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, dados $s_1, s_2 \in S$, escribiremos $s_1 * s_2$ en lugar de $*(s_1, s_2)$. Decimos que $*$ 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, la suma y el producto de los números enteros. 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. Dado un 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} es definida por $s_1 *_{\mathrm{op}} s_2 = s_2 * s_1$. Es evidente que S es un semigrupo si y sólo si lo es S^{op}, y que S es un magma conmutativo si y sólo si $S^{\mathrm{op}} = S$.

Dado un 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 S es conmutativo si y sólo si $l_s = r_s$ para todo $s \in S$, y el siguiente resultado muestra que es asociativo si y sólo si las estas funciones satisfacen algunas relaciones naturales.

Proposición 1.1. *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 $s_1, s_2 \in S$.*

Demostración. Los items 1) y 2) son equivalentes porque

$$l_{s_1}\circ r_{s_2}(s) = s_1 * (s * s_2) \quad \text{y} \quad r_{s_2}\circ l_{s_1}(s) = (s_1 * s) * s_2;$$

los item 1) y 3) lo son porque

$$l_{s_1}\circ l_{s_2}(s) = s_1 * (s_2 * s) \quad \text{y} \quad l_{s_1 * s_2}(s) = (s_1 * s_2) * s;$$

y una cuenta similar muestra que también lo son los items 1) y 4). □

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 (respectivamente a derecha), de un semigrupo S, entonces s_1s_2 también lo es. En cambio, la hipótesis de que s_1s_2 es cancelable a izquierda sólo implica que s_2 lo es, y la de que s_1s_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 S es unitario si y sólo si S^{op} lo es.

Un *monoide* es un magma unitario y asociativo. 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.

Proposición 1.2. *Un elemento s de S es inversible a izquierda si y sólo si r_s es sobreyectiva, y es inversible a derecha si y sólo si l_s es sobreyectiva.*

Demostración. Si s tiene una inversa a izquierda t, entonces

$$r_s(ut) = uts = u \quad \text{para todo } u \in S.$$

En particular r_s es sobreyectiva. Recíprocamente, si r_s es sobreyectiva, entonces $ts = 1$ para cada $t \in r_s^{-1}(1)$. La otra afirmación puede probarse en forma similar. □

Si $s \in S$ 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 el elemento t es la *inversa* de s.

Los enunciados predicables sobre elementos y subconjuntos de un magma S tienen una versión a izquierda y otra a derecha, de modo de uno es cierto en S si y sólo si el otro lo es en S^{op}. Diremos que estas afirmaciones son *duales* una de la otra. Por ejemplo,"s es inversible a izquierda" es dual de "s es inversible a derecha". En consecuencia, si una afirmación es verdadera en S y en S^{op}, entonces, por "dualidad", también lo es la afirmación dual. Un predicado es *autodual* si es igual a su dual. Por ejemplo, "s es cancelativo" es autodual. A veces enunciaremos un predicado, sin mencionar su dual. En estos casos dejamos la tarea de establecer este al lector.

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 elemento 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}. Nunca usaremos la notación aditiva 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 $1^{-1} = 1$) y que u es una inversa a izquierda de s si y sólo si s es una inversa a derecha de u. También es evidente que

- Si st es inversible a izquierda, entonces también lo es t.
- Si s' y t' son inversas a izquierda de s y t respectivamente, entonces $t's'$ es una inversa a izquierda de st.

En particular, si s y t son inversibles, entonces st también lo es y $(st)^{-1} = t^{-1}s^{-1}$. Se comprueba fácilmente que si s es inversible a izquierda, entonces es cancelable a izquierda. Similarmente, los elementos inversibles a derecha son cancelables a derecha.

PROPOSICIÓN 1.3. *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,

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

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

EJERCICIO 1.4. *Consideremos un elemento s de un monoide S. Pruebe que 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.*

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 definimos s^n para $n < 0$, por $s^n := (s^{-n})^{-1}$. 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
$$s^0, \dots, s^{|s|-1}$$
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 1.5. *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 1.6. *El conjunto* $\operatorname{Fun}(X, X)$*, de las funciones de un conjunto* X *en si mismo, es un monoide vía la composición, el cual sólo es abeliano cuando el cardinal de* X *es menor o igual que* 1.

