proposición 8.2. *Para cada ideal I de A son equivalentes:*

1. *I es primo,*
2. *A/I es un dominio.*

DEMOSTRACIÓN. 1) $\Rightarrow$ 2). Como I es propio, $A/I \neq 0$. Supongamos ahora que $[a][a'] = 0$, donde como venimos haciendo denotamos con $[a]$ y $[a']$ a la clase en A/I de dos elementos a y a' de A. Como $[aa'] = [a][a']$ se sigue de esto que $aa' \in I$ y, en consecuencia $a \in I$ o $a' \in I$. Pero entonces $[a] = 0$ o $[a'] = 0$, de donde A/I es un dominio.
2) $\Rightarrow$ 1). Dado que $A/I \neq 0$ el ideal I es propio. Supongamos que $a, a' \in A$ satisfacen $aa' \in I$. Entonces $[a][a'] = [aa'] = 0$ en A/I y, en consecuencia, debido a la hipótesis $[a] = 0$ o $[a'] = 0$. Pero esto significa que $a \in I$ o $a' \in I$ y, por lo tanto, I es primo. □

COROLARIO 8.3. *Todo ideal maximal de un anillo conmutativo es primo.*

DEMOSTRACIÓN. Como todo cuerpo es un dominio esto se sigue de la proposición anterior y de la Observación 6.5. □

PROPOSICIÓN 8.4. *Si $f\colon A \to B$ es un morfismo de anillos conmutativos y $J \subsetneq B$ es un ideal primo de B, entonces $f^{-1}(J)$ es un ideal primo de A.*

DEMOSTRACIÓN. Como un subanillo de un dominio es un dominio, esto se sigue de la Proposición 8.2 y de que $A/f^{-1}(J)$ es un subanillo de B/J. □

Notemos que la proposición anterior no se satisface para ideales maximales. Por ejemplo el ideal 0 de $\mathbb{Q}$ es maximal, pero su preimagen por la inclusión canónica $\iota\colon \mathbb{Z} \to \mathbb{Q}$ sigue siendo 0, que no es un ideal maximal de $\mathbb{Z}$.

PROPOSICIÓN 8.5. *Si $f\colon A \to B$ es un morfismo sobreyectivo de anillos conmutativos e I es un ideal primo de A que contiene al núcleo de f, entonces $f(I)$ es un ideal primo de B.*

DEMOSTRACIÓN. Dado que, debido a las hipótesis A/I es isomorfo a $B/f(I)$, esto se sigue inmediatamente de la Proposición 8.2. □

OBSERVACIÓN 8.6. *Consideremos un anillo de polinomios $A[X_1, \ldots, X_n]$ y tomemos un polinomio no nulo*

$$P = \sum a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n} \in A[X_1, \ldots, X_n].$$

El grado total de P *es por definición*

$$\operatorname{grt}(P) := \operatorname{máx}\{i_1 + \cdots + i_n : a_{i_1,\ldots,i_n} \neq 0\}.$$

Recordemos que un monomio es un polinomio de la forma $a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$ con $a_{i_1,\ldots,i_n} \neq 0$ y que un polinomio es homogeneo si es cero o si todos sus monomios tiene el mismo grado total. Notemos que hay monomios distintos que tienen el mismo coeficiente y el mismo grado total. A continuación vamos a subsanar esto. Para empezar definimos un orden total sobre $\mathbb{N}^n$ por $(i_1, \ldots, i_n) < (j_1, \ldots, j_n)$ si $i_1 + \cdots + i_n < j_1 + \cdots + j_n$ o si $i_1 + \cdots + i_n = j_1 + \cdots + j_n$ y existe $1 \leq j \leq n$ tal que $i_i = j_i$ para $i < j$ y $i_j < j_j$. El grado de P es por definición

$$\operatorname{gr}(P) := \operatorname{máx}\{(i_1, \ldots, i_n) : a_{i_1,\ldots,i_n} \neq 0\}.$$

Así el grado de P es el máximo de los grados de sus monomios. El coeficiente principal $\operatorname{cpal}(P)$ *de P es el coeficiente de su monomio de grado máximo. Así si $\operatorname{gr}(P) = (r_1, \ldots, r_n)$, entonces*

$$P = \operatorname{cpal}(P)\, X_1^{r_1} \ldots X_n^{r_n} + \textit{ suma de monomios de grado menor.}$$

Es fácil ver que si $Q \in A[X_1, \ldots, X_n]$ es otro polinomio no nulo y $\operatorname{gr}(Q) = (s_1, \ldots, s_n)$, entonces

$$PQ = \operatorname{cpal}(P)\operatorname{cpal}(Q)\, X_1^{r_1+s_1} \ldots X_n^{r_n+s_n} + \textit{ suma de monomios de grado menor.} \tag{41}$$

Por lo tanto

$$PQ = 0 \ o \ \operatorname{gr}(PQ) \leq \operatorname{gr}(P) + \operatorname{gr}(P) \tag{42}$$

y

$$PQ \neq 0 \ y \ \operatorname{gr}(PQ) = \operatorname{gr}(P) + \operatorname{gr}(P) \Longleftrightarrow \operatorname{cpal}(P)\operatorname{cpal}(Q) \neq 0. \tag{43}$$

Un argumento inductivo usando (41) *muestra que, para todo* $m \in \mathbb{N}$*,*

$$P^m = \operatorname{cpal}(P)^m X_1^{mr_1} \dots X_n^{mr_n} + \textit{suma de monomios de grado menor.} \tag{44}$$

Así

$$P^m \neq 0 \ y \ \operatorname{gr}(P^m) = m \operatorname{gr}(P) \Longleftrightarrow \operatorname{cpal}(P)^m \neq 0. \tag{45}$$

Proposición 8.7. *Para cada anillo conmutativo* A *y cada* $n \in \mathbb{N}$ *son equivalentes:*

1. A *es un dominio.*
2. $A[X_1, \dots, X_n]$ *es un dominio.*

Demostración. 1) $\Rightarrow$ 2) Por la equivalencia (43).
2) $\Rightarrow$ 1) Porque evidentemente todo subanillo de un dominio es un dominio. □

Observación 8.8. *Consideremos el anillo de polinomios* $A[X_1, \dots, X_n]$ *en varias variables, un ideal* I *de* A *y el morfismo*

$$\theta \colon A[X_1, \dots, X_n] \longrightarrow \frac{A}{I}[X_1, \dots, X_n],$$

definido por

$$\theta\left(\sum a_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n}\right) = \sum [a_{i_1,\dots,i_n}] X_1^{i_1} \dots X_n^{i_n},$$

donde para cada $a \in A$*, denotamos con* $[a]$ *a la clase de* a *en* A/I*. Es evidente que el núcleo de* θ *es*

$$I[X_1, \dots, X_n] := \{P \in A[X_1, \dots, X_n] : \textit{los coeficientes de } P \textit{ están en } I\}.$$

Por lo tanto

$$\frac{A}{I}[X_1, \dots, X_n] \simeq \frac{A[X_1, \dots, X_n]}{I[X_1, \dots, X_n]}. \tag{46}$$

Notemos que $I[X_1, \dots, X_n]$ *es el ideal* $IA[X_1, \dots, X_n]$*, de* $A[X_1, \dots, X_n]$*, generado por* I*.*

Proposición 8.9. *Un ideal* I *de* A *es primo si y sólo si* $I[X_1, \dots, X_n]$ *lo es.*

Demostración. En efecto, como un anillo de polinomios es un dominio si y sólo si su anillo de coeficientes lo es, se sigue de (46) y de la Proposición 8.2, que

$$\begin{aligned} I \text{ es primo} &\Longleftrightarrow \frac{A}{I} \text{ es un dominio} \\ &\Longleftrightarrow \frac{A[X_1, \dots, X_n]}{I[X_1, \dots, X_n]} \text{ es un dominio} \\ &\Longleftrightarrow I[X_1, \dots, X_n] \text{ es primo,} \end{aligned}$$

como queremos. □

Corolario 8.10. *Si* $p \in A$ *es primo, entonces* p *es primo como elemento de* $A[X_1, \dots, X_n]$*.*

9. Ideales radicales en anillos conmutativos

En esta sección A denota a un anillo conmutativo. Un ideal I de A es *radical* si $a^n \in I$ implica $a \in I$ (donde n es un número natural cualquiera). Es obvio que que todo ideal primo es radical.

Observación 9.1. *Es evidente que la intersección de una familia de ideales radicales de A es un ideal radical. Para cada ideal I de A, denotaremos con* $\mathrm{r}(I)$*, y llamaremos* radical de I*, al mínimo ideal radical de A que contiene a I. Debido a la Proposición 3.1 y el Corolario 8.3, si I es un ideal propio de A, entonces* $\mathrm{r}(I)$ *también lo es.*

A $\mathrm{Nil}(A) := \mathrm{r}(0)$ se lo llama el *nilradical* de A. Decimos que A es *reducido* si $A \neq 0$ y su nilradical es cero.

Proposición 9.2. *Para todo ideal I de A,*

$$\mathrm{r}(I) = \{a \in A : \textit{existe } n \in \mathbb{N}, \textit{ tal que } a^n \in I\}.$$

Demostración. Denotemos con J al conjunto de la derecha de esta igualdad. Es evidente que $I \subseteq J \subseteq \mathrm{r}(I)$. Por lo tanto, para demostrar la proposición será suficiente ver que J es un ideal radical de A. Tomemos $a, b \in A$ tales que existen n y m en $\mathbb{N}$ tal que $a^n \in I$ y $b^m \in I$. Evidentemente

$$(a+b)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} a^i b^{m+n-i-1} \in I.$$

Así, J es un grupo aditivo. Dado que si $a^n \in I$, entonces $(ab)^n = a^n b^n \in I$, también es un ideal. Para terminar la demostración resta ver que si $a^n \in J$, entonces $a \in J$. Pero si $a^n \in J$, entonces por definición existe $m \in \mathbb{N}$ tal que $a^{nm} = (a^n)^m \in I$ y, por lo tanto, $a \in J$. □

Proposición 9.3. *Para cada par de ideales I y J de A vale lo siguiente:*

1. *Si $I \subseteq J$, entonces* $\mathrm{r}(I) \subseteq \mathrm{r}(J)$.
2. $\mathrm{r}(I)$ *es un ideal radical (es decir* $\mathrm{r}(\mathrm{r}(I)) = \mathrm{r}(I)$*).*
3. *Si* $\mathrm{r}(IJ) = \mathrm{r}(I \cap J) = \mathrm{r}(I) \cap \mathrm{r}(J)$.
4. $\mathrm{r}(I + J) = \mathrm{r}(\mathrm{r}(I) + \mathrm{r}(J))$.
5. *I y J son coprimos si y sólo si* $\mathrm{r}(I)$ *y* $\mathrm{r}(J)$ *lo son.*

Demostración. 1) Es trivial.

2) Es trivial.

3) Del item 1) se sigue que $\mathrm{r}(IJ) \subseteq \mathrm{r}(I \cap J) \subseteq \mathrm{r}(I) \cap \mathrm{r}(J)$. Tomemos ahora $a \in \mathrm{r}(I) \cap \mathrm{r}(J)$. Por la Proposición 9.2 existen $n, m \in \mathbb{N}$ tales que $a^n \in I$ y $a^m \in J$. Por lo tanto $a^{n+m} = a^n a^m \in IJ$ y, así, $a \in \mathrm{r}(IJ)$.

4) Es evidente que $\mathrm{r}(I) + \mathrm{r}(J) \subseteq \mathrm{r}(I + J) \subseteq \mathrm{r}(\mathrm{r}(I) + \mathrm{r}(J))$. Así, dado que $\mathrm{r}(I + J)$ es radical, necesariamente vale la igualdad del enunciado.

5) Es obvio que si I y J son coprimos, entonces $\mathrm{r}(I)$ y $\mathrm{r}(J)$ también lo son. Supongamos ahora que esto último ocurre. Por el item 4) sabemos que $\mathrm{r}(I + J) = A$. Pero entonces $I + J = A$, ya que el radical de un ideal propio también lo es. □

Teorema 9.4. *Para cada ideal propio I de A,*

$$\mathrm{r}(I) = \bigcap_{\{P \textit{ primo tal que } I \subseteq P\}} P.$$

Demostración. Es evidente que vale la inclusión $\subseteq$. Debemos ver que si $a \notin \mathrm{r}(I)$, entonces existe un ideal primo P de A que contiene a I y tal que $a \notin P$. Por la Proposición 9.2 el conjunto $\{a^n : n \in \mathbb{N}\}$ no corta a I. Consideremos el conjunto $\mathcal{P}$ de los ideales a izquierda propios de A que contienen a I y no cortan a $\{a^n : n \in \mathbb{N}\}$. Notemos que $\mathcal{P}$ no es vacío pues $I \in \mathcal{P}$. Por el lema de Zermelo podemos tomar una cadena maximal $(I_j)_{j\in J}$ de elementos de $\mathcal{P}$. Es evidente que $P := \bigcup I_j$ no contiene a a. Así, para terminar la demostración bastará ver que P es primo. Supongamos que $x, y \in A \setminus P$ y que $xy \in P$. Como $(I_j)_{j\in J}$ es maximal y $P \subsetneq P + \langle x\rangle$, existe $n \in \mathbb{N}$ tal que $a^n \in P + \langle x\rangle$. Similarmente existe $m \in \mathbb{N}$ tal que $a^m \in P + \langle y\rangle$. Pero entonces $a^{n+m} \in (P + \langle x\rangle)(P + \langle y\rangle) \subseteq P$, lo que es imposible, pues, debido a la definición de P, esto implica que $a^{n+m} \in I_j$ para algún $j \in J$. □

Proposición 9.5. *Para cada ideal I de A son equivalentes:*

1. *I es propio y radical,*
2. *A/I es reducido.*

Demostración. 1) $\Rightarrow$ 2). Como I es propio, $A/I \neq 0$. Supongamos ahora que $[a]^n = 0$, donde como venimos haciendo denotamos con $[a]$ a la clase en A/I de un elemento a de A. Como $[a^n] = [a]^n$ se sigue de esto que $a^n \in I$ y, en consecuencia $a \in I$. Pero entonces $[a] = 0$, de donde A/I es reducido.
2) $\Rightarrow$ 1). Dado que $A/I \neq 0$ el ideal I es propio. Supongamos que $a \in A$ satisfacen $a^n \in I$. Entonces $[a]^n = [a^n] = 0$ en A/I y, en consecuencia, debido a la hipótesis $[a] = 0$. Pero esto significa que $a \in I$, y que por lo tanto, I es radical. □

Proposición 9.6. *Si $f\colon A \to B$ es un morfismo de anillos conmutativos y J es un ideal propio y radical de B, entonces $f^{-1}(J)$ es un ideal propio y radical de A.*

Demostración. Como un subanillo de un anillo reducido es un anillo reducido, esto se sigue de la Proposición 8.2 y de que $A/f^{-1}(J)$ es un subanillo de B/J. □

Proposición 9.7. *Si $f\colon A \to B$ es un morfismo sobreyectivo de anillos conmutativos e I es un ideal propio y radical de A que contiene al núcleo de f, entonces $f(I)$ es un ideal propio y radical de B.*

Demostración. Dado que, debido a las hipótesis, A/I es isomorfo a $B/f(I)$, esto se sigue inmediatamente de la Proposición 9.5. □

Proposición 9.8. *Para cada anillo conmutativo A y cada $n \in \mathbb{N}$ son equivalentes:*

1. *A es reducido.*
2. *$A[X_1, \ldots, X_n]$ es reducido.*

Demostración. 1) $\Rightarrow$ 2) Por la equivalencia (45).
2) $\Rightarrow$ 1) Porque evidentemente todo subanillo de un anillo reducido es reducido. □

Proposición 9.9. *Un ideal I de A es propio y radical si y sólo si $I[X_1, \ldots, X_n]$ lo es.*

Demostración. En efecto, como un anillo de polinomios es reducido si y sólo si su anillo de coeficientes lo es, se sigue de (46) y de la Proposición 9.5, que

$$\begin{aligned} I \text{ es radical} &\iff \frac{A}{I} \text{ es reducido} \\ &\iff \frac{A[X_1, \ldots, X_n]}{I[X_1, \ldots, X_n]} \text{ es reducido} \\ &\iff I[X_1, \ldots, X_n] \text{ es radical,} \end{aligned}$$

como queremos. □

PROPOSICIÓN 9.10. *El nilradical de* $A[X_1, \ldots, X_n]$ *es* $\mathrm{Nil}(A)[X_1, \ldots, X_n]$.

DEMOSTRACIÓN. Como $\mathrm{Nil}(A)[X_1, \ldots, X_n]$ es el ideal de $A[X_1, \ldots, X_n]$ generado por $\mathrm{Nil}(A)$ y el nilradical de $A[X_1, \ldots, X_n]$ es un ideal que contiene a $\mathrm{Nil}(A)$, es evidente que

$$\mathrm{Nil}(A)[X_1, \ldots, X_n] \subseteq \mathrm{Nil}(A[X_1, \ldots, X_n]).$$

Dado que, debido a la proposición anterior, $\mathrm{Nil}(A)[X_1, \ldots, X_n]$ es un ideal radical, necesariamente $\mathrm{Nil}(A)[X_1, \ldots, X_n] = \mathrm{Nil}(A[X_1, \ldots, X_n])$. □

PROPOSICIÓN 9.11. *Consideremos un polinomio*

$$P = \sum a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n} \in A[X_1, \ldots, X_n].$$

Son equivalentes:

1. *P es inversible.*
2. *El término independiente $a_{0,\ldots,0}$ de P es inversible, y los demás coeficientes $a_{i_1,\ldots,i_n}$ con $(i_1, \ldots, i_n) \neq (0, \ldots, 0)$, son nilpotentes.*

DEMOSTRACIÓN. 1) $\Rightarrow$ 2) Para cada ideal primo I de A, consideremos el morfismo θ definido en la Observación 8.8. Como

$$\theta(P) = \sum [a_{i_1,\ldots,i_n}] X_1^{i_1} \ldots X_n^{i_n} \in \frac{A}{I}[X_1, \ldots, X_n]$$

es inversible, se sigue de la equivalencia (43), que

$$[a_{0,\ldots,0}] \text{ es inversible} \quad \text{y} \quad [a_{i_1,\ldots,i_n}] = 0 \quad \text{para todo } (i_1, \ldots, i_n) \neq (0, \ldots, 0).$$

Por lo tanto, para cada ideal primo I de A,

$$a_{0,\ldots,0} \notin I \quad \text{y} \quad a_{i_1,\ldots,i_n} \in I \quad \text{para todo } (i_1, \ldots, i_n) \neq (0, \ldots, 0).$$

En consecuencia, por la Proposición 3.1, el Corolario 8.3 y el Teorema 9.4

$$a_{0,\ldots,0} \text{ es inversible} \quad \text{y} \quad a_{i_1,\ldots,i_n} \in \mathrm{Nil}(A) \quad \text{para todo } (i_1, \ldots, i_n) \neq (0, \ldots, 0),$$

como querenos.

2) $\Rightarrow$ 1) Por las Proposiciones 9.10 y 1.10(4). □

COROLARIO 9.12. *Para cada anillo conmutativo A son equivalentes:*

1. *A es reducido*
2. *$A \neq 0$ y $A[X_1, \ldots, X_n]^\times = A^\times$.*

DEMOSTRACIÓN. Por la proposición anterior. □

10. El cuerpo de cocientes de un dominio conmutativo

En esta sección construímos el cuerpo de cocientes de un dominio conmutativo y estudiamos sus propiedades básicas. La construcción es una generalización directa de la de los números racionales a partir de los enteros.

Dado un dominio conmutativo A consideremos la relación $\sim$, definida en $A \times (A \setminus \{0\})$, por $(p, q) \sim (r, s)$ si $ps = rq$. Un cálculo directo muestra que $\sim$ es reflexiva, simétrica y transitiva.

Para cada $p \in A$ y $q \in A \setminus \{0\}$, la *fracción* de *numerador* p y *denominador* q es la clase $\frac{p}{q}$ de (p,q) en $(A \times (A \setminus \{0\}))/\sim$. Definimos la suma y el producto de fracciones por

$$\frac{p}{q} + \frac{r}{s} = \frac{ps+qr}{qs} \qquad \text{y} \qquad \frac{p}{q}\frac{r}{s} = \frac{pr}{qs},$$

respectivamente. Es fácil ver que estas definiciones son correctas. Esto es, que no dependen de los representantes (p,q) y (r,s) elegidos. Denotamos con el símbolo $\mathbb{Q}_A$, y llamamos *cuerpo de cocientes* de A, al conjunto $(A \times (A \setminus \{0\}))/\sim$, provisto de estas operaciones.

Teorema 10.1. *El cuerpo de cocientes de A es, efectivamente, un cuerpo. Además, la aplicación*

$$\begin{aligned} A &\longrightarrow \mathbb{Q}_A \\ a &\longmapsto \tfrac{a}{1} \end{aligned}$$

es un morfismo inyectivo de anillos, que tiene la siguiente propiedad universal: dados un cuerpo k y un morfismo inyectivo $f\colon A \to k$, existe un único morfismo de cuerpos $\tilde{f}\colon \mathbb{Q}_A \to k$ tal que el triángulo

$$\begin{array}{ccc} A & \xrightarrow{f} & k \\ {\scriptstyle \iota}\downarrow & \nearrow_{\tilde{f}} & \\ \mathbb{Q}_A & & \end{array}$$

conmuta.

Demostración. Las igualdades

$$\begin{aligned}
&\Big(\frac{p}{q} + \frac{r}{s}\Big) + \frac{t}{u} = \frac{ps+qr}{qs} + \frac{t}{u} = \frac{psu+qru+qst}{qsu} = \frac{p}{q} + \frac{ru+st}{su} = \frac{p}{q} + \Big(\frac{r}{s} + \frac{t}{u}\Big), \\
&\frac{p}{q} + \frac{r}{s} = \frac{ps+qr}{qs} = \frac{rq+sp}{sq} = \frac{r}{s} + \frac{p}{q}, \\
&\frac{p}{q} + \frac{0}{1} = \frac{p1+q0}{q1} = \frac{p}{q}, \\
&\frac{p}{q} + \frac{-p}{q} = \frac{pq-qp}{q^2} = \frac{0}{q^2} = \frac{0}{1}, \\
&\Big(\frac{p}{q}\frac{r}{s}\Big)\frac{t}{u} = \frac{pr}{qs}\frac{t}{u} = \frac{prt}{qsu} = \frac{p}{q}\frac{rt}{su} = \frac{p}{q}\Big(\frac{r}{s}\frac{t}{u}\Big), \\
&\frac{p}{q}\frac{r}{s} = \frac{pr}{qs} = \frac{rp}{sq} = \frac{r}{s}\frac{p}{q}, \\
&\frac{p}{q}\frac{1}{1} = \frac{p1}{q1} = \frac{p}{q}
\end{aligned}$$

y

$$\frac{p}{q}\Big(\frac{r}{s} + \frac{t}{u}\Big) = \frac{p}{q}\frac{ru+st}{su} = \frac{pru+pst}{qsu} = \frac{prqu+qspt}{qsqu} = \frac{pr}{qs} + \frac{pt}{qu} = \frac{p}{q}\frac{r}{s} + \frac{p}{q}\frac{t}{u},$$

muestran que $\mathbb{Q}_A$ es un anillo conmutativo con neutro aditivo $\frac{0}{1}$ y neutro multiplicativo $\frac{1}{1}$. Además, es obvio que si $p \neq 0$, entonces $\frac{p}{q}$ es inversible, con inversa $\frac{q}{p}$. Como $\frac{0}{q} = \frac{0}{1}$ para todo

q, esto prueba que $\mathbb{Q}_A$ es un cuerpo. Para ver que $\iota\colon A \to \mathbb{Q}_A$ es un morfismo inyectivo es suficiente notar que

$$\frac{p}{1}+\frac{r}{1}=\frac{p+r}{1}, \quad \frac{p}{1}\frac{r}{1}=\frac{pr}{1} \quad \text{y que} \quad \frac{p}{1}=\frac{r}{1}\Rightarrow p=r.$$

Supongamos ahora que $f\colon A \to k$ es un morfismo inyectivo de A en un cuerpo. Si $\tilde{f}\colon \mathbb{Q}_A \to k$ es un morfismo de cuerpos tal que $\tilde{f}\circ\iota = f$, entonces obligatoriamente

$$\tilde{f}\Big(\frac{p}{q}\Big)=\tilde{f}\Big(\frac{p}{1}\Big)\tilde{f}\Big(\frac{1}{q}\Big)=\tilde{f}\Big(\frac{p}{1}\Big)\tilde{f}\Big(\frac{q}{1}\Big)^{-1}=f(p)f(q)^{-1}.$$

Dejamos como tarea para el lector comprobar que si $\frac{p}{q}=\frac{r}{s}$, entonces $f(p)f(q)^{-1}=f(r)f(s)^{-1}$, y que la fórmula $\tilde{f}\big(\frac{p}{q}\big)=f(p)f(q)^{-1}$ define un morfismo de anillos. □

NOTA 10.2. *Es usual identificar $a \in A$ con $\iota(a)=\frac{a}{1}$.*

11. Extensiones cuadráticas de $\mathbb{Q}$

Consideremos un número entero d que no es un cuadrado. El subanillo $\mathbb{Q}[\sqrt{d}]$ de $\mathbb{C}$ está formado por los elementos de la forma $a+b\sqrt{d}$, con $a,b\in\mathbb{Q}$. Como $\sqrt{d}\notin\mathbb{Q}$ es claro que si $a+b\sqrt{d}=a'+b'\sqrt{d}$, entonces $a=a'$ y $b=b'$, de modo que esta escritura es única. Notemos que $\mathbb{Q}[\sqrt{d}]$ es un subanillo de $\mathbb{R}$ si y sólo si $d>0$. Denotamos con $\mathbb{Z}[\sqrt{d}]$ al subanillo de $\mathbb{Q}[\sqrt{d}]$ obtenido considerando los elementos de la forma $a+b\sqrt{d}$, con $a,b\in\mathbb{Z}$. Los Ejemplos 2.4 y 2.5 son los casos particulares obtenidos tomando $d=-1$ y $d=3$ respectivamente. Escribamos $d=d'e^2$ con d' libre de cuadrados (es decir que ningún primo aparece a una potencia mayor que uno en la factorización de d). Es evidente que $\mathbb{Q}[\sqrt{d'}]=\mathbb{Q}[\sqrt{d}]$, pero que $\mathbb{Z}[\sqrt{d'}]=\mathbb{Z}[\sqrt{d}]$, sólo si $d'=d$.

Para cada $x=a+b\sqrt{d}\in\mathbb{Q}[\sqrt{d}]$ definimos el *conjugado* de x por $\overline{x}:=a-b\sqrt{d}$. Es evidente que

$$\overline{\overline{x}}=x, \quad \overline{x}=x\Leftrightarrow x\in\mathbb{Q}, \quad \overline{x}=-x\Leftrightarrow x\in\mathbb{Q}\sqrt{d} \quad \text{y} \quad x\in\mathbb{Z}[\sqrt{d}]\Leftrightarrow\overline{x}\in\mathbb{Z}[\sqrt{d}].$$

Además es fácil ver que

$$\overline{x+y}=\overline{x}+\overline{y} \quad \text{y} \quad \overline{xy}=\overline{x}\,\overline{y} \qquad \text{para todo } x,y\in\mathbb{Q}[\sqrt{d}].$$

En efecto, la primera igualdad es sencilla y por la $\mathbb{Q}$-bilinealidad es suficiente comprobar la segunda para $x,y\in\{1,\sqrt{d}\}$, casos en lo que es evidente. Por lo tanto la conjugación es un automorfismo de $\mathbb{Q}[\sqrt{d}]$ que induce por restricción y correstricción un automorfismo en $\mathbb{Z}[\sqrt{d}]$. En particular $x\in\mathbb{Z}[\sqrt{d}]$ es inversible si y sólo si $\overline{x}$ lo es.

Definimos la *norma* $\mathrm{N}(x)$ de $x\in\mathbb{Q}[\sqrt{d}]$ por $\mathrm{N}(x):=x\overline{x}$. Un cálculo directo muestra que si $x=a+b\sqrt{d}$ con $a,b\in\mathbb{Q}$, entonces

$$\mathrm{N}(x)=(a+b\sqrt{d})(a-b\sqrt{d})=a^2-b^2d\in\mathbb{Q}.$$

Como d no es un cuadrado, $x\neq 0$ si y sólo si $\mathrm{N}(x)\neq 0$. En consecuencia, si $x\neq 0$,

$$x\,\frac{1}{\mathrm{N}(x)}\overline{x}=\frac{1}{\mathrm{N}(x)}x\,\overline{x}=\frac{1}{\mathrm{N}(x)}\,\mathrm{N}(x)=1,$$

y, así, $\mathbb{Q}[\sqrt{d}]$ es un subcuerpo de $\mathbb{C}$. Notemos ahora que

$$\mathrm{N}(xy)=xy\overline{x}\overline{y}=xy\overline{y}\,\overline{x}=x\,\mathrm{N}(y)\overline{x}=x\,\overline{x}\,\mathrm{N}(y)=\mathrm{N}(x)\,\mathrm{N}(y) \quad \text{para todo } x,y\in\mathbb{Q}[\sqrt{d}].$$

Es evidente que la norma define una aplicación multiplicativa de $\mathbb{Z}[\sqrt{d}]$ sobre $\mathbb{Z}$.

PROPOSICIÓN 11.1. *Para cada número entero d que no es un cuadrado,*

$$\mathbb{Z}[\sqrt{d}]^\times = \left\{ x \in \mathbb{Z}[\sqrt{d}] : \mathrm{N}(x) \in \mathbb{Z}^\times \right\}.$$

DEMOSTRACIÓN. Tomemos $x \in \mathbb{Z}[\sqrt{d}]^\times$. Como $1 = \mathrm{N}(1) = \mathrm{N}(xx^{-1}) = \mathrm{N}(x)\,\mathrm{N}(x^{-1})$, es evidente que

$$\mathbb{Z}[\sqrt{d}]^\times \subseteq \left\{ x \in \mathbb{Z}[\sqrt{d}] : \mathrm{N}(x) \in \mathbb{Z}^\times \right\}.$$

Tomemos ahora $x \in \mathbb{Z}[\sqrt{d}]$ tal que $\mathrm{N}(x) \in \{\pm 1\}$. Como $x\,\overline{x} = \mathrm{N}(x)$ es claro que x es inversible y que $\overline{x} = \mathrm{N}(x)^{-1}\overline{x}$. □

COROLARIO 11.2. *Para cada entero d que no es un cuadrado, vale lo siguiente:*

1. *Si $d \leq -2$, entonces $\mathbb{Z}[\sqrt{d}]^\times = \{\pm 1\}$,*
2. *$\mathbb{Z}[\sqrt{-1}]^\times = \{\pm 1, \pm\sqrt{-1}\}$.*

DEMOSTRACIÓN. 1) Tomemos $x = a + b\sqrt{d}$. Por la proposición anterior x es unidad si y sólo si $a^2 - b^2 d = 1$. Como $a^2 - b^2 d \geq a^2 + 2b^2$, de esto se sigue que $\mathbb{Z}[\sqrt{d}]^\times = \{\pm 1\}$.
2) Tomemos $x = a + b\sqrt{-1}$. Por la proposición anterior x es unidad si y sólo si $a^2 + b^2 = 1$. Así $\mathbb{Z}[\sqrt{-1}]^\times = \{\pm 1, \pm\sqrt{-1}\}$. □

Definimos la *traza* $\mathrm{Tr}(x)$ de $x \in \mathbb{Q}[\sqrt{d}]$ por $\mathrm{Tr}(x) := x + \overline{x}$. Claramente si $x = a + b\sqrt{d}$, entonces $\mathrm{Tr}(x) = 2a$. Escribamos

$$\overline{\mathbb{Z}[\sqrt{d}]} := \left\{ x \in \mathbb{Q}[\sqrt{d}] : \mathrm{Tr}(x) \in \mathbb{Z} \text{ y } \mathrm{N}(x) \in \mathbb{Z} \right\}.$$

Es evidente que $x \in \overline{\mathbb{Z}[\sqrt{d}]}$ si y sólo si $\overline{x} \in \overline{\mathbb{Z}[\sqrt{d}]}$.

PROPOSICIÓN 11.3. *Supongamos que $d \in \mathbb{Z}$ es libre de cuadrados. Vale lo siguiente:*

1. *Si $d \equiv 2 \pmod 4$ o $d \equiv 3 \pmod 4$, entonces $\overline{\mathbb{Z}[\sqrt{d}]} = \mathbb{Z}[\sqrt{d}]$.*
2. *Si $d \equiv 1 \pmod 4$, entonces*

$$\overline{\mathbb{Z}[\sqrt{d}]} = \left\{ \frac{c}{2} + \frac{e}{2}\sqrt{d} : c \equiv e \pmod 2 \right\}.$$

DEMOSTRACIÓN. Es evidente que $\mathbb{Z}[\sqrt{d}] \subseteq \overline{\mathbb{Z}[\sqrt{d}]}$. Supongamos que $d \equiv 1 \pmod 4$ y tomemos $x = \frac{c}{2} + \frac{e}{2}\sqrt{d}$ con $c \equiv e \pmod 2$. Claramente

$$\mathrm{Tr}(x) = c \in \mathbb{Z} \qquad \text{y} \qquad \mathrm{N}(x) = \frac{c^2}{4} - \frac{e^2}{4}d = \frac{c^2 - e^2 d}{4} \in \mathbb{Z},$$

pues de $d \equiv 1 \pmod 4$ se sigue que

$$\frac{c^2 - e^2 d}{4} \in \mathbb{Z} \iff \frac{c^2 - e^2}{4} \in \mathbb{Z},$$

lo cual es evidente ya que $c \equiv e \pmod 2$. Para terminar la demostración debemos ver que si $x = a + b\sqrt{d} \in \overline{\mathbb{Z}[\sqrt{d}]}$, entonces

$$a, b \in \mathbb{Z} \qquad \text{o} \qquad 2a, 2b \in \mathbb{Z} \setminus 2\mathbb{Z} \quad \text{y} \quad d \equiv 1 \pmod 4.$$

Por hipótesis, $2a = \mathrm{Tr}(x) \in \mathbb{Z}$ y $a^2 - db^2 = \mathrm{N}(x) \in \mathbb{Z}$. Claramente

$$2a \text{ es par } \Leftrightarrow a \in \mathbb{Z} \quad \text{y} \qquad 2a \text{ es impar } \Leftrightarrow a - \frac{1}{2} \in \mathbb{Z}.$$

Escribamos $b = m/n$ con m y n coprimos. Supongamos primero que a es un entero. En este caso

$$d\frac{m^2}{n^2} = a^2 - \mathrm{N}(x) \in \mathbb{Z},$$

lo cual implica que $b \in \mathbb{Z}$ pues d es libre de cuadrados (de $n^2 \mid dm^2$ se sigue que $n^2 \mid d$). Supongamos ahora que $a = k + \frac{1}{2}$ con $k \in \mathbb{Z}$. En este caso

$$d\frac{m^2}{n^2} - \frac{1}{4} = a^2 - \mathrm{N}(x) - \frac{1}{4} = k^2 + k + \frac{1}{4} - \mathrm{N}(x) - \frac{1}{4} = k^2 + k - \mathrm{N}(x) \in \mathbb{Z},$$

y así, $4n^2 \mid 4dm^2 - n^2$. Por lo tanto $4 \mid n^2$ y $n^2 \mid 4dm^2$, lo cual implica que $n = 2$ y m es impar (porque m y n son coprimos y d es libre de cuadrados). Escribamos $l := \frac{m-1}{2}$. Entonces $b = l + \frac{1}{2}$ y así

$$d(l^2 + l) + \frac{d-1}{4} = db^2 - \frac{1}{4} \in \mathbb{Z},$$

por lo que $d \equiv 1 \pmod 4$. □

Proposición 11.4. *Supongamos que $d \in \mathbb{Z}$ es un entero que es libre de cuadrados. Si d es congruente a 1 módulo 4, entonces*

$$\overline{\mathbb{Z}[\sqrt{d}]} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\frac{1+\sqrt{d}}{2} : a, b \in \mathbb{Z}\right\}.$$

Demostración. La segunda igualdad se sigue de que si $d - 1 = 4k$, entonces

$$\left(\frac{1+\sqrt{d}}{2}\right)^2 = \frac{1 + 2\sqrt{d} + d}{4} = \frac{d-1}{4} + \frac{1+\sqrt{d}}{2} = k + \frac{1+\sqrt{d}}{2}.$$

Veamos la primera igualdad. Tomemos $\frac{c}{2} + \frac{e}{2}\sqrt{d} \in \overline{\mathbb{Z}[\sqrt{d}]}$. Sabemos que $c \equiv e \pmod 2$ y que, por lo tanto, existe $k \in \mathbb{Z}$ tal que $c = e + 2k$. Así

$$\frac{c}{2} + \frac{e}{2}\sqrt{d} = k + e\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

Por lo tanto la inclusión $\subseteq$ vale. Dado que

$$a + b\frac{1+\sqrt{d}}{2} = \frac{2a+b}{2} + \frac{b}{2}\sqrt{d},$$

la otra inclusión es evidente. □

Corolario 11.5. *Para cada $d \in \mathbb{Z}$ libre de cuadrados, $\overline{\mathbb{Z}[\sqrt{d}]}$ es un subanillo de de $\mathbb{Q}[\sqrt{d}]$ que contiene a $\mathbb{Z}[\sqrt{d}]$.*

Demostración. Por las Proposiciones 11.3 y 11.4. □

Proposición 11.6. *Para cada entero d que es libre de cuadrados,*

$$\overline{\mathbb{Z}[\sqrt{d}]}^{\times} = \left\{x \in \overline{\mathbb{Z}[\sqrt{d}]} : \mathrm{N}(x) \in \mathbb{Z}^{\times}\right\}.$$

DEMOSTRACIÓN. Tomemos $x \in \overline{\mathbb{Z}[\sqrt{d}]}^{\times}$. Como $1 = \mathrm{N}(1) = \mathrm{N}(xx^{-1}) = \mathrm{N}(x)\,\mathrm{N}(x^{-1})$ y, tanto $\mathrm{N}(x)$ como $\mathrm{N}(x^{-1})$ son enteros, es evidente que

$$\overline{\mathbb{Z}[\sqrt{d}]}^{\times} \subseteq \left\{ x \in \overline{\mathbb{Z}[\sqrt{d}]} : \mathrm{N}(x) \in \mathbb{Z}^{\times} \right\}.$$

Tomemos ahora $x \in \overline{\mathbb{Z}[\sqrt{d}]}$ tal que $\mathrm{N}(x) \in \{\pm 1\}$. Como $x\,\overline{x} = \mathrm{N}(x)$ y $\overline{x} \in \overline{\mathbb{Z}[\sqrt{d}]}$ es claro que x es inversible y que $x^{-1} = \mathrm{N}(x)^{-1}\overline{x}$. □

COROLARIO 11.7. *Para cada entero d libre de cuadrado, vale lo siguiente:*

1. *Si $d \leq -2$ y $d \neq -3$, entonces $\overline{\mathbb{Z}[\sqrt{d}]}^{\times} = \{\pm 1\}$,*
2. $\overline{\mathbb{Z}[\sqrt{-3}]}^{\times} = \left\{1,\, -1,\, \frac{1}{2} + \frac{1}{2}\sqrt{-3},\, \frac{1}{2} - \frac{1}{2}\sqrt{-3},\, -\frac{1}{2} + \frac{1}{2}\sqrt{-3},\, -\frac{1}{2} - \frac{1}{2}\sqrt{-3}\right\}$.