Ejemplo 1.7. *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 1.8. *El conjunto* $\operatorname{End}_k V$*, 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* $\operatorname{End}_k V$ *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 $\langle u_1, \dots, u_{\mathrm{n}}\rangle_{\mathrm{M}}$ en lugar de $\langle\{u_1, \dots, u_{\mathrm{n}}\}\rangle_{\mathrm{M}}$. 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

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

para cada familia U de elementos de S, si adoptamos la convención de que el producto vacío da 1.

Dados 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 1.9. *Si K y L son submonoides de S, entonces KL es un submonoide de S (necesariamente igual a $\langle K \cup L\rangle_{\mathrm{M}}$) 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 $LK \subseteq KLKL = KL$. $\square$

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

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

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'), donde S y S' son monoides y φ es una función del conjunto subyacente de S en el de S', que satisface:

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

El monoide S es el *dominio* de φ, y S' el *codominio*. 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

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

Los ordenes de s y de $\varphi(s)$ son iguales cuando φ es inyectivo, debido a que en este 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 $\varphi\circ\varphi^{-1}=\mathrm{id}_{S'}$.

PROPOSICIÓN 1.10. *Un morfismo $\varphi\colon S\to S'$ es un isomorfismo si y sólo si es biyectivo.*

DEMOSTRACIÓN. Supongamos que φ es biyectivo. Como φ es un morfismo,

$$\varphi\bigl(\varphi^{-1}(s)\varphi^{-1}(t)\bigr)=\varphi\bigl(\varphi^{-1}(s)\bigr)\varphi\bigl(\varphi^{-1}(t)\bigr)=st=\varphi\bigl(\varphi^{-1}(st)\bigr)\tag{1}$$

y

$$\varphi(1)=1=\varphi\bigl(\varphi^{-1}(1)\bigr),\tag{2}$$

y como es inyectivo, las igualdades (1) y (2) implican que φ^{-1} es un morfismo. Así, cada morfismo biyectivo es un isomorfismo. La recíproca vale trivialmente. □

Dos monoides S y S' son *isomorfos* si hay un isomorfismo de S en S'. En ese caso escribimos $S\approx S'$. Un *automorfismo* de S es un endomorfismo de S que es un isomorfismo. Los símbolos $\mathrm{Hom}_{\mathrm{M}}(S,S')$, $\mathrm{Iso}_{\mathrm{M}}(S,S')$, $\mathrm{End}_{\mathrm{M}}\,S$ y $\mathrm{Aut}_{\mathrm{M}}\,S$ denotan respectivamente a los conjuntos de morfismos de S en S', isomorfismos de S en S', endomorfismos de S y automorfismos de S.

Es evidente que $\mathrm{End}_{\mathrm{M}} S$ 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 inyectiva, todo morfismo inyectivo un monomorfismo, y todo morfismo sobreyectivo 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. Una propiedad un poco más dificil de verificar es que todo monomorfismo $\varphi\colon S \to S'$ es inyectivo (lo cual, en particular, muestra nuevamente que lo es toda sección). Para comprobarlo basta observar que si $\varphi(s) = \varphi(s')$, entonces $\varphi\circ\psi = \varphi\circ\psi'$, donde $\psi, \psi'\colon \mathbb{N}_0 \to S$ son los morfismos definidos por

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

Por lo tanto $\psi = \psi'$ y entonces $s = s'$.

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.

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 1.11. *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 1.12. *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 $g \in G$. □

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 1.13. *El conjunto $S^{\times}$, de los elementos inversibles de un monoide S, es un grupo, llamado el* grupo de unidades *de S, vía la operación inducida. Por ejemplo, si S es un monoide, entonces $\operatorname{Aut}_{\mathrm{M}} S$ es el grupo de unidades de $\operatorname{End}_{\mathrm{M}} S$.*

EJEMPLO 1.14. *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 1.15. *Consideremos un k-espacio vectorial V. El* grupo lineal general $\mathrm{GL}(V)$ *es el grupo de unidades del anillo de endomorfismos $\operatorname{End}_k V$. Este grupo es abeliano si y sólo si $\dim_k V = 1$.*

EJEMPLO 1.16. *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 1.17. *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 $\operatorname{Fun}(X,X)$. 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*