DEMOSTRACIÓN. Dejada al lector. □

12. Dominios principales y euclideanos

Un anillo es un *dominio principal* si es un dominio conmutativo y todos sus ideales son principales. En el Ejemplo 3.2 mostramos que los anillos de enteros y de polinomios en una variable sobre un cuerpo son dominios principales.

El ejercicio que sigue muestra que la condición de que k sea un cuerpo es necesaria para que $k[X]$ sea un dominio principal. Por ejemplo, $\mathbb{Z}[X]$ no lo es.

EJERCICIO 12.1. *Pruebe que si $A[X]$ es un dominio principal, entonces A es un cuerpo.*

DEFINICIÓN 12.2. *Consideremos un dominio conmutativo A. Una función $\delta\colon A\setminus\{0\} \to \mathbb{N}_0$ es una* función euclidea *si satisface*

1. *Si $a, b \in A \setminus \{0\}$ y $a \mid b$, entonces $\delta(a) \leq \delta(b)$,*
2. *Para cada $a, b \in A$ con $b \neq 0$ existen $q, r \in D$ tales que*

$$a = bq + r \quad y \quad r = 0 \text{ o } \delta(r) < \delta(b)$$

Un dominio conmutativo que posee una función euclidea $\delta\colon A \setminus \{0\} \to \mathbb{N}_0$, se denomina dominio euclideano.

EJEMPLO 12.3. *Los teoremas sobre existencia de algoritmo de división en $\mathbb{Z}$ y en $k[X]$ (donde k es un cuerpo) muestran que estos dominios son euclideanos.*

Desde aquí y hasta el Teorema 12.8 inclusive, A es un dominio euclideano y $\delta\colon A\setminus\{0\} \to \mathbb{N}_0$ es una función euclidea.

OBSERVACIÓN 12.4. *No pedimos que haya unicidad en el algoritmo de división, pero si $a = bq$, entonces si la hay. En efecto, si $a = bq' + r$ con $q' \neq q$ o $r \neq 0$, entonces de $r = b(q - q')$ se sigue que $q \neq q'$, $r \neq 0$ y $\delta(r) \geq \delta(b)$, por lo que el item 2) no se satisface.*

OBSERVACIÓN 12.5. *De la condición 1) se sigue que si a y b son elementos no nulos de A que se dividen mutuamente, entonces $\delta(a) = \delta(b)$.*

A continuación probamos una recíproca parcial de la Observación 12.5.

PROPOSICIÓN 12.6. *Si $a \mid b$ son no nulos y $\delta(b) \leq \delta(a)$, entonces $b \mid a$.*

Demostración. Escribamos $a = bq + r$ con $r = 0$ o $\delta(r) < \delta(b)$. Debemos ver que $r = 0$. Supongamos que no. Como $a \mid b$ existe c tal que $b = ac$. Así $r = a - bq = a(1 - qc)$, lo que implica que $\delta(a) \leq \delta(r) < \delta(b)$. Pero por la hipótesis, de esto se sigue que $\delta(a) < \delta(a)$, lo cual es imposible. □

Proposición 12.7. *Para $a \in A \setminus \{0\}$ las siguientes condiciones son equivalentes:*

1. *a es una unidad de A.*
2. *$\delta(a) = \delta(1)$.*
3. *$\delta(a) \leq \delta(b)$ para todo $b \in A \setminus \{0\}$.*
4. *$\delta(a) \leq \delta(1)$.*

Demostración. 1) ⇒ 2) Por la Observación 12.5.

2) ⇒ 3) Como $1 \mid b$ se sigue del item 1) de la Definición 12.2, que $\delta(a) = \delta(1) \leq \delta(b)$.

3) ⇒ 4) Es trivial.

3) ⇒ 4) Como $1 \mid a$ se sigue de la hipótesis y de la Proposición 12.6, que $a \mid 1$. □

Teorema 12.8. *El dominio A es principal.*

Demostración. Consideremos un ideal no nulo I de A y tomemos $a \in I \setminus \{0\}$ tal que $\delta(a)$ es el mínimo posible. Afirmamos que $I = \langle a \rangle$. Tomemos $b \in I$ arbitrario. Como A es euclideano existen $q, r \in A$ tales que $b = aq + r$ con $r = 0$ o $\delta(r) < \delta(b)$. Pero como $r = aq - b \in I$ lo último es imposible y así $a \mid b$. Por lo tanto $I \subseteq \langle a \rangle$, como queremos. □

El recíproco de este teorema es falso, pero no es fácil encontrar un dominio principal que no sea euclideano. Un ejemplo es $\mathbb{Z}[\sqrt{-19}]$.

Proposición 12.9. *Denotemos con A a un dominio conmutativo y con K a su cuerpo de fracciones. Consideremos una función multiplicativa $\delta\colon K^\times \to \mathbb{Q}^\times$ tal que $\delta(A \setminus \{0\}) \subseteq \mathbb{N}$. La restricción de δ a $A \setminus \{0\}$ es una función euclidea si y sólo si para todo $x \in K \setminus A$ existe $q \in A$ tal que $\delta(x - q) < 1$.*

Demostración. Supongamos que para todo $x \in K \setminus A$ existe $q \in A$ tal que $\delta(x - q) < 1$ y tomemos $a, b \in A$ con $b \neq 0$ tal que $b \nmid a$. Por hipótesis existe $q \in A$ tal que $\delta(a/b - q) < 1$. Escribamos $a = bq + r$ donde $r = a - bq$. Como

$$\delta(r) = \delta(b(a/b - q)) = \delta(b)\delta(a/b - q) < \delta(b),$$

la restricción de δ a $A \setminus \{0\}$ es una función euclidea de A. Supongamos ahora que esto último se satisface y tomemos $x \in K \setminus A$. Escribamos $x = a/b$ con $a, b \in A$ y $b \neq 0$. Por hipótesis existen $q, r \in A$ tales que

$$a = bq + r \qquad \text{con } r = 0 \text{ o } \delta(r) < \delta(b).$$

Pero necesariamente $r \neq 0$ pues $x \notin A$. Por lo tanto, $\delta(x - q) = \delta(r/b) = \delta(r)/\delta(b) < 1$, como queremos. □

Ejemplo 12.10. *Consideremos un entero negativo d, que no es un cuadrado. Es evidente que el cuerpo de fracciones de $\mathbb{Z}[\sqrt{d}]$ es $\mathbb{Q}[\sqrt{d}]$. Tomemos como $\delta\colon \mathbb{Q}[\sqrt{d}]^\times \to \mathbb{Q}^\times$ a la norma definida en la Subsección 11. Así $\delta(x + y\sqrt{d}) = x^2 - dy^2$. Ya sabemos que δ es multiplicativa. Además para cada $x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ existen $a, b \in \mathbb{Z}$ tales que $|x - a| \leq \frac{1}{2}$ y $|y - b| \leq \frac{1}{2}$, de modo que*

$$\delta\big((x + y\sqrt{d}) - (a + b\sqrt{d})\big) = (x - a)^2 - d(y - b)^2 \leq \frac{1 - d}{4},$$

que es menor que 1 *si* $d = -1$ *o* $d = -2$. *Por lo tanto* $\mathbb{Z}[\sqrt{-1}]$ *y* $\mathbb{Z}[\sqrt{-2}]$ *son euclideanos. Por otro lado, para todo* $a, b \in \mathbb{Z}$,

$$\delta\left(\left(\frac{1}{2}+\frac{1}{2}\sqrt{d}\right)-\left(a+b\sqrt{d}\right)\right)=\left(\frac{1}{2}-a\right)^2-d\left(\frac{1}{2}-b\right)^2\geq\frac{1-d}{4},$$

que es mayor o igual a 1 *si* $d \leq -3$.

Ejemplo 12.11. *Consideremos un entero negativo* d *congruente a* 1 *módulo* 4 *y libre de cuadrados. Tomemos como* $\delta\colon \mathbb{Q}[\sqrt{d}]^\times \to \mathbb{Q}^\times$ *a la norma definida en la Subsección 11. Notemos que cada* $z \in \mathbb{Q}[\sqrt{d}]$ *se escribe de manera única en la forma*

$$z = x + y\frac{1+\sqrt{d}}{2} \qquad \text{con } x, y \in \mathbb{Q}.$$

Por definición si $z \neq 0$,

$$\begin{aligned}\delta(z) &= \left(x+y\frac{1+\sqrt{d}}{2}\right)\overline{\left(x+y\frac{1+\sqrt{d}}{2}\right)}\\ &= \left(x+y\frac{1+\sqrt{d}}{2}\right)\left(x+y\frac{1-\sqrt{d}}{2}\right)\\ &= x^2+y^2\frac{1-d}{4}+xy\\ &= \left(x+\frac{y}{2}\right)^2-\frac{d}{4}y^2.\end{aligned}$$

Dados $x, y \in \mathbb{Q}$ *existen* $a, b \in \mathbb{Z}$ *tales que*

$$|y-b| \leq \frac{1}{2} \qquad y \qquad \left|x-a+\frac{y-b}{2}\right| \leq \frac{1}{2},$$

de modo que

$$\delta\left(\left(x+y\frac{1+\sqrt{d}}{2}\right)-\left(a+b\frac{1+\sqrt{d}}{2}\right)\right)=\left(x-a+\frac{y-b}{2}\right)^2-\frac{d}{4}(y-b)^2\leq\frac{4-d}{16},$$

que es menor que 1 *si* d *es* -3, -7 *o* -11. *Por lo tanto* $\overline{\mathbb{Z}[\sqrt{-3}]}$, $\overline{\mathbb{Z}[\sqrt{-7}]}$ *y* $\overline{\mathbb{Z}[\sqrt{-11}]}$ *son euclideanos. Por otro lado, para todo* $a, b \in \mathbb{Z}$,

$$\delta\left(\left(\frac{1}{2}+\frac{1}{2}\frac{1+\sqrt{d}}{2}\right)-\left(a+b\frac{1+\sqrt{d}}{2}\right)\right)=\left(\frac{3-4a-2b}{4}\right)^2-\frac{d}{4}\left(\frac{1-2b}{2}\right)^2\geq\frac{1-d}{16},$$

que es mayor o igual a 1 *si* $d \leq -15$.

Ejemplo 12.12. *Consideremos un entero positivo* d *que no es un cuadrado. Es evidente que el cuerpo de fracciones de* $\mathbb{Z}[\sqrt{d}]$ *es es* $\mathbb{Q}[\sqrt{d}]$. *Tomemos como* $\delta\colon \mathbb{Q}[\sqrt{d}]^\times \to \mathbb{Q}^\times$ *al módulo de la norma* N, *definida en la Subsección 11. Así* $\delta(x+y\sqrt{d}) = |x^2 - dy^2|$. *Claramente* δ *es multiplicativa ya que* N *lo es. Además para cada* $x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ *existen* $a, b \in \mathbb{Z}$ *tales que* $|x-a| \leq \frac{1}{2}$ *y* $|y-b| \leq \frac{1}{2}$, *de modo que*

$$\delta\big((x+y\sqrt{d})-(a+b\sqrt{d})\big)=|(x-a)^2-d(y-b)^2|\leq\frac{d}{4},$$

que es menor que 1 *si* $m = 2$ *o* $m = 3$. *Por lo tanto* $\overline{\mathbb{Z}[\sqrt{2}]}$ *y* $\overline{\mathbb{Z}[\sqrt{3}]}$ *son euclideanos.*

13. Los cuaterniones

En esta subsección F es un cuerpo arbitrario de característica distinta de 2. Presentaremos aquí los anillos de cuaterniones. En particular definiremos los cuaterniones de Hamilton que fueron descubiertos por él en 1843.

Fijemos elementos $a, b \in F^\times$ que pueden coincidir o no y consideremos el F-espacio vectorial A de dimensión 4 con base $\{1, i, j, k\}$. Supongamos que A tiene un producto F-bilineal que lo convierte en un anillo asociativo con neutro 1, tal que

$$i^2 := a, \quad j^2 := b, \quad ij := k \quad \text{y} \quad ji := -k. \tag{47}$$

Entonces necesariamente

$$k^2 = -ab, \quad ik = -ki = a \cdot j \quad \text{y} \quad jk = -kj = -b \cdot i. \tag{48}$$

PROPOSICIÓN 13.1. *El F-espacio vectorial A provisto del producto definido sobre $\{1, i, j, k\}$ por la condición de que 1 sea su neutro más las condiciones (47) y (48), y extendido A por F-bilinealidad, es un anillo asociativo*

DEMOSTRACIÓN. Sólo debemos verificar que el producto es asociativo y distributivo. Debido a que el producto esá definido sobre $\{1, i, j, k\}$ y extendido a A por F-bilinealidad, sólo debemos comprobar que $(xy)z = x(yz)$ para todo $x, y, z \in \{1, i, j, k\}$. Dejamos al lector la realización de esta tarea directa y sencilla. □

Denotamos con $\left(\frac{a,b}{F}\right)$ y llamamos *anillo de cuaterniones (generalizado)* al F-espacio vectorial A dotado de la estructura de anillo obtenido en la proposición anterior. Cuando $F = \mathbb{R}$ y $a = b = -1$ obtenemos el anillo de *cuaterniones de Hamilton* $\mathbb{H}$.

En el resto de esta sección escribiremos A en lugar de $\left(\frac{a,b}{F}\right)$ e identificaremos a F con $F1$.

PROPOSICIÓN 13.2. *El anillo A no tiene ideales biláteros no triviales y su centro es F.*

DEMOSTRACIÓN. Para cada $x, y \in A$ denotamos con $[x, y]$ a $xy - yx$. Un cálculo directo muestra que si $x = c_1 \cdot 1 + c_i \cdot i + c_j \cdot j + c_k \cdot k$, entonces

$$[i, x] = 2ac_k \cdot j + 2c_j \cdot k, \quad [j, x] = -2bc_k \cdot i - 2c_i \cdot k \quad \text{y} \quad [k, x] = 2bc_j \cdot i - 2ac_i \cdot j.$$

En consecuencia el cento de A es F. Supongamos ahora que $x \neq 0$ y que $x \in I$, donde I es un ideal bilátero de A. Un cálculo directo muestra que

$$-4bc_j \cdot i = [j, [i, x]] \in I, \quad 4abc_k \cdot j = [k, [j, x]] \in I \quad \text{y} \quad -4ac_i \cdot k = [i, [k, x]] \in I.$$

Por lo tanto si $c_i \neq 0$, $c_j \neq 0$ o $c_k \neq 0$, entonces I contiene a un elemento inversible. Por otro lado es evidente que si $c_i = c_j = c_k = 0$, entonces $c_1 = x \neq 0$ es también un elemento inversible de I. □

Denotemos con A_+ a $F \cdot i \oplus F \cdot j \oplus F \cdot k$. Los elementos de A_+ se denominan *cuaterniones puros*. Cada elemento $x \in A$ se escribe de manera única como

$$x = x_1 + x_+ \qquad \text{con } x_1 \in F1 \text{ y } x_+ \in A_+.$$

Definimos el *conjugado* de este x por $\overline{x} := x_1 - x_+$. Es evidente que

$$\overline{x + y} = \overline{x} + \overline{y}, \quad \overline{\overline{x}} = x, \quad \overline{x} = x \Leftrightarrow x \in F \quad \text{y} \quad \overline{x} = -x \Leftrightarrow x \in A_+.$$

Además es fácil ver que

$$\overline{xy} = \overline{y}\,\overline{x} \quad \text{para todo } x, y \in A.$$

En efecto, por la F-bilinealidad es suficiente comprobar esto para $x, y \in \{1, i, j, k\}$, lo que dejamos como ejercicio para el lector.

Definimos la *norma* $\mathrm{N}(x)$ de $x \in A$ por $\mathrm{N}(x) := x\overline{x}$. Un cálculo directo muestra que si $x = x_1 + x_+$ con $x_1 = c_1 \cdot 1 \in F1$ y $x_+ = c_i \cdot i + c_j \cdot j + c_k \cdot k \in A_+$ entonces

$$\mathrm{N}(x) = (x_1 + x_+)(x_1 - x_+) = x_1^2 - x_+^2 = c_1^2 - ac_i^2 - bc_j^2 + abc_k^2 \in F.$$

Notemos que

$$\mathrm{N}(xy) = xy\overline{xy} = xy\overline{y}\,\overline{x} = x\,\mathrm{N}(y)\overline{x} = x\,\overline{x}\,\mathrm{N}(y) = \mathrm{N}(x)\,\mathrm{N}(y) \quad \text{para todo } x, y \in A.$$

Proposición 13.3. *Para cada $x \in A$ son equivalentes:*

1. *x es inversible.*
2. *$\mathrm{N}(x) \neq 0$.*

Demostración. 1) $\Rightarrow$ 2) Porque

$$\mathrm{N}(x)\,\mathrm{N}(x^{-1}) = \mathrm{N}(xx^{-1}) = \mathrm{N}(1) = 1.$$

2) $\Rightarrow$ 1) Porque si $\mathrm{N}(x) \neq 0$, entonces

$$x\frac{1}{\mathrm{N}(x)}\overline{x} = \frac{1}{\mathrm{N}(x)}x\overline{x} = \frac{1}{\mathrm{N}(x)}\,\mathrm{N}(x) = 1,$$

y, por lo tanto, x es inversible. □

Teorema 13.4. *Son equivalentes:*

1. *A es un anillo de división.*
2. *Si $x \in A \setminus \{0\}$, entonces $\mathrm{N}(x) \neq 0$.*
3. *Si $c_1, c_i, c_j \in F$ satisfacen $c_1^2 = ac_i^2 + bc_j^2$, entonces $c_1 = c_i = c_j = 0$.*

Demostración. 1) $\Leftrightarrow$ 2) Por la Proposición 13.3.

2) $\Rightarrow$ 3) Porque si $c_1^2 = ac_i^2 + bc_j^2$, entonces

$$\mathrm{N}(c_1 \cdot 1 + c_i \cdot i + c_j \cdot j) = c_1^2 - ac_i^2 - bc_j^2 = 0.$$

3) $\Rightarrow$ 2) Supongamos que $x = c_1 \cdot 1 + c_i \cdot i + c_j \cdot j + c_k \cdot k$ y que $\mathrm{N}(x) = 0$. Entonces

$$0 = c_1^2 - ac_i^2 - bc_j^2 + abc_k^2, \tag{49}$$

lo que implica que

$$c_1^2 - bc_k^2 = a\big(c_i^2 - bc_k^2\big).$$

Por lo tanto

$$a\big(c_i^2 - bc_k^2\big)^2 = \big(c_1^2 - bc_j^2\big)\big(c_i^2 - bc_k^2\big) = \big(c_1c_i + c_jc_kb\big)^2 - b\big(c_1c_k + c_ic_j\big)^2.$$

Así, por hipótesis, $c_i^2 - bc_k^2 = 0$, lo que, nuevamente por hipótesis, implica que $c_i = c_k = 0$. Pero entonces, debido a la igualdad (49) y, por tercera vez a la hipótesis, $c_1 = c_j = 0$. □

Corolario 13.5. *El anillo $\mathbb{H}$ es de división y no conmutativo.*

Observación 13.6. *El conjunto de los cuaterniones de Hamilton que tienen cordenadas racionales forman un subanillo de división de $\mathbb{H}$.*

Observación 13.7. *Cada elemento de* $\mathbb{H}$ *se puede escribir de manera única como* $z_1 + z_2 j$ *con* $z_1, z_2 \in \mathbb{C}$*, donde identificamos* $\mathbb{C}$ *con el subanillo de* $\mathbb{H}$ *generado por* i*. La aplicación*

$$\theta\colon \mathbb{H} \to \mathrm{M}_2(\mathbb{C}),$$

dada por

$$\theta(z_1 + z_2 j) := \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix},$$

es un monomorfismo de anillos. Por lo tanto $\mathbb{H}$ *es isomorfo a un subanillo de* $\mathrm{M}_2(\mathbb{C})$*. Notemos que* $\det(\theta(z)) = \mathrm{N}(z)$ *para todo* $z \in \mathbb{H}$*.*

Observación 13.8. *Debido a la Observación 14.12 del Capítulo 1 el subgrupo de* $\mathbb{H}^\times$*, generado por* $e^{i\pi/n}$ *y* j*, es isomorfo al grupo cuaterniónico generalizado* H_n*. En particular* H_2 *es isomorfo al subgrupo* $\{\pm 1, \pm i, \pm j, \pm k\}$*. Notemos también que* $S^3 := \{z \in \mathbb{H} : \mathrm{N}(z) = 1\}$ *es un subgrupo de* $\mathbb{H}^\times$ *que contiene a las copias de los* H_n *mencionadas arriba.*

Observación 13.9. *Dado que para cada cuaternión puro* $x := c_1 \cdot i + c_2 \cdot j + c_3 \cdot k \in \mathbb{H}$ *de norma* 1*,*

$$x^2 = -\mathrm{N}(x) = -1,$$

en $\mathbb{H}$ *hay infinitas copias de* $\mathbb{C}$*.*

14. El anillo de un monoide

Para cada anillo A y cada monoide S, el conjunto $A^{(S)}$, de las funciones $\varphi\colon S \to A$ que tienen soporte finito, es un anillo, llamado *el anillo del monoide* S *con coeficientes en* A, y denotado $A[S]$, vía la suma coordenada a coordenada

$$(\varphi + \psi)(s) := \varphi(s) + \psi(s),$$

y el producto de convolución

$$(\varphi\psi)(s) := \sum_{\substack{u,v \in S \\ uv = s}} \varphi(u)\psi(v).$$

En efecto, ya sabemos que $A^{(S)}$ es un grupo abeliano vía la suma. Es el producto directo restringido de $|S|$ copias del grupo aditivo subyacente de A. El producto $\varphi\psi$ está bien definido porque la familia $(\varphi(u)\psi(v))_{u,v \in S}$ tiene soporte finito. Las igualdades

$$\begin{aligned}
\big((\varphi\psi)\vartheta\big)(s) &= \sum_{\substack{u,v \in S \\ uv = s}} (\varphi\psi)(u)\vartheta(v) \\
&= \sum_{\substack{u,v \in S \\ uv = s}} \left(\sum_{\substack{p,q \in S \\ pq = u}} \varphi(p)\psi(q) \right) \vartheta(v) \\
&= \sum_{\substack{x,y,z \in S \\ xyz = s}} \varphi(x)\psi(y)\vartheta(z) \\
&= \sum_{\substack{u,v \in S \\ uv = s}} \varphi(u) \left(\sum_{\substack{p,q \in S \\ pq = v}} \psi(p)\vartheta(q) \right)
\end{aligned}$$

$$= \sum_{\substack{u,v\in S\\ uv=s}} \varphi(u)(\psi\vartheta)(v)$$
$$= \big(\varphi(\psi\vartheta)\big)(s)$$

muestran que el producto es asociativo; las igualdades

$$\big(\varphi(\psi+\vartheta)\big)(s) = \sum_{\substack{u,v\in S\\ uv=s}} \varphi(u)(\psi(v)+\vartheta(v)) = \sum_{\substack{u,v\in S\\ uv=s}} \varphi(u)\psi(v) + \sum_{\substack{u,v\in S\\ uv=s}} \varphi(u)\vartheta(v) = (\varphi\psi+\varphi\vartheta)(s)$$

que es distributivo a izquierda respecto de la suma; y las igualdades

$$\big((\varphi+\psi)\vartheta\big)(s) = \sum_{\substack{u,v\in S\\ uv=s}} (\varphi(u)+\psi(u))\vartheta(v) = \sum_{\substack{u,v\in S\\ uv=s}} \varphi(u)\vartheta(v) + \sum_{\substack{u,v\in S\\ uv=s}} \psi(u))\vartheta(v) = (\varphi\vartheta+\psi\vartheta)(s),$$

que lo es a derecha. Por último es obvio que la función $1\colon S\to A$, definida por

$$1(s) := \begin{cases} 1 & \text{si } s=1,\\ 0 & \text{en otro caso,}\end{cases}$$

es el neutro multiplicativo de $A[S]$.

Para cada $a\in A$ y $s\in S$ llamemos $as\colon S\to A$ a la función definida por

$$(as)(t) := \begin{cases} a & \text{si } t=s,\\ 0 & \text{en otro caso.}\end{cases}$$

Cada elemento de $A[S]$ se escribe de manera única como una suma

$$\sum_{s\in S} a_s s, \tag{50}$$

con soporte finito. Una expresión como (50) es lo que se conoce con el nombre de *suma formal de elementos de S con coeficientes en A*. En términos de estas, la suma y el producto en $A[S]$ están dados por

$$\sum_{s\in S} a_s s + \sum_{s\in S} b_s s = \sum_{s\in S} (a_s+b_s)s \qquad \text{y} \qquad \left(\sum_{s\in S} a_s s\right)\left(\sum_{s\in S} b_s s\right) = \sum_{s\in S}\left(\sum_{\substack{u,v\in S\\ uv=s}} a_u b_v\right)s,$$

respectivamente.

La función $\iota_A\colon A\to A[S]$, definida por $\iota_A(a) := a1_S$ es un morfismo inyectivo de anillos, y la función $\iota_S\colon S\to A[S]$, definida por $\iota_S(s) := 1_A s$, es un morfismo inyectivo de S en el monoide multiplicativo de $A[S]$. Identificaremos $a\in A$ con $a1_S$ y $s\in S$ con $1_A s$. Con estas identificaciones el anillo $A[S]$ tiene la siguiente propiedad universal:

- Si $f\colon A\to B$ es un morfismo de anillos y $\psi\colon S\to B$ es un morfismo de S en el monoide multiplicativo de B, tal que $f(a)\psi(s) = \psi(s)f(a)$ para cada $a\in A$ y $s\in S$, entonces existe un único morfismo de anillos $\theta_\psi^f\colon A[S]\to B$, tal que los triángulos

$$\begin{array}{ccc} A & \xrightarrow{f} & B\\ {\scriptstyle \iota_A}\downarrow & \nearrow_{\theta_\psi^f} & \\ A[S] & & \end{array} \qquad \text{y} \qquad \begin{array}{ccc} S & \xrightarrow{\psi} & B\\ {\scriptstyle \iota_S}\downarrow & \nearrow_{\theta_\psi^f} & \\ A[S] & & \end{array}$$

conmutan.

En efecto, por la conmutatividad de los triángulos de arriba, debe ser

$$\theta_\psi^f\left(\sum_{s\in S} a_s s\right) = \sum_{s\in S} f(a_s)\psi(s).$$

Es evidente que con esta definición, θ_ψ^f respeta la suma y preserva la unidad. Un cálculo sencillo, usando que $f(a)\psi(s) = \psi(s)f(a)$ para cada $a \in A$ y $s \in S$, muestra que también lo hace con el producto.

EJEMPLO 14.1. *La aplicación trivial $\psi\colon S \to A$, definida por $\psi(s) := 1$ para todo $s \in S$, induce un morfismo $\varepsilon\colon A[S] \to A$, que es llamado el* morfismo de aumentación *de $A[S]$. Es evidente que*

$$\varepsilon\Big(\sum_{s\in S} a_s s\Big) = \sum_{s\in S} a_s.$$

Al núcleo I_+, de ε, se lo denomina el ideal de aumentación *de $A[S]$. Es fácil ver que*

$$I_+ = \sum_{s\in S} A\big(s - 1_S\big).$$

En efecto, es evidente que $\sum_{s\in S} A(s - 1_S) \subseteq I_+$ y, como por otro lado,

$$\sum_{s\in S} a_s = 0 \Longrightarrow \sum_{s\in S} a_s s = \sum_{s\in S} a_s s - \Big(\sum_{s\in S} a_s\Big)1_S = \sum_{s\in S} a_s\big(s - 1_S\big),$$

también vale la inclusión inversa.

EJEMPLO 14.2. *Para cada grupo G la aplicación $\psi\colon G \to A[G]^{\mathrm{op}}$, definida por $\psi(g) := g^{-1}$, es un morfismo de G en el monoide multiplicativo de $A[G]^{\mathrm{op}}$. Por lo tanto induce el morfismo de anillos*

$$\begin{array}{c} A^{\mathrm{op}}[G] \xrightarrow{\ f\ } A[G]^{\mathrm{op}} \quad , \\ \sum_g \lambda_g g \longmapsto \sum_g \lambda_g g^{-1} \end{array}$$

que es biyectivo porque la aplicación antipodal de G, introducida en el Ejemplo 11.4 del Capítulo 1, lo es. En particular, si A es conmutativo, entonces $A[G]^{\mathrm{op}}$ es isomorfo a $A[G]$.

PROPOSICIÓN 14.3. *Para cada par de anillos A_1 y A_2 y cada monoides S, hay un isomorfismo de anillos*

$$\Theta\colon (A_1 \times A_2)[S] \to A_1[S] \times A_2[S],$$

que aplica $(a_1, a_2)s$ en $(a_1 s, a_2 s)$.

DEMOSTRACIÓN. Consideremos la inclusión canónica $\iota\colon A_1 \times A_2 \to A_1[S] \times A_2[S]$ y el morfismo de monoides $\psi\colon S \to (A_1[S] \times A_2[S])^\times$, dado por $\psi(s) := (s, s)$. Por la propiedad universal de $(A_1 \times A_2)[S]$ los morfismos ι y ψ se extienden a un morfismo

$$\Theta\colon (A_1 \times A_2)[S] \to A_1[S] \times A_2[S],$$

tal que $\Theta\big((a_1, a_2)s\big) = (a_1 s, a_2 s)$. Es evidente que Θ es inyectivo. Como, para todo $a_1 \in A_1$, $a_2 \in A_2$ y $s \in S$, los pares $(a_1 s, 0)$ y $(0, a_2 s)$ están en la imagen de Θ, también es sobreyectivo. □

PROPOSICIÓN 14.4. *Para cada anillo A y cada par de monoides S y T, hay un isomorfismo de anillos*

$$\Theta\colon A[S][T] \to A[S \times T],$$

que aplica $(as)t$ en $a(s,t)$.

DEMOSTRACIÓN. Por la propiedad universal de $A[S]$ hay un único morfismo

$$\Phi\colon A[S] \to A[S \times T],$$

tal que $\Phi(a) = a$ y $\Phi(s) = (s,1)$ para todo $a \in A$ y $s \in S$. Debido ahora a la propiedad universal de $A[S][T]$, la aplicación Φ es extiende al morfismo Θ buscado. Es fácil ver que Θ es biyectivo. □

PROPOSICIÓN 14.5. *Para cada morfismo de anillos $f\colon A \to B$ y cada morfismo de monoides $\psi\colon S \to T$, existe un único morfismo de anillos $f[\psi]\colon A[S] \to B[T]$, tal que los diagramas*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \iota_A} & & \downarrow{\scriptstyle \iota_B} \\ A[S] & \xrightarrow{f[\psi]} & B[T] \end{array} \qquad y \qquad \begin{array}{ccc} S & \xrightarrow{\psi} & T \\ \downarrow{\scriptstyle \iota_S} & & \downarrow{\scriptstyle \iota_T} \\ A[S] & \xrightarrow{f[\psi]} & B[T], \end{array}$$

donde

$$\iota_A\colon A \to A[S], \qquad \iota_B\colon B \to B[T], \qquad \iota_S\colon S \to A[S] \qquad e \qquad \iota_T\colon T \to B[T],$$

son las aplicaciones canónicas, conmutan. Además

$$f[\psi]\left(\sum_{s\in S} a_s s\right) = \sum_{s\in S} f(a_s)\psi(s).$$

DEMOSTRACIÓN. Se sigue inmediatamente de la propiedad universal de $A[S]$. □

OBSERVACIÓN 14.6. *Es evidente que* $\mathrm{Im}(f[\psi]) = f(A)[\psi(S)]$ *y que el núcleo de $f[\psi]$ es la suma directa de la familia $(F_t)_{t\in \mathrm{Im}(\psi)}$, de subgrupos aditivos de $A[S]$, definida por*

$$F_t := \left\{ \sum_{s\in\psi^{-1}(t)} a_s s : \sum_{s\in\psi^{-1}(t)} f(a_s) = 0 \right\}.$$

Notemos ahora que para cada $s_t \in \psi^{-1}(t)$,

$$F_t = \ker(f)s_t \oplus \bigoplus_{s\in\psi^{-1}(t)\setminus\{s_t\}} A(s - s_t). \tag{51}$$

En efecto es evidente que

$$\ker(f)s_t \subseteq F_t \qquad y \qquad A(s - s_t) \subseteq F_t \text{ para cada } s \in \psi^{-1}(t) \setminus \{s_t\}.$$

Reciprocamente, si

$$\sum_{s\in\psi^{-1}(t)} a_s s \in F_t,$$

entonces

$$\sum_{s\in\psi^{-1}(t)} a_s s = \Big(\sum_{s\in\psi^{-1}(t)} a_s\Big)s_t + \sum_{s\in\psi^{-1}(t)\setminus\{s_t\}} a_s(s - s_t)$$

está en el lado derecho de la igualdad (51).