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

Cuando X es el conjunto $\{1, 2, \dots, n\}$ 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 1.18. *Pruebe que si un grupo G tiene exponente 2, entonces es abeliano.*

5. Subgrupos

Un submonoide H de un grupo G es un *subgrupo* 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, dado un 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}. Puesto que el conjunto de todos estos productos es un subgrupo de G,

$$\langle T\rangle = \{g_1\cdots g_n : n\ge 0 \text{ y } g_i\in T \text{ o } g_i^{-1}\in T\}. \tag{3}$$

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 $\langle T\rangle_{\mathrm{M}} \subsetneq \langle T\rangle$. 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 $\langle g_1,\dots,g_n\rangle$ en lugar de $\langle\{g_1,\dots,g_n\}\rangle$. 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

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

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 1.19. *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 1.20. *Los conjuntos $\mathbb{Q}_{>0}$ y $\mathbb{R}_{>0}$ son subgrupos de $\mathbb{Q}^\times$ y $\mathbb{R}^\times$, respectivamente*

Ejemplo 1.21. *El conjunto $\mathbb{Z}[X]$, de polinomios con coeficientes enteros, es un subgrupo de $\mathbb{Q}[X]$.*

Ejemplo 1.22. *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 con determinante* 1.

Ejemplo 1.23. *Nuevamente consideremos un espacio euclideano E, con producto interno $\langle -,-\rangle$ y función distancia $d\colon E\times E\to E$. Recordemos que una* isometría *o* movimiento rígido *de E es una función $f\colon E\to E$, que preserva distancias. Por ejemplo, las transformaciones ortogonales y las traslaciones son movimientos rígidos. El* grupo de isometrías *de E es el subgrupo* $\mathrm{ISO}(E)$ *de* S_E*, formado por los movimientos rígidos.*

Observación 1.24. *Todos los elementos de* $\mathrm{ISO}(E)$ *son composición de una transformación ortogonal con una traslación. En efecto, dada una isometría arbitraria, componiendola* *con una traslación adecuada obtenemos una isometría f que fija el 0. Entonces, para cada $u, v \in E$,*

$$d^2(f(u), f(v)) = d^2(u, v) = \langle u - v, u - v\rangle = \langle u, u\rangle - 2\langle u, v\rangle + \langle v, v\rangle$$

y

$$\begin{aligned} d^2(f(u), f(v)) &= \langle f(u) - f(v), f(u) - f(v)\rangle \\ &= \langle f(u), f(u)\rangle - 2\langle f(u), f(v)\rangle + \langle f(v), f(v)\rangle \\ &= \langle u, u\rangle - 2\langle f(u), f(v)\rangle + \langle v, v\rangle. \end{aligned}$$

Por lo tanto,

$$\langle f(u), f(v)\rangle = \langle u, v\rangle \quad \textit{para todo } u, v \in E. \tag{4}$$

Tomemos ahora $\lambda \in \mathbb{R}$ y $u, v \in E$. Por y (4) y la bilinealidad de $\langle -, -\rangle$, el segundo término de la igualdad

$$d^2(f(\lambda u + v) - \lambda f(u) - f(v)) = \langle f(\lambda u + v) - \lambda f(u) - f(v), f(\lambda u + v) - \lambda f(u) - f(v)\rangle,$$

es 0. Esto muestra que f es una transformación lineal que preserva producto interno, y concluye la prueba de la afirmación.

Observación 1.25. *Dado $v \in E$, denotemos con t_v a la traslación de E definida por $t_v(u) = u + v$. Un cálculo sencillo prueba que*

$$t_v \circ t_w = t_{v+w}, \quad t_v^{-1} = t_{-v} \quad \textit{y} \quad t_{-t(v)} \circ f \circ t_v \in \mathrm{O}(E),$$

para todo $v, w \in E$ y $f \in \mathrm{O}(E)$. En particular, esto da una fórmula para la composición de elementos de $\mathrm{ISO}(E)$, cuando son expresados como composición $t_v \circ f$, de una traslación y una transformación ortogonal.