Supongamos ahora que para $t \in \operatorname{Im}\psi$ existe $s_t \in \psi^{-1}(t)$ tal que $\psi^{-1}(t) = s_t \ker\psi$ (si S es un grupo esta condición se satisface para todo $t \in \operatorname{Im}\psi$ y todo $s_t \in \psi^{-1}(t)$). Entonces

$$\bigoplus_{s\in\psi^{-1}(t)\setminus\{s_t\}} A(s - s_t) = \bigoplus_{s\in\ker\psi\setminus\{e\}} As_t(s - 1_S).$$

Supongamos ahora que $U \subseteq \ker\psi$ es tal que $\ker\psi$ está generado como monoide por U y por inversos de elementos de U. Dado que para todo sucesión $(u_i)_{i=1,\dots,r}$, formada por elementos de U o inversos de elementos de U,

$$u_1 \cdots u_r - 1_S = \sum_{i=1}^{r} u_1 \cdots u_{i-1}(u_i - 1_S) \qquad y \qquad u^{-1} - 1_S = -u^{-1}(u - 1_S),$$

obtenemos que

$$s - 1_S \in \sum_{u\in U} \ker(\psi)(u - 1_S) \qquad \text{para todo } s \in \ker\psi \setminus \{1_S\},$$

y, así,

$$\bigoplus_{s\in\psi^{-1}(t)\setminus\{s_t\}} A(s - s_t) = \bigoplus_{s\in\ker\psi\setminus\{1_S\}} As_t(s - 1_S) = \sum_{u\in U} As_t \ker(\psi)(u - 1_S).$$

Por lo tanto si $\ker\psi$ está generado como monoide por U y por inversos de elementos de U y, para cada $t \in \operatorname{Im}\psi$, existe $s_t \in \psi^{-1}(t)$ tal que $\psi^{-1}(t) = s_t \ker\psi$, entonces

$$\begin{aligned}\ker\big(f[\psi]\big) &= \bigoplus_{t\in\operatorname{Im}\psi} \left[\ker(f)s_t \oplus \left(\sum_{u\in U} As_t \ker(\psi)(u - 1_S)\right)\right] \\ &= \bigoplus_{t\in\operatorname{Im}\psi} \ker(f)s_t \oplus \sum_{u\in U} A[S](u - 1_S).\end{aligned}$$

En particular si f es inyectivo, entonces

$$\ker\big(f[\psi]\big) = \sum_{u\in U} A[S](u - 1_S)$$

es el ideal a izquierda de $A[S]$ generado por los elementos $u - 1_S$ con $u \in U$. Todo esto se aplica en particular al ideal de aumentación. En este caso $f = \mathrm{id}_A$ y $\psi\colon S \to 1$ es el morfismo trivial, por lo que

$$I_+ = \sum_{u\in U} A[S](u - 1_S)$$

para cada conjunto U de elementos de S tal que S está generado por U y por inversas de elementos de U.

Observación 14.7. *La correspondencia introducida en la proposición anterior tiene las siguientes propiedades:*

1. $\mathrm{id}_A[\mathrm{id}_S] = \mathrm{id}_{A[S]}$.
2. *Para cada par de morfismos de anillos $f\colon A \to B$ y $g\colon B \to C$ y cada par de morfismos de monoides $\psi\colon S \to T$ y $\vartheta\colon T \to L$,*

$$g[\vartheta] \circ f[\psi] = (g \circ f)[\vartheta \circ \psi].$$

EJEMPLO 14.8. *Para cada número natural r, denotemos con $\mathbb{N}_0^r$ al monoide formado por todas las r-uplas de enteros mayores o iguales que cero, con la suma coordenada a coordenada. Introduciendo variables $X_1, \ldots, X_r$ e identificando cada r-upla $\mathbf{n} = (n_1, \ldots, n_r)$ con el monomio $\mathbf{X}^{\mathbf{n}} = X_1^{n_1} \cdots X_r^{n_r}$, podemos considerar a $\mathbb{N}_0^r$ como un monoide multiplicativo vía el producto*

$$\mathbf{X}^{\mathbf{m}}\mathbf{X}^{\mathbf{n}} = \mathbf{X}^{\mathbf{m}+\mathbf{n}}.$$

Se comprueba inmediatamente que el anillo de monoide $A[\mathbb{N}_0^r]$ y de polinomios $A[X_1, \ldots, X_r]$ coinciden.

PROPOSICIÓN 14.9. *Los anillos $A[X_1, \ldots, X_r]$ y $A[X_1, \ldots, X_l][X_{l+1}, \ldots, X_r]$ son isomorfos para cada $l < r$.*

DEMOSTRACIÓN. Es una consecuencia inmediata de la Proposición 14.4. □

OBSERVACIÓN 14.10 (Propiedad universal del anillo de polinomios). *Para cada r-upla de elementos $b_1, \ldots, b_r$ de un anillo B que conmutan entre sí, hay un único morfismo de monoides γ, de $\mathbb{N}_0^r$ en el monoide multiplicativo de B, tal que $\gamma(X_i) = b_i$ para cada índice i. En consecuencia, por la propiedad universal del anillo de monoide, si además tenemos fijado un morfismo de anillos $f\colon A \to B$, tal que $f(a)b_i = b_i f(a)$ para todo $a \in A$ y todo i, entonces hay un único morfismo de anillos $\theta_\gamma^f\colon A[X_1, \ldots, X_r] \to B$, tal que $\theta_\gamma^f(a) = f(a)$ para cada $a \in A$ y $\theta_\gamma^f(X_i) = b_i$ para cada i. Es fácil ver que θ_γ está dado por*

$$\theta_\gamma^f\left(\sum a_{n_1,\ldots,n_r} X_1^{n_1} \cdots X_r^{n_r}\right) = \sum f(a_{n_1,\ldots,n_r}) b_1^{n_1} \cdots b_r^{n_r}.$$

Terminamos esta subsección con el cálculo del centro de un anillo de grupos $A[G]$.

PROPOSICIÓN 14.11. *Para cada anillo de grupos $A[G]$,*

$$\mathrm{Z}(A[G]) = \left\{ \sum_h a_h h : a_h \in \mathrm{Z}\, A \text{ para todo } h \in G \text{ y } a_{ghg^{-1}} = a_h \text{ para todo } h, g \in G \right\}.$$

DEMOSTRACIÓN. Por definición $\mathrm{Z}_G(A[G])$ es el conjunto de los elementos de $A[G]$ que conmutan con todos los elementos de G. Es evidente que $\sum_h a_h h \in \mathrm{Z}_G(A[G])$ si y sólo si

$$\sum_h a_h ghg^{-1} = \sum_h a_h h \quad \text{para todo } g \in G.$$

Así,

$$\mathrm{Z}_G(A[G]) = \left\{ \sum_h a_h h : a_{ghg^{-1}} = a_h \text{ para todo } h, g \in G \right\}.$$

En consecuencia, como $\mathrm{Z}(A[G]) = \mathrm{Z}_G(A[G]) \cap \mathrm{Z}_A(A[G])$,

$$\mathrm{Z}(A[G]) = \left\{ \sum_h a_h h : a_h \in \mathrm{Z}\, A \text{ para todo } h \in G \text{ y } a_{ghg^{-1}} = a_h \text{ para todo } h, g \in G \right\}.$$

como queremos. □

Capítulo 6

Dominios de factorización única

El Teorema fundamental de la aritmética dice que todo número entero n se escribe de manera única como un producto

$$n = up_1^{l_1} \cdots p_m^{l_m},$$

donde los $p_1 < \cdots < p_m$ son números primos positivos, llamados los factores primos o irreducibles de n, el exponente $l_i > 0$ es la multiplicidad de p_i en la factorización y $u = \pm 1$. En este capítulo estudiaremos una clase de dominios conmutativos, llamados dominios de factorización única o factoriales, en los cuales vale una generalización directa de esta propiedad. Nuestro objetivo principal será probar que los anillos de polinomios sobre dominios factoriales son factoriales, el cual es un célebre teorema de Gauss. Las definiciones y propiedades básicas tienen sentido para monoides conmutativos y cancelativos, y las establecemos en ese contexto.

1. Monoides factoriales

Fijemos un monoide conmutativo S. Recordemos que un elemento s de S es una unidad si es inversible, y que el conjunto $S^\times$ de las unidades de S es un grupo. Dados elementos s y t de S, decimos que s *divide* a t o que es un *divisor* de t y que t *es divisible por* s, y escribimos $s \mid t$, si existe $c \in S$ tal que $sc = t$. Por ejemplo $1 \mid s$ para todo $s \in S$. La relación de divisibilidad es reflexiva y transitiva y, por lo tanto, define una estructura de preorden parcial en S. Decimos también que dos elementos s y t de S son *asociados*, y escribimos $s \sim t$, si

$$s \mid t \quad \text{y} \quad t \mid s.$$

Es evidente que $\sim$ es un relación de equivalencia y que el cociente $S/\sim$ es un conjunto parcialmente ordenado vía el orden inducido por la relación de divisibilidad en S.

Observación 1.1. *Para casa $s \in S$ vale lo siguiente:*

$$s \in S^\times \iff s \mid 1 \iff s \sim 1 \iff s \mid t \text{ para todo } t \in S.$$

Observación 1.2. *Si $s \sim t$ y $s \in S^\times$, entonces $t \in S^\times$.*

Observación 1.3. *Supongamos que S es cancelativo. En este caso si $s,t \in S$ y $s \mid t$, entonces el elemento $c \in S$ tal que $cs = t$ es único, y es llamado* el cociente de t por s. *A este elemento c se lo suele denotar con t/s o $\frac{t}{s}$. Afirmamos que s y t son asociados si y sólo existe una unidad u de S tal que $t = su$. En efecto, es claro que si u existe, entonces $s \mid t$ y $t \mid s$. Recíprocamente, si s y t son asociados, entonces hay elementos $u, v \in S$ tales que $t = su$ y $s = tv$. Por consiguiente*

$$tvu = su = t,$$

de lo cual se sigue que $vu = 1$, debido a que S es cancelativo.

Un *máximo divisor común* de dos elementos s y t de S es cualquier elemento $c \in S$ que satisface:

- $c \mid s$ y $c \mid t$,
- si $d \mid s$ y $d \mid t$, entonces $d \mid c$,

y un *mínimo múltiplo común* de s y t es cualquier elemento $e \in S$ que satisface:

- $s \mid e$ y $t \mid e$,
- si $s \mid f$ y $t \mid f$, entonces $e \mid f$.

En principio no hay ningún motivo por el cual dos elementos s y t de S deban tener un máximo divisor común, pero si tienen uno c, entonces por la misma definición es evidente que un elemento $d \in S$ es un máximo divisor común de s y t si y sólo si es asociado a c. Lo mismo es cierto para los mínimos múltiplos comunes de s y t. Por otro lado es evidente también que si d es un máximo divisor común de s y t, entonces también es un máximo divisor común de cualquier par de elementos s' y t' tales que $s' \sim s$ y $t' \sim t$.

Vamos a denotar con $\mathrm{mdc}(s,t)$ a cualquier máximo divisor común de s y t. Similarmente vamos a denotar con $\mathrm{mmc}(s,t)$ a cualquier mínimo múltiplo común de s y t. Si 1 es un máximo divisor común de s y t decimos que *s y t son coprimos*.

Observación 1.4. *Vale lo siguiente:*

$$s \mid t \iff s = \mathrm{mdc}(s,t) \iff t = \mathrm{mmc}(s,t).$$

Por ejemplo $1 = \mathrm{mdc}(1,t)$ y $t = \mathrm{mmc}(1,t)$ para todo $t \in S$.

Proposición 1.5. *En cada monoide cancelativo S vale lo siguiente:*

1. *Si d es un máximo divisor común de s y t, entonces s/d y t/d son coprimos.*
2. *Si d es un máximo divisor común de s y t y si cs y ct tienen máximo divisor común, entonces cd es un máximo divisor común de cs y ct.*
3. *Si s y t tienen un mínimo múltiplo común m, entonces tienen un máximo divisor común d. Además dm y st son asociados.*
4. *Si cada par de elementos de S tiene un máximo divisor común, entonces cada par de elementos de S tiene un mínimo múltiplo común.*

Demostración. 1) Denotemos con s' y t' a s/d y t/d respectivamente, y supongamos que c divide a s' y a t'. Entonces cd divide a s y a t y, por lo tanto, $cd \mid d$. Simplificando d obtenemos que $c \mid 1$.

2) Denotemos con e a un máximo divisor común de cs y ct. Como $cd \mid cs$ y $cd \mid ct$, sabemos que $cd \mid e$, de modo que existe $u \in S$ tal que $e = cdu$. Esto implica que cdu divide a cs y a ct,

de lo que se sigue que du divide a s y a t y, así, $du \mid d$. En consecuencia u es una unidad y, por lo tanto, cd y e son asociados.

3) Como $s \mid st$ y $t \mid st$ existe d tal que $st = dm$. Claramente $d \mid s$ y $d \mid t$. Supongamos que $c \mid s$ y $c \mid t$, de manera que existen s' y t' tales que $cs' = s$ y $ct' = t$. Como $s \mid cs't'$ y $t \mid cs't'$ sabemos que $m \mid cs't'$ y así existe z tal que $mz = cs't'$. Por lo tanto $dm = st = cs'ct' = mzc$, lo que implica que $d = zc$ y, en consecuencia, $c \mid d$.

4) Debemos ver que todo par de números s y t tiene un mínimo múltiplo común. Consideremos primero el caso en que s y t son coprimos. Afirmamos que st es un mínimo múltiplo común de s y t o, en otras palabras, que si $s \mid m$ y $t \mid m$, entonces $st \mid m$. Escribamos $m = sx = ty$. Como $\operatorname{mdc}(s, y) \mid s$ y $\operatorname{mdc}(t, x) \mid t$ podemos escribir también $s = \operatorname{mdc}(s, y)y'$ y $t = \operatorname{mdc}(t, x)x'$. Dado que

$$\begin{aligned} x' \operatorname{mdc}(t, x) \operatorname{mdc}(s, y) &= t \operatorname{mdc}(s, y) \\ &\sim \operatorname{mdc}(ts, ty) \\ &\sim \operatorname{mdc}(ts, m) \\ &\sim \operatorname{mdc}(ts, sx) \\ &\sim s \operatorname{mdc}(t, x) \\ &\sim y' \operatorname{mdc}(s, y) \operatorname{mdc}(t, x), \end{aligned}$$

sabemos que $x' \sim y'$. En consecuencia x' es una unidad (pues s y t son coprimos). Por lo tanto $t \mid \operatorname{mdc}(t, x)$, lo que implica que

$$st \mid s \operatorname{mdc}(t, x) \mid sx = m,$$

como queremos. Consideremos ahora el caso general. Denotemos con d a un máximo divisor común de s y t y escribamos $s = ds'$ y $t = dt'$. Por el item 1) los números s' y t' son coprimos. Tomemos m tal que $s \mid m$ y $t \mid m$ (lo que implica que $d \mid m$). Es evidente que $s' \mid m'$ y $t' \mid m'$, donde m' es tal que $m = dm'$. Por lo que ya hemos probado, $s't' \mid m'$ y, así, $ds't' \mid dm' = m$. Como $s \mid ds't'$ y $t \mid ds't'$, es claro que $ds't$ es un mínimo múltiplo común de s y t. □

Un elemento $p \in S \setminus S^\times$ es *irreducible* si todos sus divisores son unidades o asociados a él, y es *primo* si cada vez que divide a un producto, divide a uno de los factores. Dicho de otro modo, p es irreducible si

$$s \mid p \Rightarrow s \in S^\times \text{ o } s \sim p,$$

y es primo si

$$p \mid st \Rightarrow p \mid s \text{ o } p \mid t.$$

Notemos que si $p \sim q$ y p es irreducible o primo, entonces q también lo es.

Observación 1.6. *Si s es irreducible y $s \nmid t$, entonces s y t son coprimos.*

Observación 1.7. *Si S es cancelativo, entonces $p \in S \setminus S^\times$ es irreducible si y sólo si de $p = st$ se sigue que $s \in S^\times$ o $t \in S^\times$. En efecto, es evidente que de esta condición se sigue que p es irreducible (incluso cuando S no es cancelativo). Supongamos ahora que p es irreducible y que $p = st$. Si s es asociado a p, entonces t es una unidad debido a la Observación 1.3.*

Proposición 1.8. *Si S es cancelativo, entonces todo elemento primo $p \in S$ es irreducible.*

DEMOSTRACIÓN. Supongamos que $s \mid p$ y escribamos $p = st$. Como p es primo, $p \mid s$ o $p \mid t$. Es claro que el primer caso $p \sim s$. Supongamos entonces que $p \mid t$ y escribamos $t = vp$. Como S es cancelativo, la igualdad

$$p = st = svp,$$

implica que $sv = 1$ y así, s es una unidad de S. □

Un monoide conmutativo y cancelativo S es *semifactorial* si para todo $s \in S$ existen una unidad u e irreducibles $p_1, \ldots, p_m$ tales que

$$s = up_1 \cdots p_m \tag{52}$$

Una escritura de s como (52) es llamada una *factorización de* s como producto de irreducibles. Notemos que $m = 0$ si y sólo s es inversible, y que si $m > 0$, entonces se puede tomar $u = 1$. Decimos que S es *factorial* si es semifactorial y la escritura de cada $s \in S$ como producto de irreducibes es única en el siguiente sentido: Si

$$s = up_1 \cdots p_m = vq_1 \cdots q_n,$$

con $u, v \in S^\times$ y $p_1, \ldots, p_m, q_1, \ldots, q_n$ irreducibles, entonces $m = n$ y existe $\sigma \in \mathrm{S}_m$ tal que $p_i \sim q_{\sigma_i}$ para todo i.

Por la Proposición 1.8 sabemos que en un monoide cancelativo los elementos primos son irreducibles. El siguiente teorema muestra, en particular, que en los monoides factoriales vale la recíproca.

TEOREMA 1.9. *Para cada monoide conmutativo y cancelativo S son equivalentes:*

1. *S es factorial.*
2. *S es semifactorial y todo elemento irreducible $p \in S$ es primo.*
3. *Cada $s \in S$ se factoriza como un producto*

$$s = up_1 \cdots p_n,$$

donde u es una unidad y $p_1, \ldots, p_n$ son primos.

DEMOSTRACIÓN. 1) ⇒ 2) Es claro que S es semifactorial. Veamos que cada elemento irreducible $p \in S$ es primo. Supongamos que $p \mid st$ y $st = px$. Entonces combinando p con una factorización de x se obtiene una de st, y combinando una de s con una de t, se obtiene otra. Como la factorización de st es única salvo asociados, esto implica que $p \mid s$ o $p \mid t$

2) ⇒ 3) Es trivial.

3) ⇒ 1) Consideremos otra factorización

$$s = vq_1 \cdots q_m$$

de s en producto de una unidad v e irreducibles $q_1, \ldots, q_m$. Si $n = 0$, entonces s es inversible. Por lo tanto $m = 0$ y $v = u$. Supongamos ahora que $n > 0$ y que cada factorización es única salvo asociados siempre que $n \leq n_0$ y que $n = n_0 + 1$. Como p_n es primo, debe dividir a v o a unos de los q_i's. Pero es imposible que p_n divida a v, porque sería una unidad. Podemos asumir sin pérdida de generalidad que $p_n \mid q_i$. Puesto que q_m es irreducible y p_n no es una unidad, $q_m \sim p_n$. En consecuencia existe $w \in S^\times$ tal que

$$wq_1 \cdots q_{m-1} = p_1 \cdots p_{n-1}.$$

Ahora la demostración se termina inmediatamente usando la hipótesis inductiva. □

Consideremos un monoide conmutativo S. Una sucesión

$$s_1, s_2, s_3, \dots,$$

de elementos de S es *estacionaria* si existe $n_0 \in \mathbb{N}$ tal que $s_i \sim s_{n_0}$ para todo $i \geq n_0$. Una *cadena de divisores sucesivos* de S es una sucesión

$$s_1, s_2, s_3, \dots,$$

de elementos de S tal que $s_{i+1} \mid s_i$ para todo i. Es evidente que si S es factorial, entonces toda cadena de divisores sucesivos de S es estacionaria. Nuestro próximo objetivo es verificar que esta condición implica que S es semifactorial. Esto es, que es intermedia entre la de ser semifactorial y factorial. Para ello comenzamos estableciendo un lema.

Lema 1.10. *Si toda cadena de divisores sucesivos de S es estacionaria, entonces cada $s \in S$ que no es una unidad es divisible por un elemento irreducible de S.*

Demostración. Supongamos que la tesis es falsa para un s. Entonces se obtiene una sucesión no estacionaria

$$s_1, s_2, s_3, \dots,$$

de divisores sucesivos de S, tomando $s_1 = s$ y s_{i+1} como un divisor de s_i no inversible ni asociado a s_i. □

Proposición 1.11. *Supongamos que S es un monoide conmutativo y cancelativo. Si toda cadena de divisores sucesivos de S es estacionaria, entonces S es semifactorial.*

Demostración. Supongamos que $s_0 \in S \setminus S^\times$ no es producto de irreducibles. Afirmamos que existen $s_1, \dots, s_n, \dots, p_1, \dots, p_n, \dots \in S$, con los p_i's irreducibles, tales que $s_i = p_{i+1}s_{i+1}$ para todo $i \geq 0$. En efecto supongamos hemos obtenido $s_1, \dots, s_n, p_1, \dots, p_n \in S$ como queremos. Entonces $s_0 = p_1 p_2 \cdots p_n s_n$, por lo que, debido a la hipótesis, $s_n \notin S^\times$. En consecuencia, por el Lema 1.10, existen $p_{n+1}, s_{n+1} \in S$ con p_{n+1} irreducible, tales que $s_n = p_{n+1}s_{n+1}$. Se comprueba fácilmente ahora que la cadena de divisores sucesivos

$$s_1, s_2, s_3, s_4, \dots$$

no es estacionaria. □

Observación 1.12. *Supongamos que S es un monoide abeliano y que existe una función $\mu\colon S \to \mathbb{N}_0$ tal que $s \mid t$ implica $\mu(s) \leq \mu(t)$ y tal que $s \mid t$ y $t \nmid s$ implica $\mu(s) < \mu(t)$. Entonces toda cadena de divisores sucesivos de S es estacionaria y $\mu(s) = \min\{\mu(s) : s \in S\}$ si y sólo si s es una unidad de S.*

Una *familia de representantes de las clases de equivalencia de los irreducibles de S (módulo asociados)*, es cualquier subconjunto $\mathcal{P}$ de S, tal que para cada irreducible q de S hay un único $p \in \mathcal{P}$ asociado a q. Por ejemplo, los primos positivos son una familia de representantes de las clases de equivalencia de los irreducibles de $\mathbb{Z} \setminus \{0\}$ y los polinomios mónicos de grado 1 son una familia de representantes de las clases de equivalencia de los irreducibles de $\mathbb{C}[X] \setminus \{0\}$. Tales familias existen siempre, aunque es raro que se pueda elegir una en forma canónica, como en los ejemplos anteriores. De todos modos, en el resto de la sección consideramos fijada una, que además supondremos totalmente ordenada. Es evidente que S es factorial si cada elemento $s \in S$ se escribe de manera única como un producto

$$s = u p_1^{m_1} \cdots p_m^{m_n}, \tag{53}$$

con $u \in S^\times$, $p_1 < \cdots < p_n$ en $\mathcal{P}$ y $m_1, \ldots, m_n \in \mathbb{N}$. Los elementos $p_1, \ldots, p_n$ son los *factores irreducibles* de s, y para cada i entre 1 y m, el número m_i es la *multiplicidad* o el *exponente* de p_i en s. Decimos que $p \in \mathcal{P}$ tiene multiplicidad 0 en s si no es un factor irreducible de s. Adoptada esta convención, podemos reescribir (53) en la forma

$$s = u(s) \prod_{p \in \mathcal{P}} p^{m_p(s)},$$

donde $u(s)$ es una unidad y $m_p(s)$ es la multiplicidad de p en s.

En un monoide factorial S, cada par de elementos tiene máximo divisor común y mínimo múltiplo común. En efecto, para cada $s, t \in S$, los elementos

$$(s : t) := \prod_{p \in \mathcal{P}} p^{\text{mín}(m_p(s), m_p(t))} \qquad \text{y} \qquad [s : t] := \prod_{p \in \mathcal{P}} p^{\text{máx}(m_p(s), m_p(t))},$$

donde $\text{mín}(m_p(s), m_p(t))$ denota al mínimo de $m_p(s)$ y $m_p(t)$ y $\text{máx}(m_p(s), m_p(t))$ al máximo, son un máximo divisor común y mínimo múltiplo común de s y t, respectivamente. Este resultado es una generalización directa del método para encontrar el máximo divisor común y el mínimo múltiplo común de dos números factorizados en primos, enseñado en la escuela primaria. Notemos que

$$st \sim (s : t)[s : t],$$

lo cual se sigue también del item 3) de la Proposición 1.5.

Observación 1.13. *En cada monoide factorial vale lo siguiente:*

1. *Si $s \mid tu$ y s es coprimo con u, entonces $s \mid t$.*
2. *Si $s \mid u$, $t \mid u$ y s y t son coprimos, entonces $st \mid u$.*

2. Dominios de factorización única

Consideremos el monoide multiplicativo de un anillo conmutativo A. Es evidente que $a \mid 0$ para todo $a \in A$ y que $0 \mid a$ implica que $a = 0$. En particular 0 es irreducible si y sólo si A es un cuerpo. Además vale lo siguiente:

1. si $a \mid b$ y $a \mid c$ entonces $a \mid rb + sc$ para todo $r, s \in A$,
2. si $a = bq + c$ entonces los divisores comunes de a y b coinciden con los de b y c,
3. Un elemento $p \in A$ es primo si y sólo si el ideal $\langle p \rangle$ lo es (ver la Observación 8.1),
4. 0 es primo si y sólo si A es un dominio (ver la Proposición 8.2 del Capítulo 5).
5. Si $0 = \text{mdc}(a, b)$, entonces $a = b = 0$.
6. Si $d \mid a$, $d \mid b$ y existen $r, s \in A$ tales que $d = ra + sb$, entonces $d = \text{mdc}(a, b)$.

A una expresión $d = ra + sb$ como en el item 5) se la denomina identidad de Bezout.

Proposición 2.1. *Consideremos elementos a, b y c en un anillo comutativo A.*

1. *Si $a \mid c$, $b \mid c$ y existe una identidad de Bezout $1 = ra + sb$, entonces $ab \mid c$.*
2. *Si $a \mid bc$ y existe una identidad de Bezout $1 = ra + sb$, entonces $a \mid c$.*

DEMOSTRACIÓN. 1) Escribamos $m = ac = bd$. Entonces

$$m = ram + sbm = rabd + sbac = ab(rd + sc),$$

y así $ab \mid m$.

2) Si $d \in A$ satisface $ad = bc$, entonces

$$c = rac + sbc = rac + sad = a(rc + sd),$$

y así $a \mid c$. □

PROPOSICIÓN 2.2. *Supongamos que A es un dominio conmutativo y tomemos $a, b \in A$ con $a \neq 0$ o $b \neq 0$. Si d es un máximo divisor común de a y b y existe una identidad de Bezout $d = ra + sb$, entonces ab/d es un mínimo múltiplo común de a y b.*

DEMOSTRACIÓN. Escribamos $a = da'$ y $b = db'$. Es claro que $ab/d = ab' = a'b$ y así, a y b dividen a ab/d. Supongamos ahora que $a \mid m$ y $b \mid m$. Debemos ver que ab' divide a m. Notemos que $d \mid m$ pues $d \mid a$ y $a \mid m$, y escribamos, $m = dm'$. Como $a \mid m$ y $b \mid m$ sabemos que $a' \mid m'$ y $b' \mid m'$. Además de

$$d = ra + sb = ra'd + sb'd = (ra' + sb')d,$$

se sigue que $1 = ra' + sb'$. Por lo tanto, debido a la Proposición 2.1(1), el producto $a'b'$ divide a m' y, en consecuencia, $ab' \mid m$, como queremos. □

OBSERVACIÓN 2.3. *Consideremos un anillo conmutativo arbitrario A y tomemos $a, b \in A$. Supongamos que el ideal $\langle a, b\rangle$ es principal y escribamos $\langle d\rangle = \langle a, b\rangle$. Entonces*

$$d \mid a, \quad d \mid b \qquad y \qquad d = ra + sb \quad \text{con } r, s \in A.$$

Por lo tanto, debido al item 6 del comienzo de esta subsección, $d = \gcd(a, b)$. Similarmente si $\langle a\rangle \cap \langle b\rangle$ es principal y $\langle m\rangle = \langle a\rangle \cap \langle b\rangle$, entonces $m = \operatorname{mmc}(a, b)$.

Es evidente que un anillo conmutativo A es un dominio si y sólo si $A\backslash\{0\}$ es un submoniode del monoide multiplicativo de A y que en este caso un elemento p no nulo de A es irreducible o primo en $A \setminus \{0\}$ si y sólo si lo es en A.

Un dominio conmutativo A es *semifactorial* si $A \setminus \{0\}$ es un monoide semifactorial, y es *factorial* o de *factorización única*, si $A \setminus \{0\}$ es un monoide factorial. Ya sabemos que si este es el caso, entonces cada par de elementos no nulos $a, b \in A$ tiene máximo divisor común y mínimo múltiplo común. En realidad, estos operadores están definidos para todo a y b. Por ejemplo, cuando $b = 0$ el primero da a y el segundo 0.

PROPOSICIÓN 2.4. *Para cada elemento $p \neq 0$ de un dominio principal A son equivalentes:*

1. *$\langle p\rangle$ es maximal,*
2. *p es primo,*
3. *p es irreducible.*

DEMOSTRACIÓN. 1) $\Rightarrow$ 2). Por el Corolario 8.3 del Capítulo 5.

2) $\Rightarrow$ 3). Por la Proposición 1.8.

3) $\Rightarrow$ 1). Si $\langle p\rangle$ no fuera maximal, entonces existiría $q \in A$ tal que $\langle p\rangle \subsetneq \langle q\rangle \subsetneq A$, lo que claramente implica que $q \mid p$ pero q no es unidad ni asociado a p. □

TEOREMA 2.5. *Todo dominio principal es factorial.*

Demostración. Por el Teorema 1.9 y las Proposiciones 1.11 y 2.4 y será suficiente probar que toda cadena

$$s_1, s_2, s_3, \dots,$$

de divisores sucesivos de $A \setminus \{0\}$ es estacionaria. Veamos que esto es así. Dado que

$$\langle s_1 \rangle \subseteq \langle s_2 \rangle \subseteq \langle s_3 \rangle \subseteq \cdots$$

la unión $\bigcup_{i \in \mathbb{N}} \langle s_i \rangle$ es un ideal. Como A es un dominio principal existe $s \in A \setminus \{0\}$ tal que

$$\bigcup_{i \in \mathbb{N}} \langle s_i \rangle = \langle s \rangle.$$

Por lo tanto si $s \in \langle s_n \rangle$,

$$\langle s \rangle = \langle s_n \rangle = \langle s_{n+1} \rangle = \langle s_{n+2} \rangle = \cdots$$

y, en consecuencia, $s_n \mid s_{n+i}$ para todo $i \in \mathbb{N}$. □

Observación 2.6. *Supongamos que $d \in \mathbb{Z}$ no es un cuadrado y consideremos el dominio $A := \mathbb{Z}[\sqrt{d}]$ o $A := \overline{\mathbb{Z}[\sqrt{d}]}$. Vimos en las Proposiciones 11.1 y 11.6 que $z \in A$ es inversible si y sólo $\mathrm{N}(z) = \pm 1$. Notemos ahora que si $z = xy$ con x e y no inversibles, entonces de $\mathrm{N}(z) = \mathrm{N}(x)\,\mathrm{N}(y)$ se sigue que $\mathrm{N}(z)$ no es primo en $\mathbb{Z}$. Por lo tanto, si $\mathrm{N}(z)$ es primo en $\mathbb{Z}$, entonces z es irreducible en A. No vale la recíproca, ya que por lo que acabamos de ver si $\mathrm{N}(z)$ no es unidad y no hay ningún $x \in A$ tal que $\mathrm{N}(x) \mid \mathrm{N}(z)$ y $\mathrm{N}(x) \notin \{\pm 1, \pm \mathrm{N}(z)\}$, entonces z es irreducible en A. Por ejemplo 3 es irreducible en $\mathbb{Z}[\sqrt{-1}]$ a pesar de que $\mathrm{N}(3) = 9$, pues la igualdad*

$$a^2 + b^2 = \mathrm{N}(a + b\sqrt{-1}]) = 3$$

es imposible. Similarmente 2, 3, $1+\sqrt{-5}$ y $1-\sqrt{-5}$ son irreducibles en $\mathbb{Z}[\sqrt{-5}]$, pues $\mathrm{N}(2) = 4$, $\mathrm{N}(3) = 9$, $\mathrm{N}(1+\sqrt{-5}) = \mathrm{N}(1-\sqrt{-5}) = 6$ y la condición

$$a^2 + 5b^2 = \mathrm{N}(a + b\sqrt{-5}]) \in \{\pm 2, \pm 3\}$$

no se satisface nunca. Notemos además que ninguno de estos elementos divide a ninguno de los otros (por ejemplo $1+\sqrt{-5} \nmid 2$ ya que $\mathrm{N}(1+\sqrt{-5}) \nmid \mathrm{N}(2)$ en $\mathbb{Z}$ y $1+\sqrt{-5} \nmid 1-\sqrt{-5}$ pues ambos tienen la misma norma pero no son asociados). La igualdad

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

muestra ahora que ninguno de los elementos 2, 3, $1+\sqrt{-5}$ y $1-\sqrt{-5}$ es primo. En consecuencia $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única. Afirmamos que 2 y $1+\sqrt{-5}$ son coprimos. En efecto, si d es un divisor común de 2 y $1+\sqrt{-5}$, entonces

$$\mathrm{N}(d) \mid \mathrm{mdc}\left(\mathrm{N}(2), \mathrm{N}(1+\sqrt{-5})\right) = \mathrm{mdc}(4, 6) = 2.$$

Como vimos arriba, de esto se sigue que $\mathrm{N}(d) \in \{\pm 1\}$ y, por lo tanto, x es inversible. Veamos ahora que 2 y $1+\sqrt{-5}$ no tienen un mínimo múltiplo común. Supongamos que

$$m = \mathrm{mmc}\left(2, 1+\sqrt{-5}\right).$$

Entonces $4 = \mathrm{N}(2) \mid \mathrm{N}(m)$ y $6 = \mathrm{N}(1+\sqrt{-5}) \mid \mathrm{N}(m)$ por lo que $12 \mid \mathrm{N}(m)$. Por otra parte, como 6 y $2(1+\sqrt{-5})$ son múltiplos comunes de 2 y $1+\sqrt{-5}$, el número m los divide. Por lo tanto

$$\mathrm{N}(m) \mid \mathrm{mdc}\left(\mathrm{N}(6), \mathrm{N}(2+2\sqrt{-5})\right) = \mathrm{mdc}\,(36, 24) = 12.$$

Así $\mathrm{N}(m) = 12$. Pero esto es imposible, pues la ecuación

$$a^2 + 5b^2 = \mathrm{N}(a + b\sqrt{-5}) = 12$$

no tiene solución. Notemos finalmente que, debido a la Proposición 2.2, no hay ninguna igualdad de Bezout, para 2 *y* $1+\sqrt{-5}$.

OBSERVACIÓN 2.7. *Supongamos que* $d \in \mathbb{Z}$ *no es un cuadrado. Tanto en* $\mathbb{Z}[\sqrt{d}]$ *como en* $\overline{\mathbb{Z}[\sqrt{d}]}$*, un elemento* x *es irreducible o primo, si y sólo si su conjugado lo es.*

2.1. Factorización única en $\mathbb{Z}[i]$

Por el Teorema 12.8 del Capítulo 5, el Teorema 2.5 y el Ejemplo 12.10 del Capítulo 5, sabemos que $\mathbb{Z}[i]$ es un dominio de factorización única. En esta subsección vamos a estudiar en detalle lo primos de $\mathbb{Z}[i]$ y a caracterizar los enteros que son suma de dos cuadrados.

PROPOSICIÓN 2.8. *Si el grupo de unidades de un dominio conmutativo* A *es finito, entonces el producto de sus unidades es* -1.

DEMOSTRACIÓN. En $A^\times$ agrupamos cada elemento u con su inverso u^{-1}. Es evidente que $\{1, 1^{-1}\} = \{1\}$ y $\{-1, -1^{-1}\} = \{-1\}$. Además como A es un dominio

$$u^2 = 1 \Longleftrightarrow (u-1)(u+1) = 0 \Longleftrightarrow u = \pm 1,$$

y, por lo tanto para cada $u \in A^\times \setminus \{1, -1\}$, el conjunto $\{u, u^{-1}\}$ tiene dos elementos. Por lo tanto, al multiplicar los elementos de $A^\times$ cada $u \in A^\times \setminus \{1, -1\}$ se cancela con u^{-1} (lo que no ocurre con $u = \pm 1$) y, así, el producto de las unidades de A da -1. □

COROLARIO 2.9 (Wilson). *Para cada entero primo positivo* p*, el producto de los elemento no nulos de* $\mathbb{Z}/p\mathbb{Z}$ *da* -1.

TEOREMA 2.10 (Fermat-Gauss). *Para cada primo positivo* p *de* $\mathbb{Z}$ *son equivalentes:*

1. p *es suma de dos cuadrados en* $\mathbb{Z}$.
2. $p = 2$ *o* $p \equiv 1 \pmod 4$,
3. -1 *es un cuadrado en* $\mathbb{Z}/p\mathbb{Z}$,
4. p *no es primo en* $\mathbb{Z}[i]$.

DEMOSTRACIÓN. 1) ⇒ 2) Como $0^2 = 2^2 = 0 \pmod 4$ y $1^2 = 3^2 = 1 \pmod 4$ una suma de dos cuadrados no puede ser congruente a 3 módulo 4. Dado que si p es impar, entonces es congruente a 1 o 3 modúlo 4, necesariamente el item 2) vale.
2) ⇒ 3) Si $p = 2$, entonces $-1 = 1 = 1^2$ en $\mathbb{Z}/p\mathbb{Z}$. Supongamos ahora que $p \equiv 1 \pmod 4$ y escribamos $p = 4t + 1$. Por el Corolario 2.9, en $\mathbb{Z}/p\mathbb{Z}$,

$$\begin{aligned}
-1 &= (p-1)! \\
&= (4t)! \\
&= 1 \cdot 2 \cdots (2t-1) \cdot (2t) \cdot (2t+1) \cdot (2t+2) \cdots (4t-1) \cdot (4t) \\
&= 1 \cdot 2 \cdots (2t-1) \cdot (2t) \cdot (-(2t))(-(2t-1)) \cdots - 2 \cdot -1 \\
&= (-1)^{2t}((2t)!)^2 \\
&= ((2t)!)^2,
\end{aligned}$$

3) ⇒ 4) Si $a^2 \equiv -1 \pmod 4$, entonces $p \mid a^2 + 1 = (a+i)(a-i)$. Como es evidente que p no divide ni a $a+i$ ni a $a-i$ en $\mathbb{Z}[i]$, resulta que p no es primo en $\mathbb{Z}[i]$.

4) $\Rightarrow$ 1) Como $\mathbb{Z}[i]$ es un dominio de factorización única, p no es irreducible. En consecuencia existen $x, y \in \mathbb{Z}[i]$ no unidades, tales que $p = xy$. Así,

$$p^2 = \mathrm{N}(p) = \mathrm{N}(x)\,\mathrm{N}(y).$$

Además dado que x e y no son unidades en $\mathbb{Z}[i]$, necesariamente $\mathrm{N}(x) = \mathrm{N}(y) = p$. Por lo tanto si $x = a + bi$, entonces $p = \mathrm{N}(x) = a^2 + b^2$. □

Observación 2.11. *Tomemos un primo positivo $p \in \mathbb{Z}$ que no es congruente a 3 módulo 4. Por la proposición anterior existen $a, b \in \mathbb{Z}$ tales que $p = a^2 + b^2$. Vale lo siguiente:*

1. *Salvo el orden y el signo de a y b esta expresión es única. En efecto si $p = c^2 + d^2$, entonces*
$$p = (a + bi)(a - bi) = (c + di)(c - di)$$
y como $\mathrm{N}(a + bi) = \mathrm{N}(a - bi) = \mathrm{N}(c + di) = \mathrm{N}(c + di) = p$, estos factores son todos irreducibles. En consecuecia, debido a la unicidad de la factorización de p como producto de primos de $\mathbb{Z}[i]$, necesariamente $c + di$ es asociado a $a + bi$ o a $a - bi$ y, por lo tanto, es uno de
$$a + bi, \quad -a - bi, \quad -b + ai, \quad b - ai, \quad a - bi, \quad -a + bi, \quad b + ai, \quad -b - ai,$$
de donde se sigue lo enunciado.
2. *Como p es primo, $a \neq 0 \neq b$ y $\mathrm{mdc}(a, b) = 1$. En efecto, la primera afirmación es obvia y la segunda se sigue de que si $d = \mathrm{mdc}(a, b)$ y escribimos $a = d\alpha$ y $b = d\beta$, entonces $p = d(\alpha^2 + \beta^2)$, lo cual implica que $d = 1$ ya que $\alpha^2 + \beta^2 > 1$.*
3. *Si $p \equiv 1 \pmod 4$ y $p = a^2 + b^2$ entonces a y b tienen distinta paridad (pues de lo contrario $2 \mid p$).*

Teorema 2.12. *Un entero de Gauss z es irreducible si y sólo si es de una de las siguientes formas*

1. *$z \in \{\pm p, \pm pi\}$ con p un entero positivo primo tal que $p \equiv 3 \pmod 4$.*
2. *$z = a + bi$ con $a^2 + b^2$ primo en $\mathbb{Z}$. En este caso $a^2 + b^2 = 2$ o $a^2 + b^2 \equiv 1 \pmod 4$.*

Demostración. Los elementos de tipo 1) son irreducibles por el Teorema 2.10 y los de tipo 2) lo son porque tienen como norma un número primo. Nuevamente por el Teorema 2.10, en este caso, $a^2 + b^2 = 2$ o $a^2 + b^2 \equiv 1 \pmod 4$. Veamos que estos son todos los irreducibles de $\mathbb{Z}[i]$. Tomemos un irreducible $z = a + bi \in \mathbb{Z}[i]$. Si $a = 0$ o $b = 0$, entonces z es asociado a un entero positivo que obviamente debe ser irreducible en $\mathbb{Z}[i]$ y que así, por el Teorema 2.10, debe ser del tipo 1). En otro caso $z\,\overline{z} = a^2 + b^2$ es una factorización de $a^2 + b^2$ en $\mathbb{Z}[i]$ como producto de irreducibles. Veamos que z es del tipo 2). Es decir que $a^2 + b^2$ es un primo de $\mathbb{Z}$. Factorizemos $a^2 + b^2$ en $\mathbb{Z}$ como un producto, $a^2 + b^2 = p_1 \cdots p_r$, de primos positivos. Dado que $z \in \mathbb{Z}[i]$ es primo, $z \mid p_i$ para algún i. Escribamos $p_i = zx$. Entonces $p_i^2 = \mathrm{N}(p_i) = \mathrm{N}(z)\,\mathrm{N}(x) = (a^2 + b^2)\,\mathrm{N}(x)$. Pero $a^2 + b^2 > 1$ y x no puede ser una unidad, pues $z \notin \mathbb{Z} \cup \mathbb{Z}i$ y $p_i \in \mathbb{Z}$. Por lo tanto $\mathrm{N}(x) = p_i = a^2 + b^2$ y, así, $a^2 + b^2$ es un primo de $\mathbb{Z}$. □

2.1.1. Números positivos que son sumas de dos cuadrados

Teorema 2.13 (Fermat). *Un entero positivo es suma de dos cuadrados si y sólo si los primos congruentes a 3 módulo 4, que aparecen en su factorización (como producto de primos positivos de $\mathbb{Z}$), lo hacen a una potencia par.*

DEMOSTRACIÓN. Consideremos la factorización de n como producto de primos positivos de $\mathbb{Z}$. Si los primos congruentes a 3 módulo 4, que aparecen en esta factorización, lo hacen a una potencia par, podemos agruparlos y obtenemos que $n = m^2 p_1 \cdots p_r$, con los p_j primos de $\mathbb{Z}$ que no son congruentes a 3 módulo 4. Por el Teorema 2.10 cada uno de estos p_j se escribe en la forma $p_j = a_j^2 + b_j^2 = \mathrm{N}(z_j)$, donde $z_j := a_j + b_j i$ y, así,

$$n = \mathrm{N}(m)N(z_1)\cdots\mathrm{N}(z_r) = \mathrm{N}(mz_1\cdots z_r),$$

que claramente es una suma de dos cuadrados. Supongamos ahora que $n = a^2 + b^2 = \mathrm{N}(z)$ y factorizemos $z := a + bi$ en $\mathbb{Z}[i]$, como un producto de irreducibles $z = p_1 \cdots p_r z_1 \cdots z_s$, donde los p_i son de tipo 1) y los z_i son de tipo 2). Entonces

$$n = \mathrm{N}(z) = p_1^2 \cdots p_r^2\, \mathrm{N}(z_1)\cdots\mathrm{N}(z_s),$$

lo que termina la demostración, ya que los p_i están en $\mathbb{Z}$ y los $\mathrm{N}(z_j)$ son primos de $\mathbb{Z}$, que no son congruentes a 3 módulo 4. □

2.1.2. Ternas pitagóricas

Una terna (a, b, c) de enteros positivos tales que $a^2 + b^2 = c^2$ se llama *terna pitagórica*. Los enteros a y b son los catetos de la terna y c es su hipotenusa. La terna es *primitiva* si sus catetos son coprimos y b es par. Por ejemplo $(3, 4, 5)$ y $(5, 12, 13)$ son ternas pitagóricas primitivas.

OBSERVACIÓN 2.14. *Al menos uno de los catetos de cada terna pitagórica es par. En efecto si a y b son impares y $c^2 = a^2 + b^2$, entonces $c^2 \equiv 2 \pmod 4$, lo que es imposible.*

PROPOSICIÓN 2.15. *Toda terna pitagórica se obtiene a partir de una primitiva multiplicando cada componente de esta por el mismo entero positivo y, si es necesario, cambiando el orden de sus catetos.*

DEMOSTRACIÓN. Supongamos que (a, b, c) es una terna pitagórica y denotemos con d al máximo divisor común de a y b. Como $c^2 = a^2 + b^2$, necesariamenta $d \mid c$. Claramente $(a/d, b/d, c/d)$ es una terna pitagórica con catetos coprimos y, por la observación anterior, uno (y sólo uno) de ellos es par. Cambiando el orden de los catetos si es necesario, obtenemos la terna primitiva del enunciado. □

TEOREMA 2.16. *Si $r > s > 0$ son enteros coprimos de distinta paridad, entonces*

$$(r^2 - s^2, 2rs, r^2 + s^2)$$

es una terna pitagórica primitiva. Además toda terna pitagórica primitiva es de esta forma.

DEMOSTRACIÓN. Es evidente que una terna de la forma $(r^2 - s^2, 2rs, r^2 + s^2)$ con $r > s > 0$ es pitagórica, que el segundo de sus catetos es par y que el primero es impar si y sólo si r y s no tienen la misma paridad. Supongamos ahora que estamos en este caso y que un primo p divide a $r^2 - s^2$ y a $2rs$. Entonces p es impar (pues $r^2 - s^2$ lo es) y, así, de $p \mid 2rs$ se sigue que $p \mid r$ o $p \mid s$. Pero como r y s son coprimos p no puede dividir a ambos a la vez y, en consecuencia, $p \nmid r^2 - s^2$, contradiciendo lo que habíamos supuesto. Por lo tanto si r y s no tienen la misma paridad, entonces la terna $(r^2 - s^2, 2rs, r^2 + s^2)$ es primitiva. Veamos ahora que toda terna pitagórica primitiva (a, b, c) tiene esta forma. Probemos primero que $a + bi$ y $a - bi$ son coprimos en $\mathbb{Z}[i]$. Supongamos que no y tomemos un primo γ de $\mathbb{Z}[i]$ que divide a $a + bi$ y $a - bi$. Entonces γ también divide a su suma $2a$ y a su diferencia $2bi$. Ahora, dado

que a y b son coprimos en $\mathbb{Z}$, existen $r, s \in \mathbb{Z}$ tales que $1 = ra + sb$. Así $2 = 2ar + 2as$ y, en consecuencia, $\gamma \mid 2 = -i(1+i)^2$. Como $-i \in \mathbb{Z}[i]^\times$, y γ y $1+i$ son primos de $\mathbb{Z}[i]$, se sigue de esto que γ es asociado a $1+i$. Por lo tanto $1+i \mid a+bi$ y así existen α y β en $\mathbb{Z}$ tales que

$$a + bi = (1+i)(\alpha + \beta i) = (\alpha - \beta) + (\alpha + \beta)i.$$

Pero esto implica $a \equiv b \pmod 2$, lo que es imposible ya que $(a, b, c)|$ es una terna primitiva. En consecuencia $a + bi$ y $a - bi$ son coprimos en $\mathbb{Z}[i]$. Como

$$(a + bi)(a - bi) = a^2 + b^2 = c^2,$$

de esto y de la unicidad de la factorización de c como producto de primos de $\mathbb{Z}[i]$, se sigue que existen $r, s \in \mathbb{Z}$ tales que $a + bi$ es asociado a $(r + si)^2 = (r^2 - s^2) + 2rsi$. Sustituyendo $r + si$ por su opuesto si hace falta, podemos suponer que $r \geq 0$ y, de hecho, que $r > 0$ pues si no a o b serían cero. Los posibles casos son

$$a + bi = \pm[(r^2 - s^2) + 2rsi] \qquad \text{y} \qquad a + bi = \pm i[(r^2 - s^2) + 2rsi] = \pm[2rs + (s^2 - r^2)i].$$

Pero como a es impar, necesariamente se tiene una de las primeras. Así

$$a = r^2 - s^2 \text{ y } b = 2rs \qquad \text{o} \qquad a = s^2 - r^2 \text{ y } b = 2r(-s).$$

En el primer caso, $r > s > 0$ (pues $a > 0$ y $b > 0$), mientras que, en el segundo caso, $-s > r > 0$ (nuevamente pues $a > 0$ y $b > 0$). Finalmente como a es impar, r y s no tienen la misma paridad, y como a y b son coprimos, r y s también lo son. □

Observación 2.17. *Es fácil ver que la aplicación*

$$\Gamma\colon \{(r, s) : r, s \in \mathbb{N} \text{ y } r > s\} \longrightarrow \{\textit{ternas pitagóricas primitivas}\},$$

dada por $\Gamma(r, s) := (r^2 - s^2, 2rs, r^2 + s^2)$ *es inversible y que*

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

2.1.3. El caso $n = 4$ del último teorema de Fermat

Vamos a probar el siguiente resultado del que claramente se deduce que el último teorema de Fermat el cierto para $n = 4$.

Teorema 2.18. *La ecuación* $X^4 + Y^4 = Z^2$ *no tiene soluciones positivas.*

Demostración. Supongamos que el teorema es falso y tomemos una solución (a, b, c) con c el mínimo posible. Denotemos con d al máximo divisor común de a y b. De $c^2 = a^4 + b^4$ se sigue que $d^2 \mid c$ y $(a/d, b/d, c/d^2)$ es una solución de $X^4 + Y^4 = Z^2$. Así $d = 1$, debido a la la minimalidad de c. En consecuencia (a^2, b^2, c) o (b^2, a^2, c) es una terna pitagórica primitiva. Intercambiando a con b si es necesario podemos suponer que estamos en el primer caso. Por el Teorema 2.16 existen $r > s > 0$ coprimos y de distinta paridad, tales que

$$a^2 = r^2 - s^2, \qquad b^2 = 2rs \qquad \text{y} \qquad c = r^2 + s^2. \tag{54}$$

Considerando la primera ecuación módulo 4, obtenemos que r es impar y s es par. Además, debido a la segunda igualdad todo divisor primo de s divide a b y, por lo tanto, s y a son coprimos. En consecuencia (a, s, r) es una terna pitagórica primitiva y, por consiguiente, existen enteros coprimos $u > v > 0$, tales que

$$a = u^2 - v^2, \qquad s = 2uv \qquad \text{y} \qquad r = u^2 + v^2. \tag{55}$$

Combinado la igualdades del medio de (54) y (55), obtenemos que $b^2 = 4ruv$. Como

$$\mathrm{mdc}(r, uv) = \mathrm{mdc}(u, v) = 1,$$

se sigue de esto y de que u, v y r son positivos, que existen A, B y C positivos, tales que $u = A^2$, $v = B^2$ y $r = C^2$. Notemos ahora que, por la última igualdad de (55), la terna (A, B, C) es una solución positiva de $X^4 + Y^4 = Z^2$. Como $C = \sqrt{r} \leq r^2 < c$ y c es minimal, esto es imposible. En consecuencia la ecuación $X^4+Y^4 = Z^2$ no tiene soluciones positivas. □

2.2. Factorización única en anillos de polinomios

Supongamos que k es un cuerpo. Como $k[X]$ es euclideano, se sigue del Teorema 12.8 del Capítulo 5, que es principal. En consecuencia, por la Proposicion 2.4 un polinomio no nulo de $k[X]$ es irreducible si y sólo si es primo, mientras que por el Teorema 2.5, el dominio $k[X]$ es de factorización única. En esta subsección vamos a probar que un dominio conmmutativo A es de factorización única si y sólo si $A[X]$ lo es. Comenzaremos con una observación elemental.

Observación 2.19. *Si A es un dominio conmutativo, entonces todo polinomio $P \in A[X]$ que divide a una constante no nula, tiene grado cero. Usando esto es muy fácil ver que $A[X]^\times = A^\times$ y que una constante no nula ni inversible $p \in A$, es irreducible en A si y sólo si lo es en $A[X]$. Por el Corolario 8.10 del Capítulo 5 lo mismo vale reemplazando "irreducible" por "primo" (aunque para esto no se necesita que A sea un dominio).*

Lema 2.20. *Para cada dominio de factorización única A y cada $p \in A \setminus \{0\}$ son equivalentes:*

1. *p es irreducible en A.*
2. *p es primo en A.*
3. *p es irreducible en $A[X]$.*
4. *p es primo en $A[X]$.*

Demostración. Por la observación anterior 1) $\Leftrightarrow$ 3) y 2) $\Leftrightarrow$ 4). Así, para terminar la demostración basta observar que, por la Proposicion 1.8 y el Teorema 1.9, los items 1) y 2) son equivalentes. □

Supongamos que A es un dominio de factorización única y denotemos con $\psi\colon A \setminus \{0\} \to \mathbb{N}$ a la función que a cada $a \in A \setminus \{0\}$ le asigna la cantidad de irreducibles de su factorización contados con su multiplicidad. Notemos que $\psi(ab) = \psi(a) + \psi(b)$ y que $\psi(a) = 0$ si y sólo si $a \in A^\times$.

Lema 2.21. *Si A es un dominio de factorización única y $a \in A \setminus \{0\}$ y $P, Q, R \in A[X]$ son tales que $aP = QR$, entonces existen $Q_1, R_1 \in A[X]$ tales que $Q_1 \mid Q$, $R_1 \mid R$, $\mathrm{gr}(Q_1) = \mathrm{gr}(Q)$, $\mathrm{gr}(R_1) = \mathrm{gr}(R)$ y $P = Q_1 R_1$.*

Demostración. Supongamos que el lema es falso y tomemos un contraejemplo $aP = QR$ con $\psi(a)$ lo mínimo posible. Necesariamente $\psi(a) > 0$, pues en caso contrario $a \in A^\times$ y podemos tomar $Q_1 := a^{-1}Q$ y $R_1 := R$. Así existe un primo $p \in A$ no nulo tal que $p \mid a$. Dado que por la observación anterior p es primo en $A[X]$, sabemos que $p \mid Q$ o $p \mid R$. Podemos suponer por simetría que $p \mid Q$. Escribamos $Q = p\overline{Q}$ y $a = p\overline{a}$. Simplificando p en la igualdad $aP = QR$ obtenemos $\overline{a}P = \overline{Q}R$. Pero como $\psi(\overline{a}) = \psi(a) - 1$, esto se contradice con la minimalidad de $\psi(a)$. Por lo tanto el lema es necesariamente cierto. □

LEMA 2.22. *Supongamos que A es un dominio de factorización única y denotemos con K al cuerpo de fracciones de A. Si $P \in A[X] \setminus A$ es irreducible en $A[X]$, entonces también lo es en $K[X]$.*

DEMOSTRACIÓN. Supongamos que P no es irreducible en $K[X]$, de modo que existen $Q, R \in K[X]$ tales que

$$P = QR, \quad \text{gr}(Q) > 0 \quad \text{y} \quad \text{gr}(R) > 0.$$

Escribamos los coeficientes de Q y R como cocientes de elementos que A y denotemos con a y b a múltiplos comunes no nulos de los denominadores de los coeficientes de Q y R respectivamente. Claramente $\overline{Q} := aQ$ y $\overline{R} := bR$ están en $A[X]$. Aplicando el Lema 2.21 a la igualdad $abP = \overline{Q}\,\overline{R}$ obtenemos Q_1 y R_1 en $A[X]$ tales que

$$P = Q_1 R_1, \quad \text{gr}(Q_1) = \text{gr}(Q) \quad \text{y} \quad \text{gr}(R_1) = \text{gr}(R) > 0,$$

lo que muestra que P no es irreducible en $A[X]$. □

A continuación extendemos la función ψ definida arriba del Lema 2.21. Concretamente suponemos que A es un dominio de factorización única y denotamos con $\psi\colon A[X] \setminus \{0\} \to \mathbb{N}$ a la función que a cada $P \in A[X] \setminus \{0\}$ le asigna $\text{gr}(P) + \psi(a)$, donde a es el coeficiente principal de P. Notemos que $\psi(PQ) = \psi(P) + \psi(Q)$ y que $\psi(P) = 0$ si y sólo si $P \in A[X]^\times$.

TEOREMA 2.23. *A es un dominio de factorización única si y sólo si $A[X]$ lo es.*

DEMOSTRACIÓN. Supongamos primero que $A[X]$ es un dominio de factorización única. Por el Teorema 1.9 cada $a \in A \setminus \{0\}$ se escribe como un producto

$$a = up_1 \cdots p_n,$$

donde $u \in A[X]^\times = A^\times$ y $p_1, \ldots, p_n$ son primos de $A[X]$. Claramente los grados de estos elementos son cero y, por la Observación 2.19, los p_i's son elementos primos de A. Por lo tanto A es factorial. Supongamos ahora que A es un dominio de factorización única y veamos que $A[X]$ también lo es. Probemos primero que cada polinomio no nulo con coeficientes en A se escribe como un producto de polinomios irreducibles. Supongamos que esto es falso y tomemos $P \in A[X] \setminus \{0\}$ que no se escribe como un producto de polinomios irreducibles con $\psi(P)$ el mínimo posible. Como P no es irreducible existen Q y R en $K[X]$ tales que

$$P = QR, \quad \psi(Q) > 0 \quad \text{y} \quad \psi(R) > 0.$$

Dado que $\psi(Q) < \psi(P)$ y $\psi(R) < \psi(P)$ se sigue de la definición de P que, tanto Q como R, se escriben como productos de polinomios irreducibles y así, pegando estas factorizaciones, obtenemos una factorización de P como producto de polinomios irreducibles. Como esto contradice la definición de P necesariamente todo polinomio no nulo de $A[X]$ se escribe como un producto de polinomios irreducibles. Por el Teorema 1.9, para terminar la demostración será suficiente probar que todo polinomio irreducible P de $A[X]$ es primo. Por el Lema 2.20 podemos suponer que $\text{gr}(P) > 0$. Tomemos ahora $Q, R \in A[X]$ tales que $P \mid QR$. Por el Lemma 2.22 y los comentarios hechos al comienzo de esta subsección, P es primo en $K[X]$ y, en consecuencia, $P \mid Q$ o $P \mid R$ en $K[X]$. Por simetría podemos suponer que existe $S \in K[X]$ tal que $SP = Q$. Para terminar la demostración será suficiente ver que $S \in A[X]$. Para ello, bastará ver que si $a \in A \setminus \{0\}$ es tal que $aS \in A[X]$ con $\psi(a)$ el mínimo posible, entonces $\psi(a) = 0$. Supongamos que $\psi(a) > 0$ y escribamos $a = pb$ con p primo. Como

$$P, aS \in A[X], \qquad p \mid aQ = (aS)P \qquad \text{y} \qquad p \nmid P \text{ (pues } P \text{ es irreducible y } \text{gr}(P) > 0),$$

se sigue del Lema 2.20, que $p \mid aS$ en $A[X]$. Así existe $S_1 \in A[X]$ tal que $pS_1 = aS = pbS$. Simplificando p en esta igualdad obtenemos $bS = S_1 \in A[X]$. Como $\psi(b) = \psi(a) - 1$, esto contradice la definición de a. Por lo tanto necesariamente $\psi(a) = 0$. □

Supongamos que A es un dominio de factorización única. Un polinomio $P \in A[X]$ es *primitivo* si el máximo divisor común de sus coeficientes es 1. En otras palabras si no existe ningún primo $p \in A$ tal que $p \mid P$. Notemos que el conjunto de los polinomios primitivos es cerrado por productos. En efecto si un primo p de A divide a un producto PQ de polinomios, entonces $p \mid P$ o $p \mid Q$ (pues por la Observación 2.19 sabemos que p es primo como elemento de $A[X]$). También vale recíprca, es decir que si PQ es primitivo, entonces P y Q también lo son (pues si $p \mid P$ entonces claramente $p \mid PQ$). Por último si $P \in A[X] \setminus \{0\}$ es arbitrario y a es un máximo divisor común de los coeficientes de P, entonces $P = aP_1$, donde P_1 es un polinomio primitivo (que resulta de dividir todos los coeficientes de P por a. A continuación describimos los polinomios irreducibles de $A[X]$).

Proposición 2.24. *Supongamos que A es un dominio de factorización única y denotemos con K a su cuerpo de fracciones. Para cada polinomio no constante $P \in A[X]$, las condiciones siguientes son equivalentes:*

1. *P es irreducible en $A[X]$.*
2. *P es primitivo e irreducible en $K[X]$.*
3. *P es primitivo y si $P = QR$ con $Q, R \in K[X]$, entonces $\operatorname{gr}(Q) = 0$ o $\operatorname{gr}(R) = 0$.*
4. *P es primitivo y si $P = QR$ con $Q, R \in A[X]$, entonces $\operatorname{gr}(Q) = 0$ o $\operatorname{gr}(R) = 0$.*

Demostración. 1) ⇒ 2) Como $\operatorname{gr}(P) > 0$ y P es irreducible, es evidente que P es primitivo. Por el Lemma 2.22 ya sabemos que P es irreducible en $K[X]$.

2) ⇒ 3) Esto es evidente pues las unidades de $K[X]$ son constantes.

3) ⇒ 4) Esto es trivial.

4) ⇒ 1) Pues como P es primitivo sus divisores de grado cero son inversibles. □

Dados un anillos conmutativos A y B y un morfismo de anillos $f\colon A \to B$, denotaremos con $\Theta_f\colon A[X] \to B[X]$ al morfismo de anillos definido por

$$\Theta_f\left(a_n X^n + \cdots + a_0\right) = f(a_n)X^n + \cdots + f(a_0).$$

A veces para estudiar las factorizaciones de un polinomio $P \in A[X]$ es util considerar un morfismo de anillos $f\colon A \to B$ y analizar las factorizaciones de $\Theta_f(P)$ en $B[X]$. Esto se debe al hecho de que si $P = QR$ es una factorización de P en $A[X]$, entonces $\Theta_f(P) = \Theta_f(Q)\Theta_f(R)$ es una factorización de $\Theta_f(P)$ en $B[X]$. A continuación aplicaremos este método para ver que $X^4 + 4X + 1 \in \mathbb{Z}[X]$ es irreducible. Para ello usaremos la aplicación canónica $\pi\colon \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$. Como P no tiene raíces en $\mathbb{Z}$ una factorización no trivial en $\mathbb{Z}[X]$ debería ser escencialmente de la forma $X^4 + 4X + 1 = QR$ con $\operatorname{gr}(Q) = \operatorname{gr}(R) = 2$, lo que daría lugar a la factorización similar $\theta_\Pi(X^4 + 4X + 1) = \theta_\Pi(Q)\theta_\Pi(R)$ en $(\mathbb{Z}/3\mathbb{Z})[X]$. Pero esto es imposible, ya que

$$\theta_\Pi(X^4 + 4X + 1) = X^4 + X + 1 = (X + 2)(X^3 + X^2 + X + 2),$$

con el factor de grado 3 irreducible (porque no tiene raíces).

A continuación usamos este método para establecer tres criterios, que dan condiciones suficiente para que un polinimio $P = a_n X_n + \cdots + a_0$, de grado $n > 0$, con coeficientes en un dominio de factorización única A, sea irreducible.

PROPOSICIÓN 2.25 (Eisenstein). *Si P es primitivo y existe un irreducible p no nulo en A tal que $p \mid a_i$ para todo $0 \leq i < n$ y $p^2 \nmid a_0$, entonces P es irreducible.*

DEMOSTRACIÓN. Supongamos que P no es irreducible y que $P = QR$ es una factorización no trivial de P. Consideremos el morfismo canónico $\pi\colon A \to A/pA$. Entonces

$$\pi(a_n)X^n = \theta_\Pi(P) = \theta_\Pi(Q)\theta_\Pi(R)$$

es una factorización no trivial de $\pi(a_n)X^n$. Por lo tanto los términos independientes de Q y R son divisibles por p y, así, $p^2 \mid a_0$. En consecuencia P es irreducible. □

OBSERVACIÓN 2.26. *Usualmente se agrega la hipótesis de que $p \nmid a_n$ a las condiciones de la proposición anterior. Sin embargo esto es automático, ya que, como P es primitivo y $p \mid a_i$ para todo $0 \leq i < n$, necesariamente $p \nmid a_n$.*

PROPOSICIÓN 2.27. *Si P es primitivo y existe un irreducible p no nulo en A tal que $p \mid a_i$ para todo $0 < i \leq n$ y $p^2 \nmid a_n$, entonces P es irreducible.*

DEMOSTRACIÓN. Supongamos que P no es irreducible y Tomemos una factorización no trivial $P = QR$ de P. Consideremos el morfismo canónico $\pi\colon A \to A/pA$. Entonces

$$\pi(a_0) = \theta_\Pi(P) = \theta_\Pi(Q)\theta_\Pi(R)$$

es una factorización no trivial de $\pi(a_0)$. Por lo tanto los términos principales de Q y R son divisibles por p y, así, $p^2 \mid a_n$. En consecuencia P es irreducible. □

OBSERVACIÓN 2.28. *Usualmente se agrega la hipótesis de que $p \nmid a_0$ a las condiciones la proposición anterior. Sin embargo esto es automático, ya que, como P es primitivo y $p \mid a_i$ para todo $0 < i \leq n$, necesariamente $p \nmid a_0$.*

En la proposición que sigue k es un cuerpo y $f\colon A \to k$ es un morfismo de anillos.

PROPOSICIÓN 2.29. *Si P es primitivo, $\theta_f(P)$ es irreducible en $k[X]$ y $\operatorname{gr}(\theta_f(P)) = \operatorname{gr}(P)$, entonces P es irreducible.*

DEMOSTRACIÓN. Por la proposición 2.24 basta ver que si $P = QR$ con $Q, R \in A[X]$, entonces $\operatorname{gr}(Q) = 0$ o $\operatorname{gr}(R) = 0$. Denotemos con a, b y c a los coeficientes principales de P, Q y R, respectivamente. Entonces $a = bc \notin \operatorname{Ker}(f)$ y por lo tanto $b, c \notin \operatorname{Ker}(f)$, por lo que $\operatorname{gr}(Q) = \operatorname{gr}(\theta_f(Q))$ y $\operatorname{gr}(R) = \operatorname{gr}(\theta_f(R))$. Ahora como $\theta_f(P)$ es irreducible en $k[X]$, de $\theta_f(P) = \theta_f(Q)\theta_f(R)$ se sigue que $\operatorname{gr}(Q) = \operatorname{gr}(\theta_f(Q)) = 0$ o $\operatorname{gr}(R) = \operatorname{gr}(\theta_f(R)) = 0$, lo que termina la demostración. □

Capítulo 7

Teoría elemental de módulos

1. Módulos

Una *acción a izquierda* de un anillo A sobre un grupo abeliano M es una aplicación $(a, m) \mapsto a \cdot m$, de $A \times M$ en M, que satisface:

1. $1 \cdot m = m$ para todo $m \in M$,
2. $a \cdot (m + n) = a \cdot m + a \cdot n$ para todo $a \in A$ y $m, n \in M$,
3. $(a + b) \cdot m = a \cdot m + b \cdot m$ para todo $a, b \in A$ y $m \in M$,
4. $a \cdot (b \cdot m) = (ab) \cdot m$ para todo $a, b \in A$ y $m \in M$.

La primera igualdad dice que la acción es unitaria, las dos siguientes que es distributiva y la última que es asociativa. De ahora en más escribiremos $ab \cdot m$ en lugar de $(ab) \cdot m$.

Un *A-módulo a izquierda* o *módulo a izquierda sobre A* es un grupo abeliano M provisto de una acción a izquierda de A sobre M.

La terminología "acción a izquierda" y "A-módulo a izquierda" utilizada, sugiere que hay versiones a derecha de estos conceptos, y sólo tiene sentido si estas verdaderamente existen. Como es de esperarse, este es el caso.

Dados un anillo A y un grupo abeliano M, una *acción a derecha* de A sobre M es una aplicación $(m, a) \mapsto m \cdot a$, de $M \times A$ en M, que satisface:

1. $m \cdot 1 = m$ para todo $m \in M$,
2. $(m + n) \cdot a = m \cdot a + n \cdot a$ para todo $a \in A$ y $m, n \in M$,
3. $m \cdot (a + b) = m \cdot a + m \cdot b$ para todo $a, b \in A$ y $m \in M$,
4. $(m \cdot a) \cdot b = m \cdot (ab)$ para todo $a, b \in A$ y $m \in M$.

Un *A-módulo a derecha* o *módulo a derecha sobre A* es un grupo abeliano M provisto de una acción a derecha de A sobre M. Es evidente que una acción a derecha de A sobre un grupo abeliano es simplemente una acción a izquierda de A^{op} sobre el mismo grupo, y que un A-módulo a derecha no es otra cosa que un A^{op}-módulo a izquierda, de modo que las dos teorías son equivalentes. Debido a esto sólo consideraremos módulos a izquierda, dejando al lector

la tarea de trasladar los resultados al contexto de módulos a derecha. Consecuentemente, a partir de ahora cuando hablemos de un A-módulo o módulo sobre A nos estaremos refiriendo a un módulo a izquierda, y llamaremos *acciones* a las acciones a izquierda.

EJERCICIO 1.1. *Pruebe que*

$$a \cdot 0 = 0 \cdot m = 0 \qquad y \qquad (-a) \cdot m = a \cdot (-m) = -a \cdot m,$$

para todo $a \in A$ *y* $m \in M$.