Ejemplo 1.26. *El conjunto $\mathrm{SL}(n, k)$, de las matrices de $n \times n$ de determinante 1 con coeficientes en un cuerpo k, es un subgrupo de $\mathrm{GL}(n, k)$.*

Ejemplo 1.27. *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 $\mathrm{G}_\infty := \bigcup_{n\in\mathbb{N}} \mathrm{G}_n$.*

Ejemplo 1.28. *Consideremos el ángulo $\theta = 2\pi/n$, donde $n > 1$. El subgrupo de $\mathrm{GL}(2, \mathbb{R})$ generado por la rotación*

$$x = \begin{pmatrix} \cos\theta & \operatorname{sen}\theta \\ -\operatorname{sen}\theta & \cos\theta \end{pmatrix},$$

de ángulo θ en sentido contrario de las agujas del reloj, y por la reflexión

$$y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

respecto del eje real, es, por definición, el grupo diedral *D_n. Un cálculo directo muestra que*

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

De esto se sigue fácilmente que x e y satisfacen las relaciones $x^n = 1$, $y^2 = 1$ e $yxy^{-1} = x^{-1}$ y que D_n consiste de los $2n$ elementos $1, x \dots, x^{n-1}, y, xy, \dots, x^{n-1}y$.

Observación 1.29. *Denotemos con el símbolo P_n al polígono regular de n lados y vértices $a_0,\dots,a_{n-1}$, donde $a_j = \cos\frac{2\pi j}{n} + i\operatorname{sen}\frac{2\pi j}{n}$. Una* simetría *de P_n es un movimiento rígido que permuta sus vértices, o, lo que es igual, aplica P_n en si mismo. Las simetrías de P_n forman un grupo via la composición, y como el 0 es un punto fijo de cada una, se trata de un subgrupo de $\mathrm{O}(\mathbb{R}^2)$, que evidentemente incluye a D_n. Pero como para cada i, sólo hay 2 simetrías que mandan a_0 en a_i (cada una determinada unívocanmente por la imagen de a_1, que sólo puede ser a_{i+1} o a_{i-1}, donde los índices son tomados módulo n), el grupo de simetrías de P_n es D_n. Para entender mejor este grupo geometricamente, consideremos las rectas L_j $(0 \le j < n)$ que pasan por $(0,0)$ y forman ángulos de $j\pi/n$ radianes con la recta real. Cuando n es impar estas son las rectas que pasan por un vértice y el centro, y cuando es par son las que pasan por dos vértices opuestos y las que unen los puntos medios de lados opuestos de P_n (todas estas también pasan por el centro). Las simetrías respecto de esta rectas son la mitad de los elementos de D_n, y la otra mitad son las rotaciones de ángulo $j\frac{2\pi}{n}$ $(0 \le j < n)$ en el sentido contrario al de la agujas del reloj. Más precisamente, x^j es la rotación de ángulo $j\frac{2\pi}{n}$ y $x^j y$ es la simetría respecto de L_j. Para terminar, notemos que*

- *Los elementos $x^i y$ tienen orden 2,*
- *Los elementos x^i tienen orden $n/(n:i)$. En consecuencia, para cada divisor d de n hay $\phi(d)$ elementos de orden d de la forma x^i, donde ϕ es la función de Euler.*

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

Ejemplo 1.30. *Fijemos una raíz de la unidad $w \in \mathbb{C}$ de orden $2n$, con $n > 1$. 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*

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

Por consiguiente, x e y satisfacen las relaciones $x^n = y^2$ e $yxy^{-1} = x^{-1}$. En consecuencia $x^n = yy^2y^{-1} = yx^ny^{-1} = x^{-n}$ o, lo que es igual, $x^{2n} = 1$. Así, H_n consiste de los $4n$ elementos $1, x\dots, x^{2n-1}, y, xy\dots, x^{2n-1}y$. Es útil observar que:

- *Los elementos $x^i y$ tienen orden 4.*
- *Los elementos x^i tienen orden $2n/(2n:i)$. Debido a esto, para cada divisor d de $2n$ hay $\phi(d)$ elementos de orden d de la forma x^i en H_n.*

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 los subgrupos de G. En particular, todos los subgrupos de G son cíclicos infinitos. En efecto, es claro que $\langle g^n\rangle \ne \langle g^m\rangle$ si $n \ne m$ y que $1 = \langle g^0\rangle$. Fijemos un subgrupo $H \ne 1$ 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 $0 \le r < n_0$, entonces

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

Por lo tanto $r = 0$ y, en consecuencia, $H = \langle g^{n_0} \rangle$.