Consideremos un grupo abeliano M. Para cada acción de un anillo A sobre M y cada $a \in A$, la función $\rho(a)\colon M \to M$ definida por $\rho(a)(m) := a \cdot m$, es un endomorfismo de M, y la aplicación

$$\begin{aligned} A &\longrightarrow \mathrm{End}(M) \\ a &\longmapsto \rho(a) \end{aligned}$$

es un morfismo de anillos. Recíprocamente, si $\rho\colon A \to \mathrm{End}(M)$ es un morfismo de anillos, entonces la fórmula $a \cdot m := \rho(a)(m)$ define una acción de A sobre M. Estas construcciones son inversa una de la otra (si se empieza con una acción y se construyen sucesivamente el morfismo y la acción asociados, se recupera la acción original, y similarmente si se comienza con un morfismo). Así, dotar a un grupo abeliano M de una estructura de A-módulo es lo mismo que dar un morfismo de anillos de A en $\mathrm{End}(M)$.

EJEMPLO 1.2. *El* A-módulo nulo *es el grupo* 0 *provisto de la única acción a izquierda de* A *sobre él.*

EJEMPLO 1.3. *Cada anillo* A *es un* A*-módulo bajo la* acción regular a izquierda*, dada por la multiplicación. Cuando consideremos a* A *como módulo vía esta acción lo denotaremos* ${}_AA$.

EJEMPLO 1.4. *Un módulo sobre un cuerpo* k *es un* k*-espacio vectorial.*

EJEMPLO 1.5. *Por el Ejemplo 4.2 del Capítulo 5, para cada grupo abeliano* M *hay un único morfismo de anillos* $\iota\colon \mathbb{Z} \to \mathrm{End}(M)$*. Debido a esto las teorías de* $\mathbb{Z}$*-módulos y de grupos abelianos coinciden. Es fácil ver que*

$$n \cdot m = \begin{cases} \underbrace{m + \cdots + m}_{n \text{ veces}} & \text{si } n > 0, \\ 0 & \text{si } n = 0, \\ \underbrace{(-m) + \cdots + (-m)}_{-n \text{ veces}} & \text{si } n < 0. \end{cases}$$

EJEMPLO 1.6. *Supongamos que* $\varphi\colon A \to B$ *es un morfismo de anillos. Entonces cada* B*-módulo* M *es un* A*-módulo vía* $a \cdot m := \varphi(a) \cdot M$*. A veces denotaremos a este* A*-módulo con* M_φ*. En general, pero especialmente cuando* A *es un subanillo de* B *y* φ *es la inclusión canónica, diremos que* M_φ *es obtenido a partir de* M *por restricción de escalares.*

EJEMPLO 1.7. *Por el ejemplo anterior si* M *es un módulo sobre el anillo* $k[X]$ *de polinomios en una variable con coeficientes en un cuerpo* k*, entonces* M *es un* k*-espacio vectorial. Además dado que para todo* $m, n \in M$ *y* $\lambda \in k$*,*

$$X \cdot (m + n) = X \cdot m + X \cdot n \qquad y \qquad X \cdot (\lambda \cdot m) = (X\lambda) \cdot m = (\lambda X) \cdot m = \lambda \cdot (X \cdot m),$$

la función $f\colon M \to M$*, definida por* $f(m) := X \cdot m$ *es un endomorfismo de* k*-espacios vectoriales. Supongamos ahora que* M *es un* k*-espacio vectorial provisto de un endomorfismo de*

k-espacios vectoriales $f\colon M \to M$. Entonces la acción de k sobre M se extiende de manera única a una acción de $k[X]$ sobre M tal que $X \cdot m = f(m)$ para todo $m \in M$. Estas construcciones son inversa una de la otra. Así, tener un $k[X]$-módulo es "lo mismo" que tener un k-espacio vectorial con un endomorfismo distinguido. Una forma alternativa de probar esto es recordar que proveer de una estructura de $k[X]$-módulo a un grupo abeliano M es equivalente a dar un morfismo de anillos de $k[X]$ en $\mathrm{End}(M)$, y utilizar la propiedad universal del anillo de polinomios (Observación 14.10).

Ejemplo 1.8. *Razonando como en el ejemplo anterior se puede ver que un $\mathbb{Z}[i]$-módulo no es otra cosa que un grupo abeliano M provisto de un endomorfismo $f\colon M \to M$ que satisface $f^2 = -\mathrm{id}$.*

Ejemplo 1.9. *Consideremos el anillo $k[S]$, de un monoide S con coeficientes en un cuerpo k. Si M es un $k[S]$-módulo, entonces*

- *M es un k-espacio vectorial,*
- *Para cada $s \in S$ la función $\rho(s)\colon M \to N$, definida por $\rho(s)(m) := s \cdot m$ es un endomorfismo de k-espacios vectoriales,*
- *La función*

$$\begin{aligned} S &\xrightarrow{\ \rho\ } \mathrm{End}_k(M) \\ s &\longmapsto \rho(s) \end{aligned}$$

es un morfismo de monoides.

Recíprocamente, dados un k-módulo M y un morfismo de monoides $\rho\colon S \to \mathrm{End}_k(M)$, la acción de k sobre M se extiende de manera única a una acción de $k[S]$ sobre M, tal que $s \cdot m = \rho(s)(m)$ para todo $s \in S$ y $m \in M$.

Observación 1.10. *Una* representación *de un grupo G sobre un k-espacio vectorial M es un morfismo de grupos $\rho\colon G \to \mathrm{Aut}_k(M)$. Si en el ejemplo anterior S es un grupo, entonces $\rho(s)$ es un automorfismo para cada $s \in S$. Usando esto se ve inmediatamente que si S es un grupo, entonces un $k[S]$-módulo es un k-espacio vectorial M provisto de una representación de S sobre M.*

Un A-módulo M es fiel si para todo $a \in A \setminus \{0\}$ existe $m \in M$ tal que $a \cdot m \neq 0$ o, equivalentemente, si el morfismo de anillos asociado $\rho\colon A \to \mathrm{End}(M)$ es inyectivo. Si M no es fiel e $I = \ker \rho$, entonces M deviene un A/I-módulo fiel vía la acción inducida $[a] \cdot m = a \cdot m$. Por ejemplo, $\mathbb{Z}_6 \times \mathbb{Z}_9$ no es un $\mathbb{Z}$-módulo fiel. El núcleo del morfismo $\rho\colon Z \to \mathrm{End}(\mathbb{Z}_6 \times \mathbb{Z}_9)$ asociado es $18\mathbb{Z}$. La acción inducida de $\mathbb{Z}_{18}$ sobre $\mathbb{Z}_6 \times \mathbb{Z}_9$ es fiel. A $\ker \rho$ se lo llama también el *anulador* de M y se lo denota $\mathrm{An}(M)$.

2. Submódulos

Un subconjunto N de un A-módulo M es un *submódulo* de M si es cerrado para la suma y $a \cdot m \in N$ para todo $a \in A$ y $m \in N$. Por ejemplo 0 y M son submódulos de M. Estos son los llamados *submódulos triviales*. Un submódulo de M es *propio* si es distinto de M. Como el conjunto de los submódulos de M es cerrado bajo intersecciones, para cada $S \subseteq M$ existe un mínimo submódulo AS de M que contiene a S, llamado *el submódulo de M generado por S*, el cual es precisamente la intersección de todos los submódulos de M que contienen a S. Una

notación alternativa bastante usual para AS es $\langle S\rangle$. Es evidente que AS es el conjunto de las sumas finitas de elementos de la forma $a \cdot m$, con $a \in A$ y $m \in S$. Dado $m \in M$ escribiremos Am en lugar de $A\{m\}$. Además, cuando $S = \{s_1, \ldots, s_n\}$ escribimos $\langle s_1, \ldots, s_n\rangle$ en lugar de $\langle\{s_1, \ldots, s_n\}\rangle$. Decimos que S *genera a* M o que es un *conjunto de generadores de* M si $AS = M$. Un módulo M es finitamente generado si existe un conjunto finito S de M tal que $M = AS$, y es cíclico si existe $m \in M$ tal que $M = Am$.

La *suma* $\sum_{j\in J} M_j$, de una familia arbitraria de submódulos $(M_j)_{j\in J}$ de M, es el submódulo de M generado por la unión $\bigcup_{j\in J} M_j$ de los miembros de $(M_j)_{j\in J}$. Es fácil ver que

$$\sum_{j\in J} M_j = \left\{ \sum_{j\in J} m_j : m_j \in M_j \text{ y } (m_j)_{j\in J} \text{ tiene soporte finito} \right\}.$$

Un A-módulo M es *suma* de una familia $(M_j)_{j\in J}$ de submódulos si $\sum_{j\in J} M_j = M$.

Proposición 2.1. *Para cada A-módulo M son equivalentes:*

1. *M es finitamente generado.*
2. *Cada familia de submódulos de M cuya suma es M tiene una subfamila finita cuya suma también es M.*
3. *M pertenece a cada familia de submódulos de M que es cerrada bajo sumas finitas y cuya suma es M.*

Demostración. 1) $\Rightarrow$ 2) Supongamos que $M = A\{x_1, \ldots, x_n\}$ y que $(M_i)_{i\in I}$ es una familia de submódulos de M cuya suma es M. Para cada $1 \leq j \leq n$ existe un subconjunto finito I_j de I tal que $x_j \in \sum_{i\in I_j} M_i$ y así $M = \sum_{i\in I'} M_i$, donde $I' = I_1 \cup \cdots \cup I_n$.

2) $\Rightarrow$ 3) Esto es claro.

3) $\Rightarrow$ 1) Aplíquese el item 3) a la familia formada por los submódulos finitamente generados de M. □

Un conjunto de generadores S de M es *minimal* si ningún subconjunto propio de S genera a M. Todo conjunto finito de generadores de M contiene uno que es minimal, como puede comprobarse fácilmente. Existen módulos que no tienen conjuntos de generadores minimales. Un ejemplo es el grupo aditivo $\mathbb{Q}$.

Proposición 2.2. *Si un módulo M es finitamente generado, entonces todo conjunto de generadores de M contiene un subconjunto finito que también genera a M (en particular todos los conjuntos minimales de generadores de M son finitos). Si no lo es, entonces todos los conjuntos minimales de generadores de M (suponiendo que haya alguno) tienen el mismo cardinal.*

Demostración. Tomemos conjuntos de generadores S y T de M. Para cada $t \in T$ existe un subconjunto finito S_t de S, tal que $t \in AS_t$. Como T genera M, el subconjunto $S' = \bigcup_{t\in T} S_t$ de S también lo hace. La primera afirmación se sigue inmediatamente de este hecho tomando T finito. Supongamos ahora que S es minimal y que T es infinito. Entonces $S = S'$ y de la igualdad $S = \bigcup_{t\in T} S_t$ se sigue que $|S| \leq |T|$. En consecuencia, si T también es mininal, entonces por simetría $|S| = |T|$. □

Un módulo finitamente generado puede tener conjuntos minimales de generadores de distinto cardinal. Por ejemplo si a y $1-a$ son elementos no inversibles a izquierda de A, entonces tanto $\{1\}$ como $\{a, 1-a\}$ son conjuntos minimales de generadores de ${}_AA$.

Para terminar, consideremos algunos de los ejemplos mencionados en la sección anterior, y veamos cuales son los submódulos. Los de un k-espacio vectorial son los subespacios vectoriales; los de un $\mathbb{Z}$-módulo, los subgrupos; los de un $k[X]$-módulo, los subespacios vectoriales estables bajo la acción de X; los de un $k[S]$-módulo, los subespacios vectoriales cerrados bajo la acción de S; y los de ${}_AA$, los ideales a izquierda.

3. Morfismos de módulos

Un *morfismo* de A-módulos $f\colon M \to N$ es una terna (M, f, N), donde f es un morfismo del grupo abeliano subyacente de M en el de N, que satisface

$$f(a \cdot m) = a \cdot f(m) \qquad \text{para todo } a \in A \text{ y } m \in M.$$

El A-módulo M es el dominio de $f\colon M \to N$ y N es el codominio.

Por ejemplo, la identidad $\mathrm{id}_M\colon M \to M$ y, más generalmente, la inclusión canónica $i\colon N \to M$ de un submódulo N de M en M, es un morfismo. También lo es la composición $g \circ f\colon M \to L$, definida en forma evidente, de dos morfismos $f\colon M \to N$ y $g\colon N \to L$. Los morfismos de A-módulos son llamados también *aplicaciones A-lineales*.

Muchas de las propiedades básicas de los morfismos de A-módulos son análogas a las establecidas para los de monoides, grupos y anillos. Las definiciones de endomorfismo, isomorfismo, automorfismo, monomorfismo, epimorfismo, sección y retracción son las mismas. Sigue siendo cierto que un morfismo es un isomorfismo si y sólo si es biyectivo. Mantenemos la notación $M \simeq M'$ para señalar que los A-módulos M y M' son isomorfos. Es fácil ver que los monomorfismos, epimorfismos, secciones y retracciones son cerrados bajo composición, que toda retracción es sobreyectiva, toda sección es inyectiva, todo morfismo inyectivo es un monomorfismo, y todo morfismo sobreyectivo es un epimorfismo. También que un morfismo $f\colon M \to M'$ es un isomorfismo si y sólo si es una sección y un epimorfismo, y que esto ocurre si y sólo si es una retracción y un monomorfismo.

Todo monomorfismo $f\colon M \to M'$ es inyectivo. En efecto, si $f(m) = f(m')$, entonces $f \circ g = f \circ g'$, donde $g, g'\colon {}_AA \to M$ son los morfismos definidos por

$$g(a) = a \cdot m \quad \text{y} \quad g'(a) = a \cdot m' \text{ para todo } a \in A.$$

Por lo tanto $g = g'$ y entonces $m = m'$. También es cierto que los epimorfismos son sobreyectivos, pero no podemos probarlo todavía, por lo que dejamos la demostración para más adelante.

Los ejemplos dados en la Sección 11 del Capitulo 1 muestran que cuando $A = \mathbb{Z}$ hay monomorfismos que no son secciones y epimorfismos que no son retracciones.

Tal como para monoides, grupos y anillos, dados morfismos $f\colon M \to N$ y $g\colon N \to L$,

1. Si $g \circ f$ es una sección o un monomorfismo, entonces también lo es f.
2. Si $g \circ f$ es una retracción o un epimorfismo, entonces también lo es g.

Los símbolos $\mathrm{Hom}_A(M, M')$, $\mathrm{Iso}_A(M, M')$, $\mathrm{End}_A(M)$ y $\mathrm{Aut}_A(M)$ denotan respectivamente a los conjuntos de morfismos de A-módulos de M en M', isomorfismos de M en M',

endomorfismos de M y automorfismos de M. Es inmediato que $\mathrm{End}_A(M)$ es un monoide (cuyo elemento neutro es la función identidad) vía la composición y que $\mathrm{Aut}_A(M)$ es su grupo de unidades.

Como veremos enseguida, los morfismos de A-módulos tienen una estructura mucho más rica que los de monoides, grupos y anillos. En particular, $\mathrm{End}_A(M)$ tiene una estructura natural de anillo.

3.1. Estructuras en el conjunto de los morfismos de un módulo en otro

Para cada par de A-módulos a izquierda M y N, el conjunto $\mathrm{Hom}_A(M,N)$ es un grupo abeliano vía $(f+g)(m) := f(m)+g(m)$. El neutro es el *morfismo nulo* $0_{MN}\colon M \to N$, que envía cada elemento de M en 0, y el opuesto de un morfismo $f\colon M \to N$, es la función $-f\colon M \to N$ que envía cada $m \in M$ en $-f(m)$. La composición es distributiva con respecto a la suma y en particular $\mathrm{End}_A(M)$ es un anillo cuyo neutro es id_M. Notemos que de la distributividad de la composición con respecto a la suma se sigue también que las aplicaciones

$$v_*\colon \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,N') \quad \text{y} \quad u^*\colon \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M',N),$$

definidas para cada par de morfismos de A-módulos, $v\colon N \to N'$ y $u\colon M' \to M$, por

$$v_*(f) := v \circ f \qquad \text{y} \qquad u^*(f) := f \circ u$$

respectivamente, son morfismos de grupos abelianos. Las correspondencias $v \mapsto v_*$ y $u \mapsto u^*$ tienen la siguientes propiedades:

1. $\mathrm{id}_* = \mathrm{id}$.
2. $(v' \circ v)_* = v'_* \circ v_*$ para cada par de morfismos $v\colon N \to N'$ y $v'\colon N' \to N''$.
3. $(v'+v)_* = v'_* + v_*$ para cada par de morfismos $v, v'\colon N \to N'$.
4. $\mathrm{id}^* = \mathrm{id}$.
5. $(u \circ u')^* = u'^* \circ u^*$ para cada par de morfismos $u\colon M' \to M$ y $u'\colon M'' \to M'$.
6. $(u'+u)^* = u'^* + u^*$, para cada par de morfismos $u, u'\colon M' \to M$.

Nota 3.1. *En general* $\mathrm{Hom}_A(M,N)$ *no es un A-módulo, pero siempre es un módulo sobre el centro de A vía $(a \cdot f)(a') := a \cdot f(a')$. Con esta definición los morfismos v_* y u^* resultan ser* Z *A-lineales.*

Observación 3.2. *Para cada A-módulo M, el grupo* $\mathrm{Hom}_A(A,M)$ *es un A-módulo vía la acción definida por $(a \cdot f)(a') := f(a'a)$. Además la función*

$$\begin{aligned} M &\longrightarrow \mathrm{Hom}_A(A,M)\ , \\ m &\longmapsto f_m \end{aligned} \tag{56}$$

donde f_m es la aplicación A-lineal dada por $f_m(a) := a \cdot m$, es un isomorfismo de módulos. Su inversa es la función que cada morfismo $f\colon A \to M$ le asigna su valor en 1. Además, si $\phi\colon M \to N$ es A-lineal, entonces también lo es $\phi_*\colon \mathrm{Hom}_A(A,M) \to \mathrm{Hom}_A(A,N)$, y el diagrama

$$\begin{array}{ccc} M & \xrightarrow{\ \phi\ } & N \\ \downarrow & & \downarrow \\ \mathrm{Hom}_A(A,M) & \xrightarrow{\ \phi_*\ } & \mathrm{Hom}_A(A,N) \end{array}$$

conmuta.

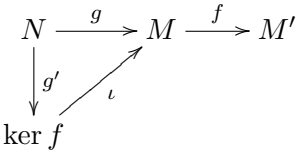
Cuando $M = A$ tiene sentido preguntarse si la aplicación dada en (56) *es un isomorfismo de anillos. Un cálculo sencillo muestra que $f_{ab} = f_b \circ f_a$, de manera que si lo es, pero de A^{op} en $\mathrm{End}_A(A)$.*

4. Núcleo e imagen

El *núcleo* $\ker f$ de un morfismo de A-módulos $f\colon M \to M'$ es la preimagen de 0 por f. Es evidente que $\ker f$ es un submódulo de M e $\mathrm{Im}\, f$ un submódulo de M'. Más aún, no es difícil comprobar que la imagen de un submódulo N de M es un submódulo de M', y que la preimagen de un submódulo N' de M' es un submódulo de M.

Es obvio que la inclusión canónica $\iota\colon \ker f \to M$ tiene las siguientes propiedades, la segunda de la cuales es llamada la *propiedad universal del núcleo*:

- $f \circ \iota = 0_{\ker f, M}$,
- Para cada morfismo de A-módulos $g\colon N \to M$ que satisface $f \circ g = 0_{NM'}$, existe un único morfismo de A-módulos $g'\colon N \to \ker f$ tal que el diagrama



  conmuta.

Proposición 4.1. *Si $f\colon M \to M'$ es un morfismo de A-módulos, entonces dos elementos $m, n \in M$ tienen la misma imagen bajo f si y sólo si $m + \ker f = n + \ker f$.*

Demostración. Por la Proposición 12.2 del Capítulo 1. □

Corolario 4.2. *Un morfismo f de A-módulos es inyectivo si y sólo si* $\ker f = 0$.

5. Cociente de módulos

Fijados un anillo A, un A-módulo M y un subgrupo N de M, consideremos el grupo cociente M/N fde M por N. Recordemos que la proyección canónica $\pi\colon M \to M/N$ es un morfismo de grupos. Afirmamos que hay una acción de A en M/N tal que M/N es un A-módulo y π es un morfismo de A-módulos si y sólo si N es un submódulo de M. Para que π respete la acción, forzosamente la acción de A sobre M/N debe estar dada por

$$a \cdot [m] = [a \cdot m]. \tag{57}$$

Así, si esta definición es correcta, entonces

$$a \in A \text{ y } m \in N \Rightarrow a \cdot [m] = a \cdot [0] = [a \cdot 0] = [0] \Rightarrow a \cdot m \in N,$$

y, por lo tanto, N es un submódulo de M. Recíprocamente, si este es el caso, entonces para todo $m \in M$ y todo $m' \in N$,

$$a \cdot [m + m'] = [a \cdot (m + m')] = [a \cdot m + a \cdot m'] = [a \cdot m],$$

de modo que la definición (57) es correcta. Las igualdades

$$1 \cdot [m] = [1 \cdot m] = [m],$$
$$aa' \cdot [m] = [aa' \cdot m] = [a \cdot (a' \cdot m)] = a \cdot [a' \cdot m] = a \cdot (a' \cdot [m]),$$
$$a \cdot ([m]+[m']) = a \cdot [m+m']) = [a \cdot (m+m')] = [a \cdot m + a \cdot m'] = [a \cdot m]+[a \cdot m'] = a \cdot [m]+a \cdot [m']$$

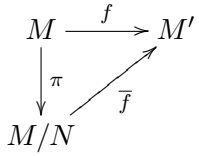
y

$$(a+a') \cdot [m] = ([(a+a') \cdot m] = [(a+a') \cdot m] = [a \cdot m + a' \cdot m] = [a \cdot m]+[a' \cdot m] = a \cdot [m]+a \cdot [m'],$$

muestran que M/N es un A-módulo. Es evidente que $\ker \pi = N$, lo cual muestra, en particular, que todo submódulo de M es el núcleo de un morfismo.

La proyección canónica $\pi \colon M \to M/N$ tiene la siguiente propiedad, llamada *propiedad universal del cociente*:

- Si $f \colon M \to M'$ es un morfismo de A-módulos cuyo núcleo incluye a N, entonces existe un único morfismo de A-módulos $\overline{f} \colon M/N \to M'$ tal que el triángulo



  conmuta.

Para comprobarlo basta observar que, por la propiedad universal del cociente de grupos, dado un morfismo de grupos abelianos $f \colon M \to M'$ con $N \subseteq \ker f$, existe un único morfismo de grupos abelianos $\overline{f} \colon M/N \to M'$ tal que $\overline{f} \circ \pi = f$, y notar que, si f es A-lineal, entonces

$$a \cdot \overline{f}([m]) = a \cdot [f(m)] = [a \cdot f(m)] = [f(a \cdot m)] = \overline{f}([a \cdot m]) = \overline{f}(a \cdot [m]).$$

Es fácil ver que $\ker \overline{f} = \ker f/N$ e $\operatorname{Im} \overline{f} = \operatorname{Im} f$ (de hecho, esto es una consecuencia inmediata de que ambas propiedades son ciertas en la teoría de grupos).

El resto de la sección estará dedicado a establecer algunos resultados que son consecuencias más o menos directa de la propiedad universal del cociente. Entre ellos, los teoremas de isomorfismo de Noether.

Teorema 5.1 (Primer teorema de isomorfismo). *Toda función A-lineal $f \colon M \to M'$ induce un isomorfismo $\overline{f} \colon M/\ker f \to \operatorname{Im} f$.*

Demostración. Es claro. □

Ejemplo 5.2. *Supongamos que $M = Am$ es cíclico. Entonces el morfismo*

$$\begin{array}{ccc} A & \longrightarrow & M \\ a & \longmapsto & a \cdot m \end{array},$$

es sobreyectivo y su núcleo es un ideal a izquierda I. Así, por el teorema anterior, $M \simeq A/I$.

Teorema 5.3 (Segundo teorema de isomorfismo). *Si $L \subseteq N$ son submódulos de un A-módulo M, entonces N/L es un submódulo de M/L y $M/N \simeq (M/L)/(N/L)$.*

Demostración. Copie la prueba del Teorema 13.4 del Capítulo 1. □

TEOREMA 5.4 (Tercer teorema de isomorfismo). *Si L y N son dos submódulos de un A-módulo M, entonces $L/L \cap N \simeq (N + L)/N$.*

DEMOSTRACIÓN. Copie la prueba del Teorema 13.5 del Capítulo 1.. □

Consideremos un morfismo de A-módulos $f\colon M \to M'$ y submódulos N de M y N' de M'. Por la propiedad universal del cociente, si $f(N) \subseteq N'$, entonces existe un único morfismo $\overline{f}\colon M/N \to M'/N'$ tal que el cuadrado

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ M/N & \xrightarrow{\overline{f}} & M'/N' \end{array},$$

donde π y π' son las proyecciones canónicas, conmuta. De las fórmulas para el núcleo y la imagen obtenidas al establecer la misma, se sigue de inmediato que

$$\operatorname{Im} \overline{f} = \pi'(\operatorname{Im} f) \qquad \text{y} \qquad \ker \overline{f} = f^{-1}(N')/N.$$

PROPOSICIÓN 5.5. *La correspondencia establecida arriba tiene las siguientes propiedades:*

1. *Para todo submódulo N de M, el morfismo $\overline{\mathrm{id}}\colon M/N \to M/N$ es la identidad de M/N.*
2. *Consideremos morfismos de A-módulos $f\colon M \to M'$ y $g\colon M' \to M''$ y submódulos N de M, N' de M' y N'' de M''. Si $f(N) \subseteq N'$ y $g(N') \subseteq N''$, entonces $g(f(N)) \subseteq N''$ y $\overline{g \circ f} = \overline{g} \circ \overline{f}$.*

DEMOSTRACIÓN. Por la unicidad de los morfismos $\overline{\mathrm{id}}$ y $\overline{g \circ f}$, basta observar que el cuadrado

$$\begin{array}{ccc} M & \xrightarrow{\mathrm{id}} & M \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ M/N & \xrightarrow{\mathrm{id}} & M/N \end{array}$$

y el rectángulo exterior del diagrama

$$\begin{array}{ccccc} M & \xrightarrow{f} & M' & \xrightarrow{g} & M'' \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi''} \\ M/N & \xrightarrow{\overline{f}} & M'/N' & \xrightarrow{\overline{g}} & M''/N'' \end{array}$$

conmutan. □

El conjunto $\mathrm{Sub}_N(M)$, de los submódulos de un A-módulo M que incluyen a un submódulo dado N, es un reticulado completo vía el orden dado por la inclusión. El ínfimo de una familia $(M_i)_{i\in I}$ de submódulos de M es la intersección $\bigcap_{i\in I} M_i$, y el supremo es la suma $\sum_{i\in I} M_i$. Cuando $N = 0$ escribiremos $\mathrm{Sub}(M)$ en lugar de $\mathrm{Sub}_0(M)$. En general este reticulado no es distributivo, pero siempre es modular. En otras palabras, dados submódulos K, L y Q de M tales que $L \subseteq K$,

$$K \cap (L + Q) = L + K \cap Q.$$

Esto puede probarse argumentando como para el reticulado de ideales de un anillo.

TEOREMA 5.6 (Teorema de la correspondencia). *Si $f\colon M \to M'$ es un morfismo sobreyectivo de A-módulos, entonces las funciones*

$$\begin{array}{ccc} \mathrm{Sub}_{\ker f}(M) & \longrightarrow & \mathrm{Sub}(M') \\ N & \longmapsto & f(N) \end{array} \qquad y \qquad \begin{array}{ccc} \mathrm{Sub}(M') & \longrightarrow & \mathrm{Sub}_{\ker f}(M) \\ N' & \longmapsto & f^{-1}(N') \end{array}$$

son isomorfismos de reticulados, inversos uno del otro. Además $L/N \simeq f(L)/f(N)$ para cada $L, N \in \mathrm{Sub}_{\ker f}(M)$ con $N \subseteq L$.

DEMOSTRACIÓN. Es una consecuencia fácil del Teorema 13.11 del Capítulo 1. Alternativamente, se lo puede probar copiando la demostración de una parte de ese resultado. □

DEFINICIÓN 5.7. *Un A-módulo M es simple si $M \neq 0$ y sus únicos submódulos son los triviales.*

DEFINICIÓN 5.8. *Un submódulo N de un A-módulo M es* maximal *si es propio y no existe ningún submódulo L de M tal que $N \subsetneq L \subsetneq M$.*

COROLARIO 5.9. *Un submódulo N de un A-módulo M es maximal si y sólo si M/N es simple.*

OBSERVACIÓN 5.10. *Un A-módulo no nulo M es simple si y sólo si $M = Am$ para todo $m \in M \setminus \{0\}$. En particular todo A-módulo simple es cíclico y, por lo tanto isomorfo a un cociente de A por un ideal a izquierda que, por el corolario anterior, es maximal.*

PROPOSICIÓN 5.11. *Para cada A-módulo M y cada submódulo N de M vale que:*

1. *Si M es finitamente generado, entonces M/N también lo es.*
2. *Si N y M/N son finitamente generados, entonces M también lo es.*

DEMOSTRACIÓN. El primer item es obvio, ya que las clases de un conjunto de generadores de M forman un conjunto de generadores de M/N. Probemos que vale el segundo. Para ello será suficiente verificar que si $\{n_1, \ldots, n_r\}$ genera N y $m_1, \ldots, m_s$ son elementos de $M \setminus N$, cuyas clases generan M/N, entonces $\{n_1, \ldots, n_r, m_1, \ldots, m_s\}$ genera M. Tomemos $m \in M$ arbitrario y escribamos

$$[m] = a_1 \cdot [m_1] + \cdots + a_s \cdot [m_s] \quad \text{con } a_1, \ldots, a_s \in A.$$

Como $m - a_1 \cdot m_1 - \cdots - a_s \cdot m_s \in N$, existen $b_1, \ldots, b_r \in A$ tales que

$$m - a_1 \cdot m_1 - \cdots - a_s \cdot m_s = b_1 \cdot n_1 + \cdots + b_r \cdot n_r,$$

lo cual termina la prueba. □

PROPOSICIÓN 5.12. *Si N es un submódulo propio de un A-módulo M y M/N es finitamente generado, entonces M tiene un submódulo maximal que incluye a N. En particular, todo A-módulo finitamente generado tiene submódulos maximales.*

DEMOSTRACIÓN. Supongamos que las clases de $m_1, \ldots, m_r \in M$ en M/N generan M/N y consideremos el conjunto $\mathcal{P}$ de los submódulos propios de M que contienen a N. Notemos que $\mathcal{P}$ no es vacío pues $N \in \mathcal{P}$. Por el lema de Zermelo podemos tomar una cadena maximal $(N_i)_{i \in I}$ de elementos de $\mathcal{P}$. Es evidente que ningún submódulo propio N de M puede contener estrictamente a $\bigcup N_i$, ya que en ese caso, agregando N a la cadena $(N_i)_{i \in I}$, obtendríamos una cadena estrictamente más grande que $(N_i)_{i \in I}$, de elementos de $\mathcal{P}$. Por lo tanto el teorema quedará probado si podemos ver que $\bigcup N_i$ es propio. Pero esto es claramente así, pues

si $m_1, \ldots, m_r$ están en esta unión, entonces $m_1, \ldots, m_r \in N_i$ para algún $i \in I$, lo que se contradice con que N_i es propio, pues $N + \langle m_1, \ldots, m_r \rangle = M$. □

EJERCICIO 5.13. *Pruebe que el $\mathbb{Z}$-módulo $\mathbb{Q}$ no tiene submódulos maximales.*

NOTA 5.14. *Por los comentarios hecos al comienzo de la sección 3 sabemos que un morfismo es un monomorfismo si y sólo si es inyectivo y que todo morfismo sobreyectivo es un epimorfismo. Ahora podemos comprobar fácilmente que vale la recíproca de esta afirmación. Supongamos que $f\colon M \to N$ no es sobreyectivo. Debemos ver que entonces no es un epimorfismo. Consideremos la aplicación canónica $\pi\colon N \to N/\operatorname{Im} f$. Como $\pi \circ f = 0$ y $\pi \neq 0$, es evidente que f no es un epimorfismo.*

6. Producto y coproducto directo

Ahora vamos a estudiar dos construcciones, el producto y el coproducto directo de módulos, las cuales son las maneras más simples de obtener nuevos módulos a partir de otros (aunque su importancia se debe más a las propiedades universales que tienen que a este hecho). Comenzamos considerando la suma directa interna, que nos da la forma más sencilla en que un módulo puede recuperase a partir de algunos de sus submódulos. Luego introducimos las nociones de producto directo y de coproducto directo o suma directa externa, y estudiamos algunas de sus propiedades y la relación que hay entre estas construcciones y la suma directa interna.

6.1. Suma directa interna

Consideremos un A-módulo M y una familia $(M_j)_{j\in J}$ de submódulos de M. En general la escritura de un elemento $m \in \sum_{j\in J} M_j$ como una suma con soporte finito

$$m = \sum_{j\in J} m_j, \tag{58}$$

de elementos $m_j \in M_j$, no es única. En particular, 0 puede tener escrituras no triviales (es decir, con algún m_j no nulo). Decimos que $(M_j)_{j\in J}$ *está en suma directa*, o que la suma de los M_j es *directa*, y escribimos $\bigoplus_{j\in J} M_j$ en llugar de $\sum_{j\in J} M_j$, si la escritura (58), de cada elemento $m \in \sum_{j\in J} M_j$, es única. Si $M = \bigoplus_{j\in J} M_j$ decimos también que M es la *suma directa interna* de la familia de sus submódulos $(M_j)_{j\in J}$. En este caso, para cada $i \in J$, las aplicaciones

$$\begin{array}{ccc} M_i & \xrightarrow{\iota_i} & M \\ m & \longmapsto & m \end{array} \qquad \text{y} \qquad \begin{array}{ccc} M & \xrightarrow{\pi_i} & M_i \\ \sum_{j\in J} m_j & \longmapsto & m_i \end{array}$$

son morfismos bien definidos de A-módulos, que satisfacen

$$\pi_i \circ \iota_j = \delta_{ij} \qquad \text{y} \qquad \sum_{j\in J} \iota_j \circ \pi_j = \mathrm{id},$$

donde δ_{ij} es la delta de Kronecker.

TEOREMA 6.1. *Consideremos un A-módulo M y una familia $(M_j)_{j\in J}$ de submódulos de M tal que $M = \sum_{j\in J} M_j$. Por brevedad denotemos con $M_{\widehat{i}}$ a $\sum_{j\in J\setminus\{i\}} M_j$. Son equivalentes:*

1. *M es suma directa interna de $(M_j)_{j\in J}$.*
2. *$\bigcap_{i\in J} M_{\widehat{i}} = 0$.*
3. *$M_i \bigcap M_{\widehat{i}} = 0$ para cada $i \in J$.*
4. *$M_i \bigcap \sum_{j<i} M_j = 0$ para todo orden total de J y cada $i \in J$.*
5. *Existe un orden total de J tal que $M_i \bigcap \sum_{j<i} M_j = 0$ para cada $i \in J$.*
6. *Si $\sum_{j\in J} m_j = 0$, donde $m_j \in M_j$ para cada j y $(m_j)_{j\in J}$ es una familia con soporte finito, entonces $m_j = 0$ para todo j (dicho de otra forma, la única escritura de 0 es la trivial).*

Demostración. 1) $\Rightarrow$ 2) Es trivial.

2) $\Rightarrow$ 3) Porque $M_i \subseteq \bigcap_{j\neq i} M_{\widehat{j}}$.

3) $\Rightarrow$ 4) Esto es claro.

4) $\Rightarrow$ 5) Pues todo conjunto puede ser bien ordenado y, en particular, totalmente ordenado.

5) $\Rightarrow$ 6) Supongamos que 0 tiene una escritura no trivial

$$0 = \sum_{j\in J} m_j$$

Si $i \in J$ es el máximo índice tal que $m_i \neq 0$, entonces $M_i \bigcap \sum_{j<i} M_j \neq 0$, lo que contradice al item 5).