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 los subgrupos de G. Además, para todo divisor positivo n de $|g|$, el orden de $\langle g^n \rangle$ es $|g|/n$, y si $n \in \mathbb{Z}$ es arbitrario, entonces $\langle g^n \rangle = \langle g^{(|g|:n)} \rangle$ (en particular g^n es un generador de $\langle g \rangle$ si y sólo si n es coprimo con $|g|$). En efecto, tomemos un subgrupo H de G y, como antes, consideremos el mínimo número natural n_0 tal que $g^{n_0} \in H$. Si $g^m \in H$ y $m = n_0 q + r$ con $0 \leq r < n_0$, entonces

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

por lo que $r = 0$ y $H = \langle g^{n_0} \rangle$. De paso, notemos que como $g^{|g|} = 1$, la cuenta anterior implica que n_0 divide a $|g|$. Es evidente ahora que el orden de H es $|g|/n_0$. Tomemos $n \in \mathbb{Z}$ arbitrario. Como 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.

6. Coclases a izquierda y a derecha

Recordemos que dados 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 $l \in L$. Si S es un grupo, entonces escribimos $K^{-1} := \{k^{-1} : k \in K\}$. Es evidente 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 $g \in G$. Decimos que H es un subgrupo de *índice finito* de G si tiene un número finito de coclases a izquierda. En este caso denotamos con $|G : H|$ y llamamos *indice de H en G* a la cantidad de coclases a izquierda de H. Por supuesto, si $K \leq H \leq G$ y K tiene índice finito, entonces H también lo tiene. 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 sus coclases a izquierda. Asimismo, como la aplicación es biyectiva, todas las coclases a izquierda tienen el mismo cardinal. Estos argumentos prueban que vale el siguiente:

TEOREMA 1.31 (Lagrange). *Para cada grupo finito G y cada $H \leq G$, los ordenes de H y G están relacionados por la igualdad*

$$|G| = |G : H||H|, \tag{5}$$

en la cual 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 (5). Más aún, como la aplicación $gH \mapsto Hg^{-1}$ es una función biyectiva del conjunto de las coclases a izquierda de H en el de las coclases a derecha, ambos tienen el mismo cardinal.

El resultado que sigue generaliza la igualdad (5).

TEOREMA 1.32. *Si K y H son subgrupos de un grupo G, $K \subseteq H$ y K tiene índice finito, 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 $j = j'$. □

Corolario 1.33. *Si G es finito, entonces el exponente de G divide al orden de G.*

Demostración. Porque por el Teorema de Lagrange el orden de cada elemento de G divide al orden de G, y el exponente es el mínimo común múltiplo de los órdenes de los elementos de G. □

Corolario 1.34. *Si un grupo tiene orden primo, entonces es cíclico.*

Observación 1.35. *Del Teorema de Lagrange se sigue inmediatamente que 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.

Observación 1.36. *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,*

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

Proposición 1.37. *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 $g = kl \in KL$. □

Ejercicio 1.38. *Pruebe que cada elemento de un cuerpo finito es suma de dos cuadrados.*

Proposición 1.39. *Si H y L son subgrupos de un grupo G y $H \cap L$ tiene índice finito en G, entonces*

$$|H : H \cap L| = |HL : L| \quad \text{y} \quad |G : H \cap L| = |G : H||HL : L|, \tag{6}$$

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

$$|H : H \cap L| \leq |G : L| \quad \text{y} \quad |G : H \cap L| \leq |G : H||G : L|. \tag{7}$$

Demostración. La primera igualdad en (6) vale porque la función

$$\begin{aligned} H/(H\cap L) &\hookrightarrow G/L\,, \\ h(H\cap L) &\longmapsto hL \end{aligned}$$

es inyectiva (pues $hL = h'L$ si y sólo si $h^{-1}h' \in L$, lo que ocurre si y sólo si $h^{-1}h' \in H\cap L$ o, lo que es igual, $h(H\cap L) = h'(H\cap L)$) y porque su imagen es $\{hL : h\in H\}$. La segunda es una consecuencia inmediata de la primera y de que $|G : H\cap L| = |G : H||H : H\cap L|$. □