6) $\Rightarrow$ 1) Si $(m_j)_{j\in J}$ y $(n_j)_{j\in J}$ son familias con soporte finito de elementos de M tales que

$$\sum_{j\in J} m_j = \sum_{j\in J} n_j$$

con $m_j, n_j \in M_j$ para todo j, entonces

$$\sum_{j\in J} (n_j - m_j) = 0$$

y, por lo tanto, $m_j = n_j$ para todo j. □

Supongamos que N es un submódulo de un A-módulo M. Decimos que N es un sumando directo de M si existe un submódulo N' de M tal que $M = N \oplus N'$. Usualmente este N' (que es llamado un complemento de N en M) no es único. Sin embargo todos los complementos N' de N en M son isomorfos, pues $N' \simeq M/N$.

Observación 6.2. *Es evidente que una suma finita de submódulos finitamente generados de un A-módulo M, es finitamente generada. Esto se aplica en particular a sumas directas. Recíprocamente, si una suma directa de A-módulos es finitamente generada, entonces tiene soporte finito y, por la Proposición 5.11, cada uno de los sumandos es finitamente generado.*

6.2. Producto directo

El producto cartesiano de una familia de A-módulos $(M_j)_{j\in J}$ es un A-módulo, llamado *producto directo* de la familia $(M_j)_{j\in J}$ y denotado $\prod_{j\in J} M_j$, vía la suma coordenada a coordenada y la *acción diagonal* $a \cdot (m_j)_{j\in J} = (a \cdot m_j)_{j\in J}$. Esta suma y acción están definidas adrede para que las proyecciones canónicas $\pi_j \colon \prod_{i\in I} M_i \to M_j$ sean morfismos de A-módulos. Es claro que el grupo aditivo subyacente al módulo $\prod_{i\in I} M_i$ es el producto directo de los grupos aditivos subyacentes a los M_i's. Procediendo como en la Subsección 15.2 del Capítulo 1,

cuando no haya posibilidad de confusión escribiremos $\prod M_i$ en lugar de $\prod_{i\in I} M_i$, y también haremos muchas otras simplificaciones similares tanto en esta como en la próxima subsección. Además, como es usual, escribiremos $M_1 \times \cdots \times M_n$ en lugar de $\prod_{i\in \mathbb{I}_n} M_i$.

El producto directo tiene la siguiente propiedad universal:

- Para cada familia $(f_i\colon M \to M_i)_{i\in I}$ de morfismos de A-módulos, existe un único morfismo $\mathbf{f}\colon M \to \prod M_i$ tal que para cada $j \in I$ el diagrama

$$\begin{array}{ccc} M & & \\ \downarrow{\scriptstyle \mathbf{f}} & \searrow^{f_j} & \\ \prod M_i & \xrightarrow{\pi_j} & M_j \end{array}$$

  conmuta.

Claramente $\mathbf{f}(m) = (f_i(m))_{i\in I}$ y $\ker \mathbf{f} = \bigcap \ker(f_i)$. Una manera equivalente de establecer la propiedad universal de $\prod M_i$ es diciendo que, para cada A-módulo M, la correspondencia

$$\begin{array}{ccc} \mathrm{Hom}_A(M, \prod M_i) & \xrightarrow{\Psi} & \prod \mathrm{Hom}_A(M, M_i) \\ f & \longmapsto & (\pi_i \circ f)_{i\in I} \end{array}$$

es biyectiva. Es fácil ver que Ψ es un isomorfismo de Z A-módulos.

Observación 6.3. *Consideremos submódulos $M_1, \ldots, M_n$ de un A-módulo M. Como en el Teorema 6.1, escribamos $M_{\widehat{i}} := M_1 + \cdots + \widehat{M_i} + \cdots + M_n$. Por la propiedad universal del producto, las proyecciones canónicas $\pi_{\widehat{i}}\colon M \to M/M_{\widehat{i}}$ inducen un morfismo*

$$M \xrightarrow{\boldsymbol{\pi}} \frac{M}{M_{\widehat{1}}} \times \cdots \times \frac{M}{M_{\widehat{n}}}\ ,$$

cuyo núcleo es $\bigcap_{i=1}^n M_{\widehat{i}}$. Por la Observación 15.4 del Capítulo 1, sabemos que $\boldsymbol{\pi}$ es sobreyectivo si y sólo si $M = M_1 + \cdots + M_n$.

Corolario 6.4. *El morfismo $\boldsymbol{\pi}$ es bijectivo si y sólo si M es suma directa interna de los submódulos $M_1, \ldots, M_n$.*

Demostración. Es consecuencia inmediata del Teorema 6.1 y la Observación 6.3. □

Proposición 6.5. *Para cada familia $(f_i\colon M_i \to N_i)_{i\in I}$ de morfismos de A-módulos, existe un único morfismo*

$$\prod f_i\colon \prod M_i \to \prod N_i$$

tal que los diagramas

$$\begin{array}{ccc} \prod M_i & \xrightarrow{\prod f_i} & \prod N_i \\ \downarrow{\scriptstyle \pi_j} & & \downarrow{\scriptstyle \pi_j} \\ M_j & \xrightarrow{f_j} & N_j \end{array}$$

conmutan.

Demostración. Se sigue de la propiedad universal de $\prod N_i$. □

Es fácil ver que

$$\prod f_i((m_i)_{i\in I}) = (f_i(m_i))_{i\in I}, \quad \ker\Big(\prod f_i\Big) = \prod \ker(f_i) \quad \text{e} \quad \operatorname{Im}\Big(\prod f_i\Big) = \prod \operatorname{Im}(f_i).$$

Observación 6.6. *La correspondencia introducida en la Proposición 6.5 tiene las siguientes propiedades:*

1. $\prod \mathrm{id}_{M_i} = \mathrm{id}_{\prod M_i}$.
2. *Para cada par* $(f_i\colon L_i \to M_i)_{i\in I}$ *y* $(g_i\colon M_i \to N_i)_{i\in I}$, *de morfismos de* A*-módulos,*

$$\Big(\prod g_i\Big) \circ \Big(\prod f_i\Big) = \prod (g_i \circ f_i).$$

Observación 6.7. *Si* N_i *es un submódulo de* M_i *para cada* $i \in I$, *entonces las proyecciones canónicas* $\pi_i\colon M_i \to M_i/N_i$ *inducen un morfismo sobreyectivo*

$$\prod M_i \xrightarrow{\prod \pi_i} \prod \tfrac{M_i}{N_i},$$

cuyo núcleo es $\prod N_i$. *Por consiguiente,*

$$\frac{\prod M_i}{\prod N_i} \simeq \prod \frac{M_i}{N_i}.$$

6.3. Coproducto directo

El *coproducto directo* o *suma directa* de una familia de A-módulos $(M_i)_{i\in I}$, es el submódulo $\bigoplus M_i$ de $\prod M_i$, formado por todos los elementos con soporte finito. Esto es:

$$\bigoplus M_i := \Big\{(m_i)_{i\in I} \in \prod M_i : m_i = 0 \text{ salvo para finitos índices } i \in I\Big\}.$$

Dado un A-módulo M denotamos con $M^{(I)}$ a la suma directa de la familia $(M_i)_{i\in I}$, donde cada M_i es una copia de M.

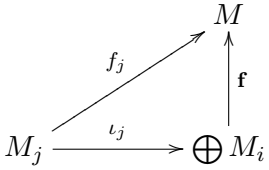
Es obvio que el grupo aditivo subyacente al módulo $\bigoplus M_i$ es el producto directo restringido de los grupos aditivos subyacentes a los M_i's y es fácil comprobar que las inclusiones canónicas $\iota_j\colon M_j \to \bigoplus M_i$ son morfismos de A-módulos. Además, por los resultados de la subsección 15.3 del Capítulo 1, sabemos que

$$\pi_i(\iota_i(m)) = m \quad \text{para todo } i \in I \text{ y } m \in M_i,$$

que

$$\sum_{i\in I} \iota_i(\pi_i(m)) = m \quad \text{para todo } m \in \bigoplus M_i,$$

y que, para cada familia $(f_i\colon M_i \to M)_{i\in I}$, de morfismos de grupos abelianos, existe un único morfismo de grupos abelianos $\mathbf{f}\colon \bigoplus M_i \to M$ tal que para cada $j \in I$ el diagrama



conmuta. Recordemos que $\mathbf{f}(m) = \sum f_j(\pi_j(m))$, donde $\pi_j\colon \bigoplus M_i \to M_j$ es la proyección canónica. Un cálculo directo muestra que si M es un A-módulo y los f_i's son A-lineales,

entonces $\mathbf{f}$ es un morfismo de A-módulos. Esto establece la propiedad universal de la suma directa, la cual puede formularse también diciendo que para cada A-módulo M, la aplicación

$$\Psi\colon \operatorname{Hom}_A\Big(\bigoplus M_i, M\Big) \to \prod \operatorname{Hom}_A(M_i, M),$$

definida por $\Psi(\varphi) := (\varphi \circ \iota_i)_{i\in I}$, es biyectiva. En realidad vale algo más fuerte, que Ψ es un isomorfismo de $\mathrm{Z}\,A$-módulos. Es obvio que

$$\ker \mathbf{f} = \left\{(m_i)_{i\in I} \in \bigoplus M_i : \sum_{i\in I} f_i(m_i) = 0\right\} \quad \text{e} \quad \operatorname{Im}\mathbf{f} = \sum \operatorname{Im} f_i.$$

Observación 6.8. *Como caso particular de lo que vimos arriba obtenemos que, para cada familia $(M_i)_{i\in I}$ de submódulos de un A-módulo M, la función $\varsigma\colon \bigoplus M_i \to M$, definida por $\varsigma((m_i)_{i\in I}) := \sum_{i\in I} m_i$, es un morfismo de A-módulos,*

$$\ker \varsigma = \left\{(m_i)_{i\in I} \in \bigoplus M_i : \sum_{i\in I} m_i = 0\right\} \quad e \quad \operatorname{Im}\varsigma = \sum M_i.$$

Proposición 6.9. *Para cada familia $(M_i)_{i\in I}$, de submódulos de un A-módulo M, son equivalentes:*

1. *$\sum M_i$ es suma directa interna de $(M_i)_{i\in I}$.*
2. *El morfismo $\varsigma\colon \bigoplus M_i \to M$, definido por $\varsigma\big((m_i)_{i\in I}\big) := \sum_{i\in I} m_i$, es inyectivo.*

Demostración. Se lo comprueba inmediatamente. □

Notemos que esto dice que los M_i's están en suma directa interna si y sólo si el morfismo ς es inyectivo.

Proposición 6.10. *Para cada familia $(f_i\colon M_i \to N_i)_{i\in I}$, de morfismos de A-módulos, existe un único morfismo*

$$\bigoplus f_i\colon \bigoplus M_i \to \bigoplus N_i$$

tal que los diagramas

$$\begin{array}{ccc} M_j & \xrightarrow{f_j} & N_j \\ \downarrow{\scriptstyle \iota_j} & & \downarrow{\scriptstyle \iota_j} \\ \bigoplus M_i & \xrightarrow{\bigoplus f_i} & \bigoplus N_i \end{array}$$

conmutan.

Demostración. Se sigue de la propiedad universal de $\bigoplus M_i$. □

Es fácil ver que

$$\Big(\bigoplus f_i\Big)((m_i)_{i\in I}) = (f_i(m_i))_{i\in I}, \quad \ker\Big(\bigoplus f_i\Big) = \bigoplus \ker(f_i) \quad \text{e} \quad \operatorname{Im}\Big(\bigoplus f_i\Big) = \bigoplus \operatorname{Im}(f_i).$$

Observación 6.11. *La correspondencia introducida en la Proposición 6.10 tiene las siguientes propiedades:*

1. *$\bigoplus \mathrm{id}_{M_i} = \mathrm{id}_{\bigoplus M_i}$.*

2. *Para cada par* $(f_i\colon L_i \to M_i)_{i\in I}$ *y* $(g_i\colon M_i \to N_i)_{i\in I}$*, de familias de morfismos de* A*-módulos,*

$$\Big(\bigoplus g_i\Big)\circ\Big(\bigoplus f_i\Big) = \bigoplus (g_i \circ f_i).$$

OBSERVACIÓN 6.12. *Si* N_i *es un submódulo de* M_i *para cada* $i \in I$*, entonces las proyecciones canónicas* $\pi_i\colon M_i \to M_i/N_i$ *inducen un morfismo sobreyectivo*

$$\bigoplus M_i \xrightarrow{\bigoplus \pi_i} \bigoplus \tfrac{M_i}{N_i},$$

cuyo núcleo es $\bigoplus N_i$*. Por consiguiente,*

$$\frac{\bigoplus M_i}{\bigoplus N_i} \simeq \bigoplus \frac{M_i}{N_i}.$$

6.4. Morfismos entre sumas directas finitas de A-módulos

Los resultados que daremos ahora son similares a los establecidos para grupos en la subsección (6.4) del Capítulo 1. En realidad son algo mejores, y esto se debe a que en cada A-módulo la suma es conmutativa.

Para cada par $\mathbf{M} = (M_1, \ldots, M_r)$ y $\mathbf{M'} = (M'_1, \ldots, M'_s)$, de familias finitas de A-módulos, el conjunto $\mathrm{M}_{s\times r}\big(\mathrm{Hom}_A(\mathbf{M}, \mathbf{M'})\big)$ formado por todas las matrices

$$(f_{ij}) = \begin{pmatrix} f_{11} & \cdots & f_{1r} \\ \vdots & \ddots & \vdots \\ f_{s1} & \cdots & f_{sr} \end{pmatrix}$$

con $f_{ij} \in \mathrm{Hom}_A(M_j, M'_i)$, es un grupo abeliano vía la suma coordenada a coordenada. Cuando $\mathbf{M} = \mathbf{M'}$ escribiremos $\mathrm{M}_r\big(\mathrm{End}_A(\mathbf{M})\big)$ en lugar de $\mathrm{M}_{r\times r}\big(\mathrm{Hom}_A(\mathbf{M}, \mathbf{M})\big)$. Notemos que $\mathrm{M}_r\big(\mathrm{End}_A(\mathbf{M})\big)$ es un anillo vía el producto de matrices. De hecho, cuando $M_1 = \cdots = M_r = M$, es el anillo de matrices $\mathrm{M}_r\big(\mathrm{End}_A(M)\big)$.

OBSERVACIÓN 6.13. *La aplicación*

$$\theta\colon \mathrm{M}_{s\times r}\big(\mathrm{Hom}_A(\mathbf{M}, \mathbf{M'})\big) \to \mathrm{Hom}_A\big(M_1 \oplus \cdots \oplus M_r, M'_1 \oplus \cdots \oplus M'_s\big),$$

definida por

$$\theta(f_{ij})(m_1, \ldots, m_r) := \Big(\sum_j f_{1j}(m_j), \ldots, \sum_j f_{sj}(m_j)\Big),$$

es un isomorfismo de grupos abelianos. Su inversa es la función que envía cada morfismo $f\colon M_1 \oplus \cdots \oplus M_r \to M'_1 \oplus \cdots \oplus M'_s$ *en la matriz* $(\pi_i \circ f \circ \iota_j)$*, donde* $\pi_i\colon M'_1 \oplus \cdots \oplus M'_s \to M'_i$ *es la proyección canónica a la* i*-ésima coordenada y* $\iota_j\colon M_j \to M_1 \oplus \cdots \oplus M_r$ *es la inclusión canónica en la* j*-ésima coordenada.*

Si escribimos los elementos de

$$M_1 \oplus \cdots \oplus M_r \quad \text{y} \quad M'_1 \oplus \cdots \oplus M'_s$$

como vectores columna, entonces

$$\theta(f_{ij})(m_1, \ldots, m_r) = \begin{pmatrix} f_{11} & \cdots & f_{1r} \\ \vdots & \ddots & \vdots \\ f_{s1} & \cdots & f_{sr} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}.$$

Supongamos ahora que $\mathbf{M}'' = (M_1'', \dots, M_t'')$ es otra familia de A-módulos. Es fácil ver que para cada $(f_{ij}) \in \mathrm{M}_{s\times r}\big(\mathrm{Hom}(\mathbf{M}, \mathbf{M}')\big)$ y $(g_{kl}) \in \mathrm{M}_{t\times s}\big(\mathrm{Hom}(\mathbf{M}', \mathbf{M}'')\big)$,

$$\theta\big((g_{kl})(f_{ij})\big) = \theta(g_{kl}) \circ \theta(f_{ij}),$$

donde $(g_{kl})(f_{ij})$ es el producto de matrices. En particular

$$\theta\colon \mathrm{M}_r\big(\mathrm{End}_A(\mathbf{M})\big) \to \mathrm{End}_A(M_1 \oplus \cdots \oplus M_r)$$

es un isomorfismo de anillos.

Observación 6.14. *Para cada* $\mathrm{B} := (b_{ij}) \in \mathrm{M}_{s\times r}(A^{\mathrm{op}})$*, denotemos con* $l_{\mathrm{B}}\colon A^r \to A^s$ *al morfismo de* A*-módulos que a cada* r*-upla de elementos de* A *le asigna el resultado de escribirla como vector columna con coeficientes pensados en* A^{op} *y multiplicarla a izquierda por* B*. Esto es:*

$$l_{\mathrm{B}}(a_1, \dots, a_r) = \begin{pmatrix} b_{11} & \dots & b_{1r} \\ \vdots & \ddots & \vdots \\ b_{s1} & \dots & b_{sr} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix}$$

para todo $(a_1, \dots, a_r) \in A^r$*. Usando los resultados de la presente subsección y la Observación 3.2, se comprueba fácilmente que la correspondencia*

$$\begin{array}{ccc} \mathrm{M}_{s\times r}(A^{\mathrm{op}}) & \longrightarrow & \mathrm{Hom}_A(A^r, A^s) \\ \mathrm{B} & \longmapsto & l_{\mathrm{B}} \end{array}$$

es un isomorfismo de grupos abelianos. Más aún, evidentemente $l_{\mathrm{I}_r} = \mathrm{id}_{A^r}$ *y* $l_{\mathrm{CB}} = l_{\mathrm{C}} l_{\mathrm{B}}$ *para cada par de matrices* $\mathrm{B} \in M_{s\times r}(A^{\mathrm{op}})$ *y* $\mathrm{C} \in M_{t\times s}(A^{\mathrm{op}})$*.*

7. Sucesiones exactas cortas

Una sucesión de A-módulos y morfismos

$$\cdots \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} M_4 \longrightarrow \cdots$$

es una *sucesión exacta* si la imagen de cada morfismo es el núcleo del siguiente. Esto es, si la sucesión subyacente de morfismos de grupos abelianos es exacta. Una *sucesión exacta corta* es una sucesión exacta de la forma

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0. \tag{59}$$

Como vimos en la Sección 17 del Capítulo 1, esto pasa si y sólo si f es inyectiva, g es sobreyectiva y $\ker g = \mathrm{Im}\, f$. Decimos que la sucesión exacta corta (59) es equivalente a la sucesión exacta corta

$$0 \longrightarrow M' \xrightarrow{i} N \xrightarrow{p} M'' \longrightarrow 0\ ,$$

si existe un morfismo de A-módulos $h\colon M \to N$ tal que el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_{M'}} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle \mathrm{id}_{M''}} & & \\ 0 & \longrightarrow & M' & \xrightarrow{i} & N & \xrightarrow{p} & M' & \longrightarrow & 0 \end{array}$$

conmuta. Como vimos en la Sección 17 del Capítulo 1, en ese caso h es un isomorfismo. Una consecuencia inmediata de la definición es que la relación de equivalencia de sucesiones exactas cortas es reflexiva y transitiva. Ahora es claro que también es simétrica.

PROPOSICIÓN 7.1. *Para cada sucesión exacta corta de A-módulos*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0 \ ,$$

son equivalentes:

1. *g es una retracción.*
2. *f es una sección.*
3. *Existen morfismos $s\colon M'' \to M$ y $r\colon M \to M'$ tales que $f \circ r + s \circ g = \mathrm{id}_M$.*

Además, si $s\colon M'' \to M$ y $r\colon M \to M'$ satisfacen la propiedad del item 3), entonces la sucesión

$$0 \longrightarrow M'' \xrightarrow{s} M \xrightarrow{r} M' \longrightarrow 0$$

es exacta, s es una sección de g y r una retracción de f. Por último, cada sección s de g puede completarse de manera única a un par (s, r) que satisface las condiciones requeridas en el item 3), y lo mismo vale para cada retracción r de f.

DEMOSTRACIÓN. Asumamos que s y r satisfacen las condiciones requeridas en el item 3). Como g es un epimorfismo, de la igualdad

$$g \circ s \circ g = g \circ (f \circ r + s \circ g) = g = \mathrm{id}_{M''} \circ g,$$

se sigue que s es una sección de g. Así el item 1) se satisface. Una cuenta similar muestra que r es una retracción de f, lo que prueb que también vale 2). Además

$$r \circ s = r \circ (f \circ r + s \circ g) \circ s = r \circ f \circ r \circ s + r \circ s \circ g \circ s = r \circ s + r \circ s,$$

por lo que $\operatorname{Im} s \subseteq \ker r$. En realidad $\operatorname{Im} s = \ker r$ porque

$$m = (f \circ r + s \circ g)(m) = s \circ g(m) \quad \text{para cada } m \in \ker r.$$

A continuación probaremos lo que resta.

1) $\Rightarrow$ 3) Supongamos que s es una sección de g. Como f es un isomorfismo de M' con el núcleo de g y $g \circ (\mathrm{id}_M - s \circ g) = 0$, existe un único morfismo de A-módulos $r\colon M \to M'$ tal que $f \circ r = \mathrm{id}_M - s \circ g$.

2) $\Rightarrow$ 3) Supongamos que r es una retracción de f. Como g induce un isomorfismo de $M/\operatorname{Im} f$ en M'' e $(\mathrm{id}_M - f \circ r) \circ f = 0$, existe un único morfismo de A-módulos $s\colon M'' \to M$ tal que $s \circ g = \mathrm{id}_M - f \circ r$. □

Una sucesión exacta corta es *escindida* si satisface las condiciones equivalentes listadas en la proposición anterior. Por ejemplo, para cada par de A-módulos M' y M'', la sucesión exacta corta

$$0 \longrightarrow M' \xrightarrow{\iota_{M'}} M' \oplus M'' \xrightarrow{\pi_{M''}} M'' \longrightarrow 0 \ , \tag{60}$$

donde $\iota_{M'}$ y $\pi_{M''}$ son la inclusión y proyección canónicas, es escindida. El siguiente resultado muestra que este ejemplo es arquetípico.

PROPOSICIÓN 7.2. *Una sucesión exacta corta de A-módulos*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0 \tag{61}$$

es escindida si y sólo si es equivalente a la sucesión exacta corta (60).

DEMOSTRACIÓN. Basta observar que un morfismo $(r, h)\colon M \to M' \oplus M''$ realiza una equivalencia entre las sucesiones exactas cortas (60) y (61) si y sólo si $h = g$ y r es una retracción de f. □

Capítulo 8

Algunos tipos de módulos

1. Módulos libres

Consideremos un A-módulo M y un subconjunto S de M. Una *combinación lineal* de elementos de S es una suma

$$\sum_{s\in S} a_s \cdot s,$$

donde cada $a_s \in A$ y $(a_s)_{s\in S}$ es una familia con soporte finito. Al escalar a_s se lo llama el *coeficiente* de s en la combinación lineal. Es evidente que el conjunto de las combinaciones lineales de elementos de S coincide con el submódulo de M generado por S. Decimos que S es *linealmente independiente* si

$$\sum_{s\in S} a_s \cdot s = 0 \Rightarrow a_s = 0 \quad \text{para todo } s.$$

Es decir, si la única combinación lineal de elementos de S que da cero es la trivial. En este caso cada elemento de AS se escribe de manera única como combinación lineal de elementos de S, porque

$$\sum_{s\in S} a_s \cdot s = \sum_{s\in S} b_s \cdot s \Rightarrow \sum_{s\in S} (a_s - b_s) \cdot s = 0 \Rightarrow a_s - b_s = 0 \quad \text{para todo } s.$$

Por último, decimos que S es una *base* de M, si es un conjunto linealmente independiente de generadores de M. Un A-módulo M es *libre* si tiene una base. No todo A-módulo es libre. Por ejemplo el $\mathbb{Z}$-módulo $\mathbb{Z}/2\mathbb{Z}$ no lo es. Por otra parte, para cada conjunto I, el A-módulo $A^{(I)}$ es libre. Una base, que siguiendo una tradición firmemente establecida, llamaremos *base canónica* de $A^{(I)}$, es el conjunto $\{e_i : i \in I\}$, donde $e_i \colon I \to A$ es la función que vale 1 en i y 0 en todos los otros puntos de su dominio.

Observación 1.1. *Si M es un A-módulo libre con base S y $f \colon M \to N$ es un isomorfismo de A-módulos, entonces N es libre con base $f(S)$.*

Todo par (M, S), formado por un A-módulo libre M y una base S de M, satisface la siguiente propiedad universal:

- Cada función $f\colon S \to N$ de S en un A-módulo N se extiende de manera única a un morfismo de M en N. En otras palabras, existe un único morfismo de A-módulos $\overline{f}\colon M \to N$, tal que el triángulo

$$\begin{array}{ccc} S & \xrightarrow{f} & N \\ {\scriptstyle \iota}\downarrow & \nearrow_{\overline{f}} & \\ M & & \end{array},$$

  donde $\iota\colon S \to M$ es la inclusión canónica, conmuta.

En efecto, debido a que cada elemento $m \in M$ es una combinación lineal

$$m = \sum_{s \in S} a_s \cdot s, \tag{62}$$

necesariamente $\overline{f}(m) = \sum_{s\in S} a_s \cdot f(s)$. Como la escritura (62) es única, esta definición no es ambigua. Finalmente, es fácil comprobar que la función $\overline{f}$ que acabamos de determinar, es A-lineal.

Proposición 1.2. *Si M es un A-módulo libre con una base S, entonces M es canónicamente isomorfo a $A^{(S)}$.*

Demostración. Por las propiedades universales de (M, S) y $(A^{(S)}, \{e_s : s \in S\})$, existen morfismos únicos de A-módulos

$$f\colon A^{(S)} \to M \qquad \text{y} \qquad g\colon M \to A^{(S)}$$

tales que $f(e_s) = s$ y $g(s) = e_s$ para todo $s \in S$. Como los triángulos

$$\begin{array}{ccc} S & \xrightarrow{\iota} & M \\ {\scriptstyle \iota}\downarrow & \nearrow_{f\circ g} & \\ M & & \end{array} \qquad \text{y} \qquad \begin{array}{ccc} S & \xrightarrow{\iota} & M \\ {\scriptstyle \iota}\downarrow & \nearrow_{\mathrm{id}} & \\ M & & \end{array}$$

conmutan, se sigue de la unicidad en la propiedad universal de (M, S) que $f \circ g = \mathrm{id}_M$. Similarmente, $g \circ f = \mathrm{id}_{A^{(S)}}$. □

Nota 1.3. *La palabra canónicamente en el enunciado de la proposición anterior hace referencia al hecho de que el isomorfismo $f\colon A^{(S)} \to M$ es el único que extiende a la biyección $e_s \mapsto s$, de la base canónica de $A^{(S)}$ en S.*

Teorema 1.4. *Supongamos que A es un anillo no nulo. Son equivalentes:*

1. *Todos los A-módulos son libres.*
2. *A tiene un A-módulo simple libre.*
3. *A es un anillo de división.*

Demostración. 1) ⇒ 2) Es suficiente verificar que hay un A-módulo simple. Para ello basta notar que por la Proposición 5.12 del Capítulo 7 el anillo A tiene un ideal a izquierda maximal I y, que por la Proposición 5.9 del mismo capítulo, A/I es simple.

2) ⇒ 3) Tomemos un A-módulo simple M con una base B. Como M no es nulo, B tiene un elemento $m \neq 0$. Como M es simple y m es linealmente independiente, la función

$$\begin{array}{ccc} A & \xrightarrow{\rho(a)} & M \\ a & \longmapsto & a \cdot m \end{array}$$

es un isomorfismo. Por lo tanto, A es un A-módulo simple y así, debido a la Proposición 3.4 del Capítulo 5, un anillo de división.

3) ⇒ 1) Consideremos un A-módulo M. Si $M = 0$, entonces M es libre con base $\emptyset$. Supongamos que $M \neq 0$. Por el Lema de Zorn, M tiene un conjunto linealmente independiente maximal S. Si $m \in M \setminus S$, entonces $S \cup \{m\}$ es linealmente dependiente y, por lo tanto, hay una combinación lineal no trivial

$$\lambda_m \cdot m + \sum_{s \in S} \lambda_s \cdot s = 0.$$

Por la independencia lineal de S, necesariamente $\lambda_m \neq 0$. Despejando obtenemos que

$$m = -\sum_{s \in S} \lambda_m^{-1} \lambda_s \cdot s,$$

lo cual prueba que $\langle S \rangle \supseteq (M \setminus S) \cup S = M$ y muestra que S es una base de M. □

Observación 1.5. *Todo A-módulo M es isomorfo a un cociente de un módulo libre. Más precisamente, si S es un conjunto de generadores de M, entonces la función $\pi\colon A^{(S)} \to M$, definida por $\pi(e_s) := s$, para todo $s \in S$, es un epimorfismo. Por lo tanto $M \simeq A^{(S)}/\ker \pi$.*

Ampliando un poco la definición dada arriba, diremos que un *A-módulo libre sobre un conjunto X* es cualquier par (M, j), formado por un A-módulo M y una función $j\colon X \to M$, que tiene la siguiente propiedad universal:

- Para cada función $f\colon X \to N$, de X en un A-módulo N, existe un único morfismo de A-módulos $\overline{f}\colon M \to N$, tal que el triángulo

$$\begin{array}{ccc} X & \xrightarrow{f} & N \\ {\scriptstyle j}\downarrow & \nearrow_{\overline{f}} & \\ M & & \end{array} \quad ,$$

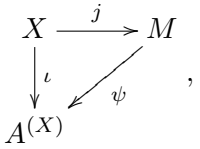
  conmuta.

Observación 1.6. *Si (M, j) es un A-módulo libre sobre X, $l\colon Y \to X$ es una función biyectiva y $\varphi\colon M \to N$ es un isomorfismo de A-módulos, entonces $(N, \varphi \circ j \circ l)$ es un A-módulo libre sobre Y.*

Proposición 1.7. *Un par (M,j), formado por un A-módulo M y una función $j\colon X \to M$, es un A-módulo libre sobre X si y sólo si la aplicación A-lineal $\varphi\colon A^{(X)} \to M$, definida por $\varphi(e_x) := j(x)$, es un isomorfismo. En consecuencia, j es inyectiva y $j(X)$ es una base de M.*

Demostración. Por la observación anterior si φ es un isomorfismo, entonces (M, j) es un A-módulo libre. Recíprocamente, si (M, j) es un A-módulo libre, entonces hay un único

morfismo $\psi\colon M \to A^{(X)}$ tal que el triángulo



donde ι es la función que manda x en e_x, conmuta. Como $\psi\circ\varphi\circ\iota = \iota$ y $\varphi\circ\psi\circ j = j$, debido a las propiedades universales de $(A^{(X)}, \iota)$ y (M, j), debe ser $\psi\circ\varphi = \mathrm{id}_{A^{(X)}}$ y $\varphi\circ\psi = \mathrm{id}_M$. □

Proposición 1.8. *Si un módulo libre M es finitamente generado, entonces todas sus bases son finitas; y si no lo es, entonces todas tienen el mismo cardinal.*

Demostración. Puesto que las bases son conjuntos minimales de generadores, esto es una consecuencia inmediata de la Proposición 2.2 del capítulo 7. □

Decimos que un anillo A satisface la propiedad de *invariancia del cardinal de las bases*, o, por brevedad, que tiene o satisface la ICB, si en cada A-módulo libre todas las bases tienen el mismo cardinal. Como un módulo libre finitamente generado es isomorfo a uno de la forma A^n y, por la proposición anterior, todas las bases de un módulo libre no finitamente generado, son coordinables, A tiene la ICB si y sólo si $A^n \simeq A^m \Leftrightarrow n = m$. Finalmente, puesto que tener un isomorfismo $A^n \simeq A^m$ es lo mismo que tener matrices $\mathrm{A} \in \mathrm{M}_{m\times n}(A)$ y $\mathrm{B} \in \mathrm{M}_{n\times m}(A)$ tales que $\mathrm{AB} = \mathrm{I}_m$ y $\mathrm{BA} = \mathrm{I}_n$, donde $\mathrm{I}_m \in \mathrm{M}_m(A)$ e $\mathrm{I}_n \in \mathrm{M}_n(A)$ son las matrices identidad, es inmediato que A tiene la ICB si y sólo si la existencia de tales matrices es imposible cuando $m \neq n$.

Ejemplo 1.9. *Para cada anillo no nulo A, el anillo $B := \mathrm{End}_A(A^{(\mathbb{N})})$ no tiene la ICB. Para verificarlo basta observar que la aplicación $\psi = (\psi_1, \psi_2)$ de B en $B \oplus B$, definida por*

$$\psi_1(f)(e_i) := f(e_{2i-1}) \qquad y \qquad \psi_2(f)(e_i) := f(e_{2i}),$$

donde $\{e_n : n \in \mathbb{N}\}$ es la base canónica de $A^{(\mathbb{N})}$, es un isomorfismo de B-módulos.

Proposición 1.10. *Se satisfacen las siguientes propiedades:*

1. *Un anillo A tiene la ICB si y sólo si A^{op} la tiene.*
2. *Si A tiene la ICB, entonces $\mathrm{M}_r(A)$ tiene la ICB para todo $r \in \mathbb{N}$.*
3. *Si $f\colon A \to B$ es un morfismo de anillos, y B tiene la ICB, entonces A también la tiene.*

Demostración. La primera afirmación se sigue fácilmente de que la transpuesta de un producto AB de matrices con coeficientes en A es el producto como matrices con coeficientes en A^{op} de la transpuesta de B con la transpuesta de A. La segunda vale porque cada matriz en $\mathrm{M}_{m\times n}(\mathrm{M}_r(A))$ puede verse de manera evidente como una matriz en $\mathrm{M}_{mr\times nr}(A)$ y porque esta correspondencia respeta productos e identidades. Para probar que vale la tercera es suficiente mostrar que si dos matrices $\mathrm{A} \in \mathrm{M}_{m\times n}(A)$ y $\mathrm{B} \in \mathrm{M}_{n\times m}(A)$ satisfacen $\mathrm{AB} = \mathrm{I}_m$ y $\mathrm{BA} = \mathrm{I}_n$, entonces $m = n$. Para ello basta observar que aplicando f en cada coordenada de A y de B se obtienen matrices $\mathrm{A}' \in \mathrm{M}_{m\times n}(B)$ y $\mathrm{B}' \in \mathrm{M}_{n\times m}(B)$ tales que $\mathrm{A}'\mathrm{B}' = \mathrm{I}_m$ y $\mathrm{B}'\mathrm{A}' = \mathrm{I}_n$, y que (como por hipótesis B tiene la ICB) esto implica que $m = n$. □

Un A-módulo a izquierda M es *hopfiano* si todo endomorfismo sobreyectivo $f\colon M \to M$ es un isomorfismo.

PROPOSICIÓN 1.11. *Si todo A-módulo libre finitamente generado es hopfiano, entonces A satisface la ICB.*

DEMOSTRACIÓN. Supongamos que existe un isomorfismo $f\colon A^m \to A^n$, con $m, n \in \mathbb{N}$, y $m < n$. Entonces la función

$$\begin{array}{c} A^n \xrightarrow{\quad g \quad} A^n \\ (x_1, \ldots, x_n) \longmapsto f(x_1, \ldots, x_m) \end{array},$$

es un endomorfismo sobreyectivo que no es inyectivo. □

Más adelante, cuando estudiemos las condiciones de cadena, veremos que hay muchos anillos para los que todo módulo finitamente generado es hopfiano.