Corolario 1.40. *Consideremos un grupo G. Para cada par H y L de subgrupos de G, tal que $H\cap L$ tiene índice finito, vale que:*

- *Si $|H : H\cap L| = |G : L|$, entonces $HL = G$.*
- *Si $|G : H\cap L| = |G : H||G : L|$, entonces $|H : H\cap L| = |G : L|$.*

Corolario 1.41. *Consideremos subgrupos H y L de un grupo G. Si $H\cap L$ tiene índice finito en G y HL es un subgrupo de G, entonces*

$$|H : H\cap L||G : HL| = |G : L| \qquad y \qquad |G : H\cap L||G : HL| = |G : H||G : L|.$$

En particular, si $HL = G$, entonces en (7) *valen las igualdades.*

Por último, notemos que si $H\cap L$ tiene índice finito, entonces, como $|G : H|$ y $|G : L|$ dividen a $|G : H\cap L|$, su mínimo común múltiplo también lo divide. En consecuencia, si $|G : H|$ y $|G : L|$ son coprimos,

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

y, por lo tanto, $|G : H||G : L| \le |G : H\cap L|$. Como también vale la desigualdad recíproca, si $|G : H|$ y $|G : L|$ son coprimos, $|G : H\cap L| = |G : H||G : L|$.

7. Productos de subgrupos

Las tres proposiciones de esta sección tratan sobre propiedades del producto de subgrupos. En la primera establecemos las leyes modular y de Dedekind, la segunda da una fórmula para calcular el cardinal de este producto y la tercera da una condición necesaria y suficiente para que dicho producto sea un subgrupo.

Proposición 1.42. *Si $K\le H$ 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 $K\subseteq H$. Así, $K(H\cap L)\subseteq H\cap KL$. 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 1.43. *Si H y L son subgrupos finitos 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

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

No hay duda de que $\{(hy, y^{-1}l) : y \in H \cap L\} \subseteq \varsigma^{-1}(g)$. 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 $y \in H \cap L$. □

Proposición 1.44. *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) ⇒ 2) y 2) ⇒ 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. □

8. 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

$$|G : L| = \sum_{i \in I} |H : H \cap g_iLg_i^{-1}|. \tag{8}$$

Denotemos con $|Hg_iL : L|$ a la cantidad de coclases a izquierda de L incluídas en Hg_iL. Como $|G| = \sum_{i \in I} |Hg_iL|$, y cada coclase a izquierda de L está incluída en un único Hg_iL, para probar la afirmación bastará ver que

$$|Hg_iL : L| = |H : H \cap g_iLg_i^{-1}|,$$

o, lo que es igual, que

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

Pero como H y $g_iLg_i^{-1}$ son subgrupos de G y $|Hg_iL| = |Hg_iLg_i^{-1}|$, por Proposición 1.43

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

como necesitamos. Cuando $L = 1$, la fórmula (8) se reduce a la establecida en el Teorema de Lagrange.

Ejemplo 1.45. *Escribamos* $\mathrm{S}_3 = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$, *donde*

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

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

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

9. Subgrupos normales

Un subgrupo N de un grupo G es *normal* o *invariante* si $gNg^{-1} = N$ para todo $g \in G$. Escribiremos $N \triangleleft G$ o $G \triangleright N$ para señalar que N es un subgrupo normal de G. 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 1.46. *Para cada* $N \le G$ *son equivalentes:*

1. *Dado* $g \in G$ *existe* $h \in G$ *tal que* $gN \subseteq Nh$.
2. *Dado* $g \in G$ *existe* $h \in G$ *tal que* $gNh^{-1} \subseteq N$.
3. *Dado* $g \in G$ *existe* $h \in G$ *tal que* $Ng \subseteq hN$.
4. *Dado* $g \in G$ *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

$$gN \subseteq Nh \quad \text{si y sólo si} \quad gNh^{-1} \subseteq Nhh^{-1} = N.$$

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

Ejercicio 1.47. *Pruebe que un subgrupo* N *de* G *es invariante si y sólo si* $hg \in N$ *siempre que* $gh \in N$.

Observación 1.48. *Si* $N \subseteq L$ *son subgrupos de un grupo* G *y* $N \triangleleft G$, *entonces* $N \triangleleft L$.