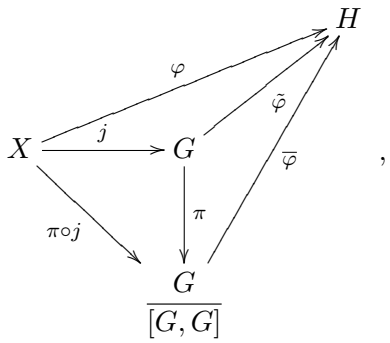
TEOREMA 1.12. *Todos los anillos conmutativos satisfacen la ICB.*

DEMOSTRACIÓN. Por el Corolario 6.6 del Capítulo 5, hay un morfismo de A en un cuerpo. Así el teorema se sigue del item 3) de la Proposición 1.10 y de que todos los anillos de división satisfacen la ICB. □

Ahora estamos en posición de probar el Teorema 14.5 del Capítulo 1. Para ello será conveniente establecer primero un resultado auxiliar, que es importante en si mismo.

PROPOSICIÓN 1.13. *Si (G, j) es un grupo libre, entonces el par $(G/[G,G], \pi \circ j)$, donde $\pi\colon G \to G/[G,G]$ es la proyección canónica, es un $\mathbb{Z}$-módulo libre.*

DEMOSTRACIÓN. Denotemos con X al dominio de j y tomemos una función $\varphi\colon X \to H$, de X en un grupo abeliano H. Por las propiedades universales de (G, j) y del abelianizado de G, existen morfismos únicos $\tilde{\varphi}\colon G \to H$ y $\overline{\varphi}\colon G/[G,G] \to H$ tales que el diagrama



conmuta. En particular, $\overline{\varphi} \circ \pi \circ j = \varphi$. Además $\overline{\varphi}$ es el único morfismo con esta propiedad, porque si $\widehat{\varphi}\colon G/[G,G] \to H$ también satisface $\widehat{\varphi} \circ \pi \circ j = \varphi$, entonces, por la propiedad universal de (G, j), forzosamente $\widehat{\varphi} \circ \pi = \overline{\varphi} \circ \pi$ y, por lo tanto, dado que π es sobreyectivo, $\widehat{\varphi} = \overline{\varphi}$. □

DEMOSTRACIÓN DEL TEOREMA 14.5 DEL CAPÍTULO 1. Supongamos que (G, j) y (H, l) son grupos libres sobre X e Y respectivamente. Por los comentarios hechos al comienzo de la subsección 18.4 del Capítulo 1, sabemos que si G y H son isomorfos, entonces $G/[G,G]$ y $H/[H,H]$ también lo son. Debido la Proposición 1.13 y al Teorema 1.12, esto implica que $|X| = |Y|$. Recíprocamente, por la propiedad universal de (G, j), dada una biyección

$\varphi\colon X \to Y$, existen morfismos únicos $\overline{\varphi}\colon G \to H$ y $\overline{\varphi^{-1}}\colon H \to G$ tales que los diagramas

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & Y \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle l} \\ G & \xrightarrow{\overline{\varphi}} & H \end{array} \qquad \text{y} \qquad \begin{array}{ccc} Y & \xrightarrow{\varphi^{-1}} & X \\ \downarrow{\scriptstyle l} & & \downarrow{\scriptstyle j} \\ H & \xrightarrow{\overline{\varphi^{-1}}} & G \end{array}$$

conmutan. Como

$$\overline{\varphi^{-1}} \circ \overline{\varphi} \circ j = j \circ \varphi^{-1} \circ \varphi = j,$$

debe ser $\overline{\varphi^{-1}} \circ \overline{\varphi} = \mathrm{id}_G$. Un argumento similar muestra que $\overline{\varphi} \circ \overline{\varphi^{-1}} = \mathrm{id}_H$. □

2. Módulos de torsión

En esta sección asumimos que A es un dominio conmutativo.

Un elemento m de un A-módulo M es *de torsión* si existe $a \in A \setminus \{0\}$ tal que $a \cdot m = 0$. Por ejemplo $([1], 0)$ es un elemento de torsión del $\mathbb{Z}$-módulo $\mathbb{Z}_3 \oplus \mathbb{Z}$, mientras que $(0, 1)$ no lo es. La *torsión* de M es el conjunto

$$\mathrm{T}(M) := \{m \in M : m \text{ es de torsión}\}.$$

Un A-módulo M es *de torsión* si $\mathrm{T}(M) = M$ y es *sin torsión* si $\mathrm{T}(M) = 0$.

Ejemplo 2.1. *Cada A-módulo libre es sin torsión.*

Ejemplo 2.2. *El $\mathbb{Z}$-módulo $\mathbb{Q}$ no tiene torsión pero no es libre.*

Proposición 2.3. *Para cada A-módulo M, el conjunto $\mathrm{T}(M)$ es un submódulo de M.*

Demostración. Basta observar que para todo $b \in A$ y $m, m' \in M$, si $a \cdot m = a' \cdot m' = 0$ con $a, a' \in A \setminus \{0\}$, entonces

$$aa' \cdot (m + m') = aa' \cdot m + aa' \cdot m' = a'a \cdot m + aa' \cdot m' = 0 \quad \text{y} \quad a \cdot (b \cdot m) = b \cdot (a \cdot m) = 0$$

porque A es conmutativo, y que $aa' \neq 0$ porque A es un dominio. □

Proposición 2.4. *Para cada A-módulo M, el submódulo $T(M)$ es de torsión y el módulo cociente $M/T(M)$ es sin torsión.*

Demostración. Es evidente que la primera afirmación es verdadera. Veamos que también lo es la segunda. Tomemos $m \in M$. Si $[m] \in T(M/T(M))$, entonces $a \cdot m \in T(M)$ para algún $a \in A \setminus \{0\}$ y, por lo tanto, existe $b \in A \setminus \{0\}$ tal que $ba \cdot m = b \cdot (a \cdot m) = 0$. Como $ba \neq 0$, esto implica que $m \in T(M)$. □

Proposición 2.5. *Para cada morfismo de A-módulos $f\colon M \to N$,*

$$f(T(M)) \subseteq T(N).$$

Además si f es inyectivo, entonces $f(T(M)) = f(M) \cap T(N)$.

Demostración. Tomemos $a \in A \setminus \{0\}$ y $m \in M$. La inclusión se sigue inmediatamente de que si $a \cdot m = 0$, entonces $a \cdot f(m) = f(a \cdot m) = 0$. Supongamos ahora que f es inyectiva y que $a \cdot f(m) = 0$. Entonces $f(a \cdot m) = a \cdot f(m) = 0$ y así $a \cdot m = 0$. esto muestra que en este caso $f(T(M)) = f(M) \cap T(N)$. □

Observación 2.6. *Por la proposición anterior cada morfismo de A-módulos $f\colon M \to N$ induce por restricción y por paso al cociente, morfismos*

$$f_{\mathrm{T}}\colon \mathrm{T}(M) \to \mathrm{T}(N) \qquad y \qquad \overline{f}_{\mathrm{T}}\colon \frac{M}{\mathrm{T}(M)} \to \frac{N}{\mathrm{T}(N)}.$$

Se comprueba fácilemente que

$$(\mathrm{id}_M)_{\mathrm{T}} = \mathrm{id}_{\mathrm{T}(M)} \qquad y \qquad (\overline{\mathrm{id}_M})_{\mathrm{T}} = \mathrm{id}_{M/\mathrm{T}(M)}$$

para cada A-módulo M, y que

$$(g \circ f)_{\mathrm{T}} = g_{\mathrm{T}} \circ f_{\mathrm{T}} \qquad y \qquad \overline{(g \circ f)}_{\mathrm{T}} = \overline{g}_{\mathrm{T}} \circ \overline{f}_{\mathrm{T}},$$

para cada par de morfismos de A-módulos $f\colon M \to N$ y $g\colon N \to L$.

Teorema 2.7. *Si N es un A-módulo finitamente generado y sin torsión, entonces existe un A-módulo libre finitamente generado y un monomorfismo $\iota\colon N \to M$.*

Demostración. Fijemos un conjunto finito $S = \{n_1, \ldots, n_s\}$ de generadores de N, tomemos un subconjunto linealmente independiente maximal $T = \{n_{i_1}, \ldots, n_{i_d}\}$ de S y denotemos con M a $\langle T\rangle$. Por la definición de T, para cada $n_j \in S \setminus T$ existe $\lambda_j \in A \neq 0$, tal que $\lambda_j \cdot n_j \in M$. Escribamos $\lambda := \prod \lambda_j$. Notemos que, como A es un dominio conmutativo, $\lambda \neq 0$ y $\lambda \cdot n \in M$ para todo $n \in N$. Así podemos considerar la aplicación

$$\begin{array}{ccc} N & \xrightarrow{\ \iota\ } & M \\ n & \longmapsto & \lambda \cdot n \end{array}.$$

Dado que A es conmutativo y N es sin torsión, ι es un morfismo inyectivo de A-módulos. Como M es libre con base B, esto termina la prueba. □

3. Módulos divisibles

En esta sección asumimos que A es un dominio.

Definición 3.1. *Decimos que un A-módulo M es* divisible *si para cada $m \in M$ y cada $a \in A \setminus \{0\}$, existe $m' \in M$ tal que $a \cdot m' = m$.*

Ejemplo 3.2. *Los $\mathbb{Z}$-módulos $\mathbb{Q}$ y $\mathbb{Q}/\mathbb{Z}$ son divisibles. En cambio $\mathbb{Z}$ no lo es. Notemos que en el primer caso el m' garantizado por la definición de divisibilidad es único, pero en el segundo, no.*

Proposición 3.3. *Los módulos divisibles tienen las siguientes propiedades:*

1. *El producto directo de una familia de módulos divisibles es divisible.*
2. *La suma directa de una familia de módulos divisibles es divisible.*
3. *Todo sumando directo de un módulo divisible es divisible.*

Demostración. Dejada al lector. □

Proposición 3.4. *Si un A-módulo M es divisible, entonces también lo es cada uno de sus cocientes M/N.*

Demostración. Porque $a \cdot m' = m \Rightarrow a \cdot [m'] = [m]$. □

Lema 3.5. *Si M es un A-módulo divisible y sin torsión, entonces para cada $m \in M$ y cada $a \in A \setminus \{0\}$ existe un único $m' \in M$ tal que $a \cdot m' = m$.*

Demostración. Como M es divisible, existe m' tal que $a \cdot m' = m$. Si también $a \cdot m'' = m$, entonces

$$a \cdot (m' - m'') = 0,$$

por lo que $m' = m''$, debido a que M es sin torsión. □

Teorema 3.6. *Supongamos que A es un dominio conmutativo. Si M es un A-módulo divisible y sin torsión, entonces tiene una única estructura de $\mathbb{Q}_A$-espacio vectorial (donde $\mathbb{Q}_A$ es el cuerpo de cocientes de A) que extiende a su estructura de A-módulo.*

Demostración. Si tal estructura existe, entonces para cada $\frac{p}{q} \in \mathbb{Q}_A$ y $m \in M$,

$$q \cdot \left(\frac{p}{q} \cdot m\right) = \frac{q}{1}\frac{p}{q} \cdot m = p \cdot m.$$

Pero por el lema anterior sabemos que existe un único $m' \in M$ tal que $q \cdot m' = p \cdot m$. Esto prueba la unicidad y obliga a definir

$$\frac{p}{q} \cdot m := m'. \tag{63}$$

Para ver que esta definición es buena, basta observar que si $\frac{p}{q} = \frac{r}{s}$ y $s \cdot m'' = r \cdot m$, entonces $m' = m''$. Pero esto es así pues M no tiene torsión, $qs \neq 0$ y

$$qs \cdot m'' = qr \cdot m = sp \cdot m = qs \cdot m'.$$

Notemos que

$$q \cdot \left(\frac{p}{q} \cdot m\right) = q \cdot m' = p \cdot m \quad \text{para todo } \frac{p}{q} \in \mathbb{Q}_A \text{ y } m \in M.$$

Para concluir la demostración debemos probar que M es un $\mathbb{Q}_A$-módulo via (63). Es claro que $1 \cdot m = m$ para todo $m \in M$. Afirmamos que

$$\frac{p}{q} \cdot (m + n) = \frac{p}{q} \cdot m + \frac{p}{q} \cdot n$$

para todo $\frac{p}{q} \in \mathbb{Q}_A$ y $m, n \in M$. En efecto, esto se sigue inmediatamente de que M es sin torsión y

$$q \cdot \left(\frac{p}{q} \cdot (m+n)\right) = p \cdot (m+n) = p \cdot m + p \cdot n = q \cdot \left(\frac{p}{q} \cdot m\right) + q \cdot \left(\frac{p}{q} \cdot n\right) = q \cdot \left(\frac{p}{q} \cdot m + \frac{p}{q} \cdot n\right).$$

Argumentos similares muestran que M también satisface los otros axiomas de $\mathbb{Q}_A$-espacio vectorial. □

Proposición 3.7. *Supongamos que A es un dominio conmutativo. Para todo A-módulo N existen un A-módulo divisible M y un monomorfismo $\iota\colon N \to M$. Si N no tiene torsión, entonces se puede tomar M sin torsión.*

Demostración. Tomemos un conjunto I de generadores de N arbitrario. Es claro que podemos suponer sin pérdida de generalidad que $N = A^{(I)}/S$ para un submódulo S de $A^{(I)}$. Pero por la Proposición 3.4 sabemos que $M = \mathbb{Q}_A^{(I)}/S$ es divisible, y es evidente que la inclusión canónica de $A^{(I)}$ en $\mathbb{Q}_A^{(I)}$ induce un monomorfismo ι de N en M. Además, debido a la Proposición 2.5,

$$\iota(N) \cap \mathrm{T}(M) = \iota(T(N)).$$

En consecuencia si $\mathrm{T}(N) = 0$, entonces $\iota(N) \cap T(M) = 0$ y, así, la composición

$$N \xrightarrow{\iota} M \xrightarrow{\pi} \frac{M}{T(M)},$$

donde π es la proyección canónica, es inyectiva. Por lo tanto, en este caso podemos reemplazar M por el módulo sin torsión $M/\mathrm{T}(M)$. □

Notemos que si N es sin torsión, entonces la dimensión del $\mathbb{Q}_A$-espacio vectorial M, construído en la demostración, es menor o igual al cardinal del conjunto de generadores de N elegido.

4. Módulos proyectivos y módulos inyectivos

En la Subsección 3.1 vimos que los conjuntos $\mathrm{Hom}_A(M, N)$ tienen estructuras naturales de grupos abelianos tales que dados morfismos de A-módulos $v\colon N \to N'$ y $u\colon M' \to N$, las funciones

$$v_*\colon \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N') \quad \text{y} \quad u^*\colon \mathrm{Hom}_A(M', N) \to \mathrm{Hom}_A(M, N),$$

definidas por $v_*(f) = v \circ f$ y $u^*(f) = f \circ u$, son morfismos de grupos. En esta sección estudiamos el comportamiento de estas funciones respecto de la exactitud.

Teorema 4.1. *Una sucesión*

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'',$$

de morfismos de A-módulos, es exacta si y sólo si la sucesión inducida

$$0 \longrightarrow \mathrm{Hom}_A(M, N') \xrightarrow{f_*} \mathrm{Hom}_A(M, N) \xrightarrow{g_*} \mathrm{Hom}_A(M, N'')$$

lo es, para cada módulo M.

Demostración. Por definición, f es un monomorfismo si y sólo si f_* es inyectivo para todo M. Además es claro que

$$g \circ f = 0 \Rightarrow g_* \circ f_* = 0$$

para tódo A-módulo M. Recíprocamente, si $g_* \circ f_* = 0$ para $M := N'$, entonces

$$g \circ f = (g_* \circ f_*)(\mathrm{id}_{N'}) = 0.$$

Supongamos ahora que f es un monomorfismo e $\mathrm{Im}\, f = \ker g$, y tomemos $v\colon M \to N$ tal que $g_*(v) = 0$, debido a la propiedad universal de la inclusión canónica $\iota\colon \ker g \to N$ y a que f define un isomorfismo de N' en $\ker g$, existe un único morfismo $v'\colon M \to N'$ tal que

$$f_*(v') = f \circ v' = v.$$

Así, en este caso, $\ker(g_*) = \mathrm{Im}(f_*)$ para todo A-módulo M. Para terminar la demostración será suficiente ver que si para $M := \ker g$ vale la igualdad $\ker(g_*) = \mathrm{Im}(f_*)$, entonces $\ker g \subseteq \mathrm{Im}\, f$. Pero dado que para la inclusión canónica $\iota\colon \ker g \to N$ vale la igualdad $g_*(\iota) = 0$, se sigue de la hipótesis que existe $\iota'\colon \ker g \to N'$ tal que $f \circ \iota' = f_*(\iota') = \iota$ y, así, $\ker g = \mathrm{Im}\, \iota \subseteq \mathrm{Im}\, f$. □

TEOREMA 4.2. *Una sucesión*

$$N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$

de morfismos de A-módulos, es exacta si y sólo si la sucesión inducida

$$0 \longrightarrow \mathrm{Hom}_A(N'', M) \xrightarrow{g^*} \mathrm{Hom}_A(N, M) \xrightarrow{f^*} \mathrm{Hom}_A(N', M)$$

lo es, para cada módulo M.

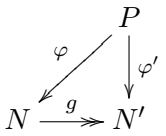
DEMOSTRACIÓN. Dejada al lector. □

PROPOSICIÓN 4.3. *Consideremos morfismos de A-módulos $f\colon N' \to N$ y $g\colon N \to N''$. Son equivalentes:*

1. *La sucesión*
$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$
es escindida.
2. *Para cada módulo M, la sucesión inducida*
$$0 \longrightarrow \mathrm{Hom}_A(M, N') \xrightarrow{f_*} \mathrm{Hom}_A(M, N) \xrightarrow{g_*} \mathrm{Hom}_A(M, N'') \longrightarrow 0$$
es exacta.
3. *Para cada módulo M, la sucesión inducida*
$$0 \longrightarrow \mathrm{Hom}_A(N'', M) \xrightarrow{g^*} \mathrm{Hom}_A(N, M) \xrightarrow{f^*} \mathrm{Hom}_A(N', M) \longrightarrow 0$$
es exacta.

DEMOSTRACIÓN. Si s es una sección de g, entonces claramente s_* es una sección de g_*, cualquiera sea M. En particular g_* es sobreyectiva. Recíprocamente, si g_* es sobreyectiva para $M := N''$, entonces existe $s\colon N'' \to N$ tal que $g \circ s = g_*(s) = \mathrm{id}_{N''}$. Por el Teorema 4.1, esto prueba que 1) $\Leftrightarrow$ 2). La demostración de la equivalencia entre 1) y 3) es similar. □

Decimos que un A-módulo P es *proyectivo* si para cada morfismo $\varphi'\colon P \to N'$ y cada morfismo sobreyectivo $g\colon N \twoheadrightarrow N'$, existe un morfismo $\varphi\colon P \to N$ tal que el diagrama



conmuta.

PROPOSICIÓN 4.4. *La suma de una familia de módulos proyectivos es un módulo proyectivo y todo sumando directo de un módulo proyectivo es proyectivo.*

DEMOSTRACIÓN. Supongamos que $(P_i)_{i\in I}$ es una familia de módulos proyectivos, que $g\colon N \twoheadrightarrow N'$ es un morfismo sobreyectivo y que

$$\varphi'\colon \bigoplus_{i\in I} P_i \to N'$$

es un morfismo. Como los P_j's son módulos proyectivos, existen morfismos $\varphi_j\colon P_j \to N$ tales que $g \circ \varphi_j = \varphi' \circ \iota_j$, donde ι_j es la inclusión canónica de P_j en $\bigoplus_{i\in I} P_i$. Por la propiedad universal de la suma directa hay un único morfismo

$$\varphi\colon \bigoplus_{i\in I} P_i \to N$$

tal que $\varphi\circ\iota_j = \varphi_j$ para todo $j \in J$. Para concluir que la primera afirmación es verdadera resta probar que $g \circ \varphi = \varphi'$, pero esto es consecuencia inmediata de que $g \circ \varphi \circ \iota_j = g \circ \varphi_j = \varphi' \circ \iota_j$ para todo $j \in I$.

Consideremos ahora la segunda afirmación. Supongamos que $g\colon N \twoheadrightarrow N'$ es un epimorfismo, que $\varphi'\colon P \to N'$ es un morfismo y que existe un módulo Q tal que $P \oplus Q$ es proyectivo. Entonces hay un morfismo $\varphi\colon P \oplus Q \to N$ tal que $g \circ \varphi = \varphi' \circ \pi_P$, donde $\pi_P\colon P \oplus Q \to P$ es la proyección canónica. Componiendo con la inclusión canónica $\iota_P\colon P \to P \oplus Q$ obtenemos la igualdad

$$g \circ \varphi \circ \iota_P = \varphi' \circ \pi_P \circ \iota_P = \varphi',$$

la cual muestra que P es proyectivo. □

En la siguiente proposición damos varias caracterizaciones de los módulos proyectivos

Proposición 4.5. *Para cada A-módulo P son equivalentes:*

1. *P es proyectivo.*
2. *Si $g\colon N \to N'$ es un epimorfismo, entonces $g_*\colon \mathrm{Hom}_A(P, N) \to \mathrm{Hom}_A(P, N')$ es un epimorfismo.*
3. *Si*

   $$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$

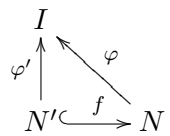
   es una sucesión exacta, entonces

   $$0 \longrightarrow \mathrm{Hom}_A(P, N') \xrightarrow{f_*} \mathrm{Hom}_A(P, N) \xrightarrow{g_*} \mathrm{Hom}_A(P, N'') \longrightarrow 0$$

   también lo es.
4. *Todo epimorfismo $g\colon N \to P$ es una retracción.*
5. *P es isomorfo a un sumando directo de un módulo libre.*

Demostración. Es claro que 1) $\Leftrightarrow$ 2). Además, por el Teorema 4.1, los items 2) y 3) también son equivalentes. El cuarto item se sigue del primero tomando $\varphi' = \mathrm{id}_P$ en la definición de módulo proyectivo. Como todo módulo es cociente de un módulo libre, 4) $\Rightarrow$ 5). Finalmente, debido a la proposición anterior, para probar que 5) $\Rightarrow$ 1) es suficiente ver que A es proyectivo, lo cual es evidente. □

Un A-módulo I es *inyectivo* si para cada morfismo $\varphi'\colon N' \to I$ y cada morfismo inyectivo $f\colon N' \hookrightarrow N$, existe un morfismo $\varphi\colon N \to I$ tal que el diagrama



conmuta.

PROPOSICIÓN 4.6. *El producto de una familia de módulos inyectivos es un módulo inyectivo y todo sumando directo de un módulo inyectivo es inyectivo.*

DEMOSTRACIÓN. Dejada al lector. □

PROPOSICIÓN 4.7. *Para cada A-módulo I son equivalentes:*

1. *I es inyectivo.*
2. *Si $f\colon N' \to N$ es un monomorfismo, entonces $f^*\colon \mathrm{Hom}_A(N, I) \to \mathrm{Hom}_A(N', I)$ es sobreyectiva.*
3. *Si*
$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$
es una sucesión exacta, entonces
$$0 \longrightarrow \mathrm{Hom}_A(N'', I) \xrightarrow{g^*} \mathrm{Hom}_A(N, I) \xrightarrow{f^*} \mathrm{Hom}_A(N', I) \longrightarrow 0$$
también lo es.
4. *Todo monomorfismo $f\colon I \to N$ es una sección.*

DEMOSTRACIÓN. Es claro que 1) $\Leftrightarrow$ 2). Además, por el Teorema 4.2, los items 2) y 3) también son equivalentes. El cuarto item se sigue del primero tomando $\varphi' = \mathrm{id}_I$ en la definición de módulo inyectivo. Solamente resta probar que 4) $\Rightarrow$ 1). Para ello, dados un morfismo $\varphi'\colon N' \to I$ y un morfismo inyectivo $f\colon N' \hookrightarrow N$, consideremos el diagrama conmutativo

$$\begin{array}{ccc} I & \xrightarrow{\iota_I} & I \oplus_{\varphi', f} N \\ {\scriptstyle\varphi'}\uparrow & & \uparrow{\scriptstyle\iota_N} \\ N' & \xhookrightarrow{f} & N \end{array}$$

donde $I \oplus_{\varphi', f} N$ es el cociente de $I \oplus N$ por el submódulo $J := \{(\varphi'(n), -f(n)) : n \in N'\}$ e ι_I, ι_N son los morfismos inducidos por las inclusiones canónicas a la suma directa. Afirmamos que ι_I es inyectivo. En efecto si $(m, 0) = (\varphi'(n), -f(n))$, entonces $n = 0$ porque f es un monomorfismo y, por lo tanto, $m = \varphi'(0) = 0$. Así, por hipótesis, ι_I tiene una retracción r, y es evidente que $r \circ \iota_N \circ f = r \circ \iota_I \circ \varphi' = \varphi'$. □

TEOREMA 4.8 (Baer). *Si todo morfismo de un ideal a izquierda de A en un A-módulo I, se extiende a ${}_AA$, entonces I es inyectivo.*

DEMOSTRACIÓN. Supongamos que $f\colon N' \to N$ es un monomorfismo y que $\varphi'\colon N' \to I$ es un morfismo. Una extensión parcial de φ' es un par (L, l), formado por un submódulo L de N que contiene a $f(N')$ y un morfismo $l\colon L \to I$ tal que $l \circ f = \varphi'$. El conjunto de las extensiones parciales de φ' está ordenado por

$$(L, l) \leq (H, h) \quad \text{si} \quad L \subseteq H \ \text{ y } \ h_{|L} = l.$$

Por el lema de Zorn hay una extensión parcial maximal $\varphi\colon M \to I$ de φ'. Para terminar la prueba será suficiente verificar que $M = N$. Para ello tomemos $n \in N$ arbitrario, escribamos $(M : n) := \{a \in A : a \cdot n \in M\}$ y consideremos la aplicación A-lineal $\phi\colon (M : n) \to I$, dada por $\phi(a) := \varphi(a \cdot n)$. Por hipótesis ϕ se extiende a un morfismo $\psi\colon A \to I$. Definamos $\overline{\varphi}\colon M + An \to I$ por $\overline{\varphi}(m + a \cdot n) := \varphi(m) + \psi(a)$ para $m \in M$ y $a \in A$. Esta definición es

correcta porque si $m + a \cdot n = m' + a' \cdot n$ con $a, a' \in A$ y $m, m' \in M$, entonces $a' - a \in (M : n)$ y así,

$$\varphi(m) - \varphi(m') = \varphi((a' - a) \cdot n) = \phi(a' - a) = \psi(a') - \psi(a).$$

Debido a la maximalidad de (M, φ), de la existencia de la extensión $(M + An, \overline{\varphi})$, se sigue que $n \in M$. □

PROPOSICIÓN 4.9. *Supongamos que A es un dominio. Entonces todo módulo inyectivo es divisible. Si además todo ideal a izquierda de A es principal, entonces vale la recíproca.*

DEMOSTRACIÓN. Supongamos primero que I es inyectivo, tomemos $m \in I$ y $a \in A$ y consideremos la aplicación A-lineal $f\colon Aa \to I$, dada por $f(ba) := b \cdot m$. Por hipótesis, existe una extensión $\overline{f}\colon {}_AA \to I$ de f. Es evidente que $a \cdot \overline{f}(1) = f(a) = m$. Supongamos ahora que I es divisible y que todo ideal a izquierda de A es monogenerado. Por el teorema de Baer, para probar que I es inyectivo será suficiente mostrar que, para cada $a \in A$, todo morfismo $f\colon Aa \to I$ se extiende a ${}_AA$. Como I es divisible, existe $m \in I$ tal que $a \cdot m = f(a)$. Es claro que la función $\overline{f}\colon A \to I$, definida por $\overline{f}(b) := b \cdot m$, es un morfismo de A-módulos que extiende a f. □

Capítulo 9

Condiciones de cadena

Nuestro objetivo en esta sección es introducir las nociones de anillos noetherianos y artinianos y estudiar sus propiedades básicas. En esta exposición M designa a un A-módulo arbitrario.

1. Módulos noetherianos

Un A-módulo es *noetheriano* si todos sus submódulos son finitamente generados. En el siguiente resultado establecemos otras caracterizaciones muy útiles de estos módulos. Una sucesión $M_1, M_2, M_3, M_4, \ldots$ de submódulos de M es *estacionaria* si existe $n \in \mathbb{N}$ tal que $M_n = M_{n+i}$ para todo $i \in \mathbb{N}$.

Proposición 1.1. *Son equivalentes:*

1. *M es noetheriano.*
2. *Toda sucesión creciente $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ de submódulos de M es estacionaria.*
3. *Toda familia no vacía de submódulos de M tiene un elemento maximal.*

Demostración. 1) $\Rightarrow$ 2) Consideremos una cadena creciente

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

de submódulos de M. Como $N = \bigcup_i M_i$ es finitamente generado, existe $n \in \mathbb{N}$ tal que $M_n = N$. En consecuencia $M_n = M_{n+i}$ para todo $i \in \mathbb{N}$.

2) $\Rightarrow$ 3) Supongamos, por el contrario, que existe una familia $(M_i)_{i\in I}$ no vacía de submódulos de M que no tiene elemento maximal. Afirmamos que hay una sucesión $i_1, i_2, i_3, \ldots$ de elementos de I tal que

$$M_{i_1} \subsetneq M_{i_2} \subsetneq M_{i_3} \subsetneq \cdots .$$

En efecto, esto se sigue inmediatamente de que habiendo elegido $i_1, \ldots, i_n$ con esta propiedad, por hipótesis existe $i_{n+1} \in I$ tal que $M_{i_n} \subsetneq M_{i_{n+1}}$.

3) $\Rightarrow$ 1) Debemos probar que cada submódulo N de M es finitamente generado. Por hipótesis, N tiene un submódulo finitamente generado maximal N'. Como $N' + Am$ es finitamente generado para todo $m \in N$, necesariamente $N' = N$. □

TEOREMA 1.2. *Para cada submódulo N de M son equivalentes:*

1. *M es noetheriano.*
2. *N y M/N son noetherianos.*

DEMOSTRACIÓN. Es claro que si M es noetheriano, entonces todos los submódulos de N son finitamente generados. También lo es cada submódulo L de M/N, porque $L = \pi(\pi^{-1}(L))$, donde $\pi\colon M \to M/N$ es la proyección canónica, y $\pi^{-1}(L)$ es finitamente generado por hipótesis. Así, 1) implica 2). Veamos que vale la recíproca. Tomemos un submódulo M' de M. Por hipótesis

$$M' \cap N \qquad \text{y} \qquad \frac{M'}{M' \cap N} \simeq \frac{M' + N}{N}$$

son finitamente generados. Pero entonces, por el item 2) de la Proposición 5.11, también lo es M'. □

COROLARIO 1.3. *Una suma directa de A-módulos $M_1 \oplus \cdots \oplus M_n$ es noetheriana si y sólo si cada M_i lo es.*

DEMOSTRACIÓN. Por inducción en n usando el teorema anterior. □

PROPOSICIÓN 1.4. *Todo A-módulo noetheriano M es hopfiano.*

DEMOSTRACIÓN. Si $f\colon M \to M$ es un morfismo sobreyectivo que no es inyectivo, entonces

$$0 \subsetneq \ker f \subsetneq \ker(f^2) \subsetneq \ker(f^3) \subsetneq \cdots$$

es una sucesión estrictamente creciente de submódulos de M. En efecto, $0 \subsetneq \ker f$ por hipótesis, y, por el teorema de la correspondencia,

$$\ker(f^i) \subsetneq \ker(f^{i+1}) \Rightarrow \ker(f^{i+1}) = f^{-1}\big(\ker(f^i)\big) \subsetneq f^{-1}\big(\ker(f^{i+1})\big) = \ker(f^{i+2}).$$

Por consiguiente, M no es noetheriano. □

Un anillo A es *noetheriano a izquierda* si lo es como A-módulo a izquierda, y es *noetheriano a derecha* si A^{op} es noetheriano a izquierda. Si A es noetheriano a ambos lados, entonces se dice simplemente que es *noetheriano*. En estas notas consideraremos sólo anillos noetherianos a izquierda.

OBSERVACIÓN 1.5. *Todo cociente de un anillo noetheriano a izquierda es noetheriano a izquierda.*

TEOREMA 1.6 (de la base de Hilbert). *Si un anillo A es noetheriano a izquierda, entonces también lo es el anillo de polinomios $A[X]$.*

DEMOSTRACIÓN. Supongamos que en $A[X]$ hay un ideal a izquierda I que no es finitamente generado. Definimos una sucesión de polinomios $P_1, P_2, \ldots$ en I como sigue: Tomamos como P_1 a un polinomio no nulo de grado mínimo de I. Habiendo elegido $P_1, \ldots, P_i$, tomamos como P_{i+1} a un polinomio no nulo de grado mínimo de $I \setminus \sum_{j=1}^{i} A[X]P_j$. Llamemos a_i al coeficiente principal de P_i. Por hipótesis el ideal a izquierda $J := \sum_{j\geq 1} Aa_j$ de A, es finitamente

generado. Así, existe $m \in \mathbb{N}$ tal que $J = \sum_{j=1}^{m} Aa_j$. Escribamos $a_{m+1} = u_1a_1 + \cdots + u_ma_m$. Como el grado de P_{m+1} no es menor que el de ninguno de los polinomios $P_1, \ldots, P_m$,

$$P := u_1X^{\mathrm{gr}(P_{m+1})-\mathrm{gr}(P_1)}P_1 + \cdots + u_mX^{\mathrm{gr}(P_{m+1})-\mathrm{gr}(P_m)}P_m \in \sum_{j=1}^{m} A[X]P_j.$$

Puesto que además P_{m+1} pertenece a $I \setminus \sum_{j=1}^{m} A[X]P_j$, la diferencia $P_{m+1} - P$ también está en $I \setminus \sum_{j=1}^{m} A[X]P_j$. Como $\mathrm{gr}(P_{m+1}-P) < \mathrm{gr}(P_{m+1})$, esto contradice la elección de P_{m+1}. □

Corolario 1.7. *Si A es noetheriano a izquierda, entonces $A[X_1, \ldots, X_n]/I$ es noetheriano para cada ideal I de $A[X_1, \ldots, X_n]$.*

Demostración. Es consecuencia inmediata del teorema de la base de Hilbert y de la Observación 1.5. □

Proposición 1.8. *Si A es noetheriano a izquierda y M es un A-módulo finitamente generado, entonces M es noetheriano.*

Demostración. Por el Corolario 1.3, todo módulo libre finitamente generado es noetheriano a izquierda. El resultado se sigue ahora del Teorema 1.2, ya que al ser finitamente generado, M es un cociente de un módulo libre, que también lo es. □

Corolario 1.9. *Todo anillo noetheriano a izquierda o a derecha satisface la ICB.*

Demostración. Por el item 1) de la Proposición 1.10 del capítulo 8 basta probarlo para anillos noetherianos a izquierda, y para estos vale por las Proposiciones 1.11 del mismo Capítulo y las Proposiciones 1.4 y 1.8. □

Corolario 1.10. *Los anillos de división satisfacen la ICB.*

Proposición 1.11. *Consideremos submódulos $M_1, \ldots, M_n$ de M. Son equivalentes:*

1. *M_i es noetheriano para todo i.*
2. *$M_1 + \cdots + M_n$ es noetheriano.*

Demostración. Veamos primero que el segundo item es una consecuencia del primero. Por el Corolario 1.3, la suma directa $M_1 \oplus \cdots \oplus M_n$ es noetheriana. En consecuencia, por el Teorema 1.2, el módulo $M_1 + \cdots + M_n$ es noetheriano, debido a que es un cociente de $M_1 \oplus \cdots \oplus M_n$. La recíproca se sigue inmediatamente del mismo teorema. □

Corolario 1.12. *Consideremos submódulos $M_1, \ldots, M_n$ de M. Son equivalentes:*

1. *Todos los cocientes M/M_i son noetherianos.*
2. *$\frac{M}{M_1 \cap \cdots \cap M_n}$ es noetheriano.*

Demostración. Supongamos que cada cociente M/M_i es noetheriano. Entonces, por el Corolario 1.3, también lo es $\bigoplus_{i=1}^{n} M/M_i$. Como las proyecciones canónicas $M \to M/M_i$ inducen un morfismo inyectivo

$$\frac{M}{M_1 \cap \cdots \cap M_n} \longrightarrow \bigoplus_{i=1}^{n} \frac{M}{M_i},$$

se sigue del Teorema 1.2 que $\frac{M}{M_1 \cap \cdots \cap M_n}$ es noetheriano. La recíproca es consecuencia inmediata del mismo teorema, porque cada M/M_i es un cociente de $\frac{M}{M_1 \cap \cdots \cap M_n}$. □

2. Módulos artinianos

En esta subsección introducimos los módulos artinianos y estudiamos algunas de sus propiedades básicas.

PROPOSICIÓN 2.1. *Son equivalentes:*

1. *Toda sucesión decreciente $M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots$ de submódulos de M es estacionaria.*
2. *Toda familia de submódulos de M tiene un elemento minimal.*

DEMOSTRACIÓN. 1) $\Rightarrow$ 2) Supongamos que existe una familia $(M_i)_{i\in I}$ no vacía de submódulos de M que no tiene elemento minimal. Afirmamos que hay una sucesión $i_1, i_2, i_3 \ldots$ de elementos de I tal que

$$M_{i_1} \supsetneq M_{i_2} \supsetneq M_{i_3} \supsetneq \cdots .$$

En efecto, esto se sigue inmediatamente de que habiendo elegido $i_1, \ldots, i_n$ con esta propiedad, por hipótesis existe $i_{n+1} \in I$ tal que $M_{i_n} \supsetneq M_{i_{n+1}}$.
2) $\Rightarrow$ 1) Debemos mostrar que toda sucesión decreciente

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots$$

de submódulos de M es estacionaria. Para ello basta notar que por hipótesis $\{M_i : i \in \mathbb{N}\}$ tiene un elemento minimal M_n, y que entonces $M_n = M_{n+i}$ para todo $i \in \mathbb{N}$. □

TEOREMA 2.2. *Para cada submódulo N de M son equivalentes:*

1. *M es artiniano.*
2. *N y M/N son artinianos.*

DEMOSTRACIÓN. Es claro que si M es artiniano, entonces toda sucesión decreciente de submódulos de N es estacionaria. También lo es cada sucesión decreciente

$$L_1 \supseteq L_2 \supseteq L_3 \supseteq \cdots$$

de submódulos de M/N, porque $L_i = \pi(\pi^{-1}(L_i))$ para cada i, donde $\pi\colon M \to M/N$ es la proyección canónica, y

$$\pi^{-1}(L_1) \supseteq \pi^{-1}(L_2) \supseteq \pi^{-1}(L_3) \supseteq \cdots$$

es estacionaria por hipótesis. Así, 1) implica 2). Para probar que vale la recíproca consideremos una sucesión decreciente

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots$$

de submódulos de M. Por hipótesis existe $n \in \mathbb{N}$ tal que

$$M_i \cap N = M_n \cap N \qquad \text{y} \qquad \pi(M_i) = \pi(M_n)$$

para todo $i > n$. Pero entonces

$$M_i + N = \pi^{-1}(\pi(M_i)) = \pi^{-1}(\pi(M_n)) = M_n + N$$

y, en consecuencia, $M_i = M_n$ por el item 2) de la Proposición 8.1 del Capítulo 1. □

COROLARIO 2.3. *Una suma directa de A-módulos $M_1 \oplus \cdots \oplus M_n$ es artiniana si y sólo si cada M_i lo es.*

DEMOSTRACIÓN. Por inducción en n, usando el teorema anterior. □

Diremos que un A-módulo es *cohopfiano* si todo endomorfismo inyectivo $f\colon M \to M$ es un isomorfismo.

PROPOSICIÓN 2.4. *Todo A-módulo artiniano M es cohopfiano.*

DEMOSTRACIÓN. Si $f\colon M \to M$ es un morfismo inyectivo que no es sobrectivo, entonces

$$M \supsetneq f(M) \supsetneq f^2(M) \supsetneq f^3(M) \supsetneq \cdots$$

es una sucesión estrictamente decreciente de submódulos de M. En efecto, $M \supsetneq f(M)$ por hipótesis, y

$$f^i(M) \supsetneq f^{i+1}(M) \Rightarrow f^{i+1}(M) \supsetneq f^{i+2}(M),$$

debido a que f es inyectiva. Por consiguiente, M no es artiniano. □

Un anillo A es *artiniano a izquierda* si lo es como A-módulo a izquierda, y es *artiniano a derecha* si A^{op} es artiniano a izquierda. Si A es artiniano a ambos lados, entonces se dice simplemente que es *artiniano*. En estas notas consideraremos sólo anillos artinianos a izquierda.

OBSERVACIÓN 2.5. *Todo cociente de un anillo artiniano a izquierda es artiniano a izquierda.*

Se puede probar que todo anillo artiniano a izquierda es noetheriano a izquierda. La recíproca no vale. Por ejemplo, $\mathbb{Z}$ es noetheriano, pero no artiniano. En realidad, para anillos, la condición de artinianidad es mucho más restrictiva que la de noetherianidad. Los siguientes ejemplos muestran que existen anillos artinianos.

EJEMPLO 2.6. *Todo anillo finito es artiniano.*

EJEMPLO 2.7. *Todo anillo que es un espacio vectorial de dimensión finita sobre un subanillo de división, es artiniano (por ejemplo, si A es un anillo de división y S es un monoide finito, entonces $A[S]$ es artiniano).*

PROPOSICIÓN 2.8. *Si A es artiniano a izquierda y M es un A-módulo finitamente generado, entonces M es artiniano.*

DEMOSTRACIÓN. Por el Corolario 2.3, todo módulo libre finitamente generado es artiniano a izquierda. El resultado se sigue ahora del Teorema 2.2, ya que al ser finitamente generado, M es un cociente de un módulo libre con base finita. □

COROLARIO 2.9. *Consideremos submódulos $M_1, \ldots, M_n$ de M. Son equivalentes:*

1. *M_i es artiniano para todo i.*
2. *$M_1 + \cdots + M_n$ es artiniano.*

DEMOSTRACIÓN. Veamos primero que el segundo item es consecuencia del primero. Por el Corolario 2.3, la suma directa $M_1 \oplus \cdots \oplus M_n$ es artiniana. Así, por el Teorema 2.2, el módulo $M_1 + \cdots + M_n$ es artiniano, debido a que es un cociente de $M_1 \oplus \cdots \oplus M_n$. La recíproca es una consecuencia inmediata del mismo teorema. □

PROPOSICIÓN 2.10. *Consideremos submódulos $M_1, \ldots, M_n$ de M. Son equivalentes:*

1. *Todos los cocientes M/M_i son artinianos.*
2. *$\frac{M}{M_1 \cap \cdots \cap M_n}$ es artiniano.*

DEMOSTRACIÓN. Supongamos que cada cociente M/M_i es artiniano. Entonces, por el Corolario 2.3, también lo es $\bigoplus_{i=1}^n M/M_i$. Como las proyecciones canónicas $M \to M/M_i$ inducen un morfismo inyectivo

$$\frac{M}{M_1 \cap \cdots \cap M_n} \longrightarrow \bigoplus_{i=1}^{n} \frac{M}{M_i},$$

del Teorema 2.2 se sigue que $\frac{M}{M_1\cap\cdots\cap M_n}$ es artiniano. La recíproca es consecuencia inmediata del mismo teorema, porque cada M/M_i es un cociente de $\frac{M}{M_1\cap\cdots\cap M_n}$. □

El anillo $\mathbb{Z}$ es un ejemplo de grupo abeliano que es noetheriano y no artiniano. También hay grupos abelianos que son artinianos y no noetherianos. Por ejemplo para cada primo $p \in \mathbb{N}$, el grupo

$$\mathbb{Z}_{p^\infty} := \frac{\{a/p^n : a \in \mathbb{Z} \text{ y } n \in \mathbb{N}\}}{\mathbb{Z}}$$

lo es. Para ver que esto es así será suficiente probar que si I es un subgrupo propio de $\mathbb{Z}_{p^\infty}$, entonces $I = \langle [1/p^n] \rangle$, donde $n \in \mathbb{N}_0$ es el máximo entero no negativo tal que $[1/p^n] \in I$. Tomemos para ello $[a/p^m] \in I$ con a coprimo con p y escribamos $1 = ra + sp^m$ con r y s enteros. Entonces,

$$[1/p^m] = [(ra + sp^m)/p^m] = r[a/p^m] \in I.$$

En consecuencia $m \leq n$ y, por lo tanto, $[a/p^m] = ap^{n-m}[1/p^m] \in \langle [1/p^n] \rangle$.

3. Módulos de longitud finita

Ahora vamos a estudiar los módulos que son simultáneamente noetherianos y artinianos. Decimos que dos cadenas crecientes finitas

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_m \qquad \text{y} \qquad N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq N_n,$$

de submódulos de un A-módulo M, son *equivalentes* si $m = n$ y existe una permutación $\sigma \in \mathrm{S}_m$ tal que

$$\frac{M_i}{M_{i-1}} \simeq \frac{N_{\sigma(i)}}{N_{\sigma(i)-1}} \quad \text{para todo } i \text{ entre 1 y } m;$$

y decimos que la primera *refina* a la segunda si existen índices $1 \leq i_1 < \cdots < i_n \leq m$, tales que $M_{i_j} = N_j$ para todo j.

LEMA 3.1 (Lema de la Mariposa). *Dados submódulos $N_1 \subseteq N_2$ y $M_1 \subseteq M_2$ de M, existen isomorfismos canónicos*

$$\frac{N_1 + (N_2 \cap M_2)}{N_1 + (N_2 \cap M_1)} \simeq \frac{N_2 \cap M_2}{(N_1 \cap M_2) + (N_2 \cap M_1)} \simeq \frac{M_1 + (N_2 \cap M_2)}{M_1 + (N_1 \cap M_2)}.$$

DEMOSTRACIÓN. El primer isomorfismo se obtiene aplicando el isomorfismo $\frac{L}{L\cap K} \simeq \frac{L+K}{K}$ con $L = N_2 \cap M_2$ y $K = N_1 + (N_2 \cap M_1)$ y usando la modularidad del reticulado de submódulos de M. El segundo sale por simetría. □

TEOREMA 3.2 (Schreier). *Dos cadenas finitas de submódulos de M siempre se pueden refinar a cadenas equivalentes.*

DEMOSTRACIÓN. Consideremos dos cadenas finitas

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_m \qquad \text{y} \qquad N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq N_n$$

de submódulos de M. Sin pérdida de generalidad podemos suponer que $M_0 = N_0 = 0$ y $M_m = N_n = M$. Escribamos

$$M_{ij} = M_{j-1} + (N_i \cap M_j) \qquad \text{y} \qquad N_{ij} = N_{i-1} + (N_i \cap M_j),$$

donde en cada caso los subíndices recorren todos los valores para los cuales la expresión a la derecha del signo igual tiene sentido. Intercalando los M_{ij} en la primer cadena y los N_{ij} en la segunda, obtenemos cadenas

$$M_0 = M_{01} \subseteq M_{11} \subseteq \cdots \subseteq M_{n1} = M_1 = M_{02} \subseteq \cdots \subseteq M_{nm} = M_m$$

y

$$N_0 = N_{10} \subseteq N_{11} \subseteq \cdots \subseteq N_{1m} = N_1 = N_{20} \subseteq \cdots \subseteq N_{nm} = N_n,$$

donde no necesariamente las inclusiones son propias. Por el lema de la Mariposa

$$\frac{M_{ij}}{M_{i-1,j}} \simeq \frac{N_{ij}}{N_{i,j-1}} \quad \text{para } 1 \leq i \leq n \text{ y } 1 \leq j \leq m.$$

El resultado es consecuencia inmediata de esto. □

Una cadena $0 = M_0 \subseteq \cdots \subseteq M_n = M$ de submódulos de M es una *serie de composición de longitud* n de M si cada cociente M_i/M_{i-1} es simple.

TEOREMA 3.3 (Jordan-Hölder). *Si M tiene una serie de composición, entonces cada cadena estrictamente creciente de submódulos de M se puede refinar a una serie de composición. Además todas las series de composición de M son equivalentes y, en particular, tienen la misma longitud.*

DEMOSTRACIÓN. Es un corolario inmediato del teorema de Schreier. □

Definimos la *longitud* $\ell(M)$ de un A-módulo M, por

$$\ell(M) := \begin{cases} 0 & \text{si } M = 0, \\ n & \text{si } M \text{ tiene una serie de composición de longitud } n, \\ \infty & \text{en otro caso.} \end{cases}$$

Por el teorema de Jordan Hölder, esta definición no es ambigua.

TEOREMA 3.4. *Consideremos un submódulo N de un A-módulo M. Entonces M tiene una serie de composición si y sólo si N y M/N la tienen. Además $\ell(M) = \ell(N) + \ell(M/N)$.*

DEMOSTRACIÓN. Evidentemente podemos suponer que N es un submódulo no trivial de M. Es claro que si M tiene una serie de composición, entonces refinando la cadena $0 \subseteq N \subseteq M$ a una serie de composición

$$0 = N_0 \subseteq \cdots \subseteq N_i = N \subseteq \cdots \subseteq N_m = M, \tag{64}$$

obtenemos series de composición

$$0 = N_0 \subseteq \cdots \subseteq N_i = N \qquad \text{y} \qquad 0 = \frac{N_i}{N} \subseteq \cdots \subseteq \frac{N_m}{N} = \frac{M}{N}, \tag{65}$$

de N y M/N, respectivamente. Notemos que además

$$\ell(M) = m = i + (m - i) = \ell(N) + \ell(M/N).$$

Recíprocamente, si M tiene un submódulo N tal que N y M/N tienen series de composición como (65), combinándolas se obtiene una serie de composición como (64). □

TEOREMA 3.5 (Teorema de la dimensión). *Dos submódulos M_1 y M_2 de M tienen longitud finita si y sólo si su suma e intersección la tienen. Además*

$$\ell(M_1 + M_2) + \ell(M_1 \cap M_2) = \ell(M_1) + \ell(M_2).$$

DEMOSTRACIÓN. Basta aplicar el teorema anterior a los submódulos y módulos cocientes que aparcen en las sucesiones exactas cortas

$$0 \longrightarrow M_1 \cap M_2 \longrightarrow M_1 \longrightarrow \frac{M_1}{M_1 \cap M_2} \longrightarrow 0$$

y

$$0 \longrightarrow M_2 \longrightarrow M_1 + M_2 \longrightarrow \frac{M_1 + M_2}{M_2} \longrightarrow 0\ ,$$

y usar que $\frac{M_1}{M_1 \cap M_2} \simeq \frac{M_1 + M_2}{M_2}$. □

PROPOSICIÓN 3.6. *Un A-módulo M tiene una serie de composición si y sólo si es noetheriano y artiniano.*

DEMOSTRACIÓN. Supongamos que M tiene longitud finita. Dado que toda cadena estrictamente creciente o estrictamente decreciente de submódulos de M tiene a lo sumo $\ell(M) + 1$ componentes, es inmediato que M es noetheriano y artiniano. Supongamos ahora que M es noetheriano y artiniano. Afirmamos que M tiene longitud finita. Tomemos un submódulo N de M, maximal entre los que tienen longitud finita. Para terminar la demostración es suficiente ver que $N = M$, pero esto se sigue de que si no podríamos tomar un submódulo N' de M, minimal entre los que contienen a N estrictamente y, de que entonces, $\ell(N') = \ell(N) + 1 < \infty$, contradiciendo la maximalidad de N. □

Capítulo 10

Módulos sobre dominios principales

Recordemos que A es un dominio principal si es un dominio conmutativo y todo ideal de A es cíclico y que todo dominio principal es de factorización única. Una consecuencia particular de esto es que los primos no nulos de A coinciden con los irreducibles.

1. Módulos libres

En toda esta sección A denota a un dominio principal.

TEOREMA 1.1. *Todo submódulo de un A-módulo libre es libre.*

DEMOSTRACIÓN. Supongamos que L es un A-módulo libre y que M es un submódulo de L. Fijemos una base bien ordenada $\mathcal{B} = (v_i)_{i\in I}$ de L y, para cada $i \in I$, consideremos los submódulos

$$L_i := \bigoplus_{j<i} \langle v_j\rangle, \quad \overline{L}_i := \bigoplus_{j\leq i} \langle v_j\rangle, \quad M_i = M \cap L_i \quad \text{y} \quad \overline{M}_i = M \cap \overline{L}_i,$$

de L. Notemos que $\overline{L}_i = L_i \oplus \langle v_i\rangle$ y que cada $m \in \overline{M}_i$ tiene una escritura única

$$m = m_i + \lambda_m \cdot v_i, \quad \text{con } m_i \in L_i \text{ y } \lambda_m \in A.$$

Es evidente que la fórmula $g_i(m) := \lambda_m$ define una aplicación A-lineal $g_i\colon \overline{M}_i \to A$. Como A es un dominio principal, la imagen de g_i es cero o es un A-módulo libre de dimensión 1 (dependiendo de si $M_i = \overline{M}_i$ o no). En ambos casos la sucesión exacta corta

$$0 \longrightarrow M_i \xrightarrow{\ \iota\ } \overline{M}_i \xrightarrow{\ g_i\ } \operatorname{Im}(g_i) \longrightarrow 0\ ,$$

donde ι es la inclusión canónica, es escindida y, por lo tanto, existe un submódulo M_i' de $\overline{M}_i$, tal que $\overline{M}_i = M_i \oplus M_i'$ y $M_i' \simeq \operatorname{Im}(g_i)$. Afirmamos que $\sum_{i\in I} M_i'$ es directa y que $M = \bigoplus_{i\in I} M_i'$. Veamos primero que la suma es directa. Para ello escribimos

$$0 = m_{i_1} + \cdots + m_{i_r}, \quad \text{con } r \geq 1,\ m_{i_h} \in M_{i_h}' \text{ e } i_1 < i_2 < \cdots < i_r,$$

y procedemos por inducción en r. Es claro que si $r = 1$, entonces $m_{i_1} = 0$. Supongamos ahora que $r > 1$. Como

$$m_{i_1} + \cdots + m_{i_{r-1}} \in M_{i_r} \quad \text{y} \quad \overline{M}_{i_r} = M_{i_r} \oplus M'_{i_r},$$

debe ser $m_{i_r} = 0$ y, a posteriori, $m_{i_1} = \cdots = m_{i_{r-1}} = 0$. Veamos a continuación que

$$M = \bigoplus_{i \in I} M'_i.$$

Es evidente que $\bigoplus_{i\in I} M'_i \subseteq M$. Supongamos que la inclusión recíproca no vale y tomemos $m \in M \setminus \bigoplus_{i\in I} M'_i$ con $i(m)$ mínimo, donde para cada $m \in M \setminus \{0\}$ denotamos con $i(m)$ al menor de los $i \in I$ tal que $m \in \overline{L}_i$. Dado que

$$m \in \overline{L}_{i(m)} \cap M = \overline{M}_{i(m)} = M_{i(m)} \oplus M'_{i(m)},$$

existen $m' \in M_{i(m)}$ y $m'' \in M'_{i(m)}$ tales que $m = m' + m''$. Como, por la minimalidad de $i(m)$,

$$m' \in \bigoplus_{i \in I} M'_i,$$

también

$$m = m' + m'' \in \bigoplus_{i \in I} M'_i,$$

contradiciendo la suposición hecha arriba. Por lo tanto, M es la suma directa de los M'_i, como queremos. □

Corolario 1.2. *Todo A-módulo finitamente generado sin torsión es libre.*

Demostración. Es consecuencia inmediata de los Teoremas 2.7 y 1.1. □

Corolario 1.3. *Para todo A-módulo finitamente generado M existe $n \in \mathbb{N}_0$ tal que*

$$M = \mathrm{T}(M) \oplus \frac{M}{\mathrm{T}(M)} \simeq \mathrm{T}(M) \oplus A^{(n)}. \tag{66}$$

Además n no depende del isomorfismo elegido.

Demostración. Basta observar que la sucesión exacta corta

$$0 \longrightarrow \mathrm{T}(M) \xrightarrow{\ \iota\ } M \xrightarrow{\ p\ } M/T(M) \longrightarrow 0\ ,$$

se parte porque, por el corolario anterior existe $n \in \mathbb{N}_0$ tal que $M/\mathrm{T}(M) \simeq A^{(n)}$. La unicidad de n se sigue de que el isomorfismo que aparece en (66) induce un isomorfismo

$$\frac{M}{\mathrm{T}(M)} \simeq \frac{\mathrm{T}(M) \oplus A^{(n)}}{\mathrm{T}\big(\mathrm{T}(M) \oplus A^{(n)}\big)} = \frac{\mathrm{T}(M) \oplus A^{(n)}}{\mathrm{T}(M)} \simeq A^{(n)}$$

y de que todo anillo conmutativo satisface la ICB. □

2. Módulos de torsión

Consideremos un dominio principal A y un elemento irreducible $p \in A\setminus\{0\}$. Un A-módulo M es *p-primario* si para todo $m \in M$ existe $n \in \mathbb{N}$ tal que $p^n \cdot m = 0$. Para cada A-módulo M, el conjunto

$$M_p := \{m \in M : p^n \cdot m = 0 \text{ para algún } n \in \mathbb{N}\}$$

es un submódulo p-primario de M, llamado *la componente p-primaria de M*.

Observación 2.1. *Para todo morfismo de A-módulos $f\colon M \to N$ y cada primo $p \in A$ no nulo, $f(M_p) \subseteq N_p$. En efecto esto se sigue de que si $p^n \cdot m = 0$, entonces*

$$p^n \cdot f(m) = f(p^n \cdot m) = f(0) = 0.$$

Teorema 2.2. *Si M es un A-módulo de torsión, entonces*

$$M = \bigoplus_{p\in\mathcal{P}} M_p,$$

donde $\mathcal{P}$ es una familia de representantes de las clases de equivalencia de los irreducibles de A módulo asociados.

Demostración. Por hipótesis, dado $m\in M$, existe $a\in A\setminus\{0\}$ tal que $a\cdot m=0$. Escribamos

$$a = up_1^{l_1}\cdots p_r^{l_r},$$

con $u \in A^\times$, $p_1,\dots,p_r \in \mathcal{P}$ y $n_1,\dots,n_r \in \mathbb{N}$. Consideremos los elementos $b_i := a/p_i^{l_i}$. Como los b_i's son coprimos, existen $c_1,\dots,c_r \in A$ tales que $c_1b_1 + \cdots + c_rb_r = 1$. Por lo tanto

$$m = 1 \cdot m = c_1b_1 \cdot m + \cdots + c_rb_r \cdot m.$$

Además, $b_i \cdot m \in M_{p_i}$ porque $p_i^{l_i} \cdot (b_i \cdot m) = a \cdot m = 0$ y así,

$$M = \sum_{p\in\mathcal{P}} M_p.$$

Resta probar que la suma es directa. Supongamos que

$$m_1 + \cdots + m_s = 0 \qquad \text{con } m_j \in M_{p_j}.$$

Debemos mostrar que $m_1 = \cdots = m_s = 0$. Esto es obvio si $s = 1$. Supongamos que es cierto cuando $s = n$ y que $s = n + 1$. Tomemos $h_1,\dots,h_{n+1} \in \mathbb{N}$ tales que $p_j^{h_j} \cdot m_j = 0$. Entonces

$$0 = p_1^{h_1}\cdots p_n^{h_n} \cdot (m_1 + \cdots + m_n) = -p_1^{h_1}\cdots p_n^{h_n} \cdot m_{n+1}.$$

Pero como $p_1^{h_1}\cdots p_n^{h_n}$ y $p_{n+1}^{h_{n+1}}$ son coprimos, existen $a, b \in A$ tales que

$$ap_1^{h_1}\cdots p_n^{h_n} + bp_{n+1}^{h_{n+1}} = 1,$$

y, por lo tanto,

$$m_{n+1} = ap_1^{h_1}\cdots p_n^{h_n} \cdot m_{n+1} + bp^{h_{n+1}} \cdot m_{n+1} = 0.$$

Ahora $m_1 = \cdots = m_n = 0$, por hipótesis inductiva. □

Nota 2.3. *Si M es finitamente generado, entonces el conjunto $\mathcal{P}' := \{p \in \mathcal{P} : M_p \neq 0\}$ es finito y, para cada $p \in \mathcal{P}'$ existe $r_p \in \mathbb{N}$ tal que $\mathrm{An}(M_p) = \langle p^{n_p}\rangle$.*

Teorema 2.4. *Si $M \neq 0$ es un A-módulo p-primario y existe $r \in \mathbb{N}$ tal que $p^rM = 0$, entonces M es suma directa de módulos cíclicos.*

DEMOSTRACIÓN. Denotemos con V a M/pM y consideremos las filtraciones

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots \qquad \text{y} \qquad V_1 \subseteq V_2 \subseteq V_3 \subseteq \cdots$$

de M y V respectivamente definidas por

$$M_i := \{m \in M : p^i \cdot m = 0\} \qquad \text{y} \qquad V_i := \frac{M_i + pM}{pM}.$$

Es evidente que $M = \bigcup M_i$ y $V = \bigcup V_i$. Tomemos una base S de V como A/pA-espacio vectorial, tal que $S \cap V_i$ es una base de V_i y para cada $s \in S$ denotemos con $i(s)$ al mínimo i tal que $s \in S \cap V_i$. Para cada $s \in S$ elijamos un representante s' de s en $M_{i(s)}$ (es decir elijamos $s' \in M_{i(s)}$ tal que $\pi(s') = s$) y definamos

$$\varphi\colon \bigoplus_{s\in S} \frac{A}{p^{i(s)}A} \longrightarrow M$$

por

$$\varphi\big((\overline{a}_s)_{s\in S}\big) := \sum_{s\in S} a_s \cdot s'.$$

donde $a_s \in A$ y $\overline{a}_s$ denota a la clase de a_s en $A/p^{i(s)}A$. Es fácil comprobar que φ está bien definido y que es un morfismo de A-módulos. Así, para terminar la demostración, sólo debemos probar que también es biyectivo. Veamos primero que si $\varphi\big((\overline{a}_s)_{s\in S}\big) = 0$, entonces $\overline{a}_s = 0$ para todo $s \in S$. Claramente para esto es suficiente probar que

$$\overline{a}_s \in \frac{p^i A}{p^{i(s)}A} \qquad \text{para todo } s \in S \text{ y todo } i \in \mathbb{N}_0. \tag{67}$$

Procedemos por inducción en i. Para $i = 0$ no hay nada que probar. Supongamos ahora que (67) vale para $i = k$ con $k \in \mathbb{N}_0$ fijo. Entonces

$$\sum_{\substack{s\in S\\ i(s)\geq k+1}} a_s \cdot s' = \sum_{s\in S} a_s \cdot s' = 0,$$

pues de (67) se sigue que $\overline{a}_s = 0$ para todo s tal que $i(s) \leq k$. De (67) se sigue también que para cada $s \in S$ tal que $i(s) \geq k+1$ existe $a'_s \in A$ tal que $a_s = p^k a'_s$. Claramente

$$p^k \sum_{\substack{s\in S\\ i(s)\geq k+1}} a'_s \cdot s' = \sum_{\substack{s\in S\\ i(s)\geq k+1}} p^k a'_s \cdot s' = \sum_{\substack{s\in S\\ i(s)\geq k+1}} a_s \cdot s' = 0,$$

lo cual implica que

$$\sum_{\substack{s\in S\\ i(s)\geq k+1}} a'_s \cdot s' \in M_k.$$

Considerando la imagen de esta igualdad en V obtenemos que

$$\sum_{\substack{s\in S\\ i(s)\geq k+1}} \overline{a'}_s \cdot s \in V_k,$$

de donde $a'_s \equiv 0 \pmod{p}$ para todo $s \in S$ tal que $i(s) \geq k+1$. En consecuencia

$$a_s = p^k a'_s \in p^{k+1}A \qquad \text{para todo } s \in S \text{ tal que } i(s) \geq k+1,$$

como queremos. Resta ver que φ es sobreyectivo. Afirmamos que

$$M = \operatorname{Im}\varphi + p^i M \qquad \text{para todo } i \in \mathbb{N}. \tag{68}$$

En efecto para $i = 1$ esto se sigue de que la imagen en V de $\operatorname{Im}\varphi$ coincide con V. Supongamos ahora que la igualdad (68) vale para $i = k$ con $k \in \mathbb{N}$ fijo. Entonces

$$M = \operatorname{Im}\varphi + pM = \operatorname{Im}\varphi + p(\operatorname{Im}\varphi + p^i M) = \operatorname{Im}\varphi + p\operatorname{Im}\varphi + p^{i+1}M = \operatorname{Im}\varphi + p^{i+1}M,$$

como queremos. Como $p^r M = 0$ se sigue de la igualdad (68) para $i := r$ que $M = \operatorname{Im}\varphi$. □

Observación 2.5. *Supongamos que $M \neq 0$ es un A-módulo p-primario y finitamente generado donde p es un primo no nulo de A y que $r \in \mathbb{N}$ es el mínimo natural tal que $p^r M = 0$. El teorema anterior dice que existen $n_1, \ldots, n_r \in \mathbb{N}_0$ con $n_r > 0$ tales que*

$$M \simeq \bigoplus_{j=1}^{r} \left(\frac{A}{Ap^j}\right)^{(n_j)}. \tag{69}$$

Afirmamos que los n_j's no dependen del isomorfismo (69)*. Probaremos esto por inducción en r. Cuando $r = 1$ el resultado es evidente pues en este caso n_1 es la dimensión de M como $\frac{A}{\langle p\rangle}$-espacio vectorial. Supongamos ahora que $r>1$ y que el resultado vale para $r-1$. Dado que*

$$pM \simeq \bigoplus_{j=1}^{r} \left(\frac{Ap}{Ap^j}\right)^{(n_j)} \simeq \bigoplus_{j=2}^{r} \left(\frac{A}{Ap^{j-1}}\right)^{(n_j)} \quad y \quad \frac{M}{pM} \simeq \left(\frac{A}{Ap}\right)^{(n_1+\cdots+n_r)}, \tag{70}$$

se sigue de la hipótesis inductiva que los n_j's no dependen del isomorfismo (69)*.*

3. Teoremas de estructura

En lo que sigue A es un dominio principal y $\mathcal{P}$ es una familia de representantes de las clases de equivalencia de los irreducibles de A, módulo asociados.

Teorema 3.1. *Para todo módulo finitamente generado M hay un isomorfismo*

$$f\colon M \longrightarrow A^{(n)} \oplus \bigoplus_{p\in\mathcal{P}'} \bigoplus_{j=1}^{r_p} \left(\frac{A}{Ap^j}\right)^{(n_{pj})}$$

donde $\mathcal{P}'$ es un subconjunto finito de $\mathcal{P}$, n y los n_{pj} son enteros no negativos que no dependen del isomorfismo f y $n_{pr_p} > 0$ para todo $p \in \mathcal{P}'$.

Demostración. La existencia de f se sigue del Corolario 1.3 y de los Teoremas 2.2 y 2.4. Por otro lado del Corolario 1.3 se sigue también que n no depende de f. Para ver que los n_{pj} tampoco lo hacen basta notar que, por la Observación 2.1, para cada $p \in \mathcal{P}'$ el morfismo f induce un isomorfismo

$$f_p\colon M_p \longrightarrow \bigoplus_{j=1}^{r_p} \left(\frac{A}{Ap^j}\right)^{(n_{pj})}$$

y aplicar la Observación 2.5. □

Nota 3.2. *Con las notaciones del teorema anterior $\langle \prod_{p\in\mathcal{P}'} p^{r_p}\rangle = \operatorname{An}(T(M))$.*

Teorema 3.3. *Para todo módulo finitamente generado M hay un isomorfismo*

$$f\colon M \longrightarrow A^{(n)} \oplus \bigoplus_{j=1}^{s} \left(\frac{A}{Ad_j}\right)^{(n_j)}$$

donde los d_i's son elementos no nulos de A tales que d_i/d_{i+1} para $1 \leq i < s$ y los d_iA no dependen del isomorfismo f.

Demostración. Usaremos libremente las notaciones del Teorema 3.1. Veamos primero la existencia. Debemos probar que existen elementos no nulos $d_1, \ldots, d_r$ de A tales que d_i/d_{i+1} para $1 \leq i < r$ y

$$\bigoplus_{p\in\mathcal{P}'} \bigoplus_{j=1}^{r_p} \left(\frac{A}{Ap^j}\right)^{(n_{pj})} \simeq \bigoplus_{j=1}^{s} \frac{A}{Ad_j}.$$

Escribamos $d := \prod_{p\in\mathcal{P}'} p^{r_p}$. Por el teorema chino del resto

$$\frac{A}{Ad} = \bigoplus_{p\in\mathcal{P}'} \frac{A}{Ap^{r_p}}.$$

Así, por el Teorema 3.1

$$\bigoplus_{p\in\mathcal{P}'} \bigoplus_{j=1}^{r_p} \left(\frac{A}{Ap^j}\right)^{(n_{pj})} \simeq \bigoplus_{p\in\mathcal{P}'} \left(\left(\bigoplus_{j=1}^{r_p-1} \left(\frac{A}{Ap^j}\right)^{(n_{pj})}\right) \oplus \left(\frac{A}{Ap^{r_p}}\right)^{(n_{pr_p}-1)}\right) \oplus \frac{A}{Ad}. \tag{71}$$

Notemos que dA es el anulador del módulo que está a la izquierda de $\simeq$. Si la suma de los n_{pj} (con j y p variando) es igual al cardinal de $\mathcal{P}'$, entonces la demostración está terminada. Supongamos que este no es el caso. Por inducción en la suma de los n_{pj} (con j y p variando) existen $s \geq 2$ y elementos no nulos $d_1, \ldots, d_{s-1}$ de A tales que d_j/d_{j+1} para $1 \leq j < s-1$, y

$$\bigoplus_{p\in\mathcal{P}'} \left(\left(\bigoplus_{j=1}^{r_p-1} \left(\frac{A}{Ap^j}\right)^{(n_{pj})}\right) \oplus \left(\frac{A}{Ap^{r_p}}\right)^{(n_{pr_p}-1)}\right) \simeq \bigoplus_{j=1}^{s-1} \left(\frac{A}{Ad_j}\right)^{(n_j)} \tag{72}$$

Notemos que $d_{s-1}A$ es el anulador del módulo que está a la izquierda de $\simeq$ y que, por lo tanto, $d_{s-1} \mid d$. Escribamos d_s en lugar de d. Combinamdo (71) con (72) obtenemos que

$$\bigoplus_{p\in\mathcal{P}'} \bigoplus_{j=1}^{r_p} \left(\frac{A}{Ap^j}\right)^{(n_{pj})} \simeq \bigoplus_{j=1}^{s} \frac{A}{Ad_j}.$$

Esto termina la prueba de la existencia de los d_j's. Veamos ahora la unicidad de los d_j's. El isomorfismo f induce un isomorfismo entre

$$T(M) \simeq \bigoplus_{j=1}^{s} \frac{A}{Ad_j}. \tag{73}$$

Denotemos con $\mathcal{P}'$ al subconjunto de $\mathcal{P}$ formados por los primos que dividen a d_s. Como $d_j \mid d_{j+1}$ para $1 \leq j < s$, la factorización de cada d_j es de la forma

$$d_j = u_j \prod_{p\in\mathcal{P}'} p^{r_{pj}},$$

con $u_j \in A^\times$, cada r_{pj} en $\mathbb{N}_0$ y $r_{p1} \leq r_{p2} \leq \cdots \leq r_{ps}$. Por el Teorema chino del resto

$$\frac{A}{Ad_j} \simeq \bigoplus_{p\in\mathcal{P}'} \frac{A}{Ap^{r_{pj}}}$$

Combinando esto con (73) obtenemos que $T(M) = \bigoplus_{p\in\mathcal{P}'} T(M)_p$ y, para cada $p \in \mathcal{P}'$,

$$T(M)_p = \bigoplus_{j=1}^{s} \frac{A}{Ap^{r_{pj}}}.$$

Como $r_{p1} \leq r_{p2} \leq \cdots \leq r_{ps}$ se sigue de esto y de la Observación 2.5 que los r_{pj}'s están determinados por $T(M)_p$. Por lo tanto los d_j's son únicos módulo asociados. □