Observación 1.49. *Si $N \lhd G$, entonces $NL = LN$ para todo subconjunto L de G. Si además L es un subgrupo de G, entonces NL también lo es. Por último, si $L \lhd G$, entonces $NL \lhd G$.*

El siguiente resultado será mejorado más adelante.

Proposición 1.50. *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,

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

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, dado un 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 (3), 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 1.51. *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 1.49, $G_iG_j = G_jG_i$ para todo $i, j \in I$. □

10. Una caracterización de los grupos cíclicos finitos

Recordemos que 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 el y coprimos con el. 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 $\{0, \dots, p^n - 1\}$ tiene p^n elementos, de los cuales p^{n-1} son múltiplos de p. 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.

Dado un grupo G vamos a denotar con $\operatorname{gen}(G)$ al conjunto de los generadores de G.

LEMA 1.52. *Cada grupo G es la unión*

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

de los generadores de los subgrupos cíclicos C de G.

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

PROPOSICIÓN 1.53. *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, por el lema anterior

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

como queríamos. □

TEOREMA 1.54. *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 1.52 y la Proposición 1.53,

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

donde C recorre el conjunto de los subgrupos cíclicos de G. Por lo tanto, debido a que $|\operatorname{gen}(C)| = \phi(|C|)$, 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 1.55. *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. □

PROPOSICIÓN 1.56. *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 $r \le 2$, pero no lo es si $r > 2$. En este caso*

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

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

DEMOSTRACIÓN. Tomemos $x < p^r$. 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 $r > 1$. En la demostración usaremos que si $p = 2$ e $i > 1$ o si p es un primo impar e $i \geq 1$, entonces

$$y \cong 1 + p^i \pmod{p^{i+1}} \Rightarrow y^p \cong 1 + p^{i+1} \pmod{p^{i+2}}, \tag{9}$$

como puede comprobarse mediante un cálculo sencillo. Una consecuencia inmediata es que cuando p es impar,

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

En particular, $p+1$ tiene orden p^{r-1}. Debido a esto, para concluir la prueba de la primera afirmación será suficiente mostrar que existe $x \in \mathbb{Z}_{p^r}^{\times}$ de orden $p-1$, porque entonces $x(p+1)$ será un generador de $\mathbb{Z}_{p^r}^{\times}$. Pero si $z < p$ tiene orden $p-1$ en $\mathbb{Z}_p$, entonces z es inversible en $\mathbb{Z}_{p^r}$ (puesto que 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 evidente que el grupo de unidades de $\mathbb{Z}_{2^r}$ es cíclico si $r = 2$. Supongamos entonces que $r > 2$. Como $5 = 1 + 2^2$, de (9) se sigue que

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

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

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

y, en consecuencia, es distinto de -1 en $\mathbb{Z}_{2^r}$. Por el Teorema 1.54, 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 a $\{5^i : 0 \leq i < 2^{r-2}\}$ y coincide entonces con $\mathbb{Z}_{2^r}^{\times}$. □

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 $\varphi\colon G \to G'$ 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. El mismo argumento que se usó en el caso de monoides prueba que un morfismo de grupos es un isomorfismo si y sólo si es biyectivo. Mantenemos la notación $G \approx G'$ para señalar que los grupos G y G' son isomorfos. Nuevamente los monomorfismos, epimorfismos, secciones y retracciones son cerrados bajo la composición, toda retracción es sobreyectiva, toda sección inyectiva, todo morfismo sobreyectivo 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 es cierto que un morfismo $\varphi\colon G \to G'$ 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. Por último, es verdad que todo epimorfismo es sobreyectivo, pero esto es mucho más dificil de probar, y lo dejamos para después.

Ejemplo 1.57. *Hay monomorfismos que no son secciones y epimorfismos que no son retracciones. En efecto:*

1. *El morfismo* $j\colon \mathbb{Z}_2 \to \mathbb{Z}_4$*, definido por* $j(0) = 0$ *y* $j(1) = 2$*, es un monomorfismo que 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, dados morfismos $\varphi\colon G \to G'$ y $\psi\colon G' \to G''$,

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 $\operatorname{Hom}(G, G')$, $\operatorname{Iso}(G, G')$, $\operatorname{End} G$ y $\operatorname{Aut} G$ 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 $\operatorname{End} G$ es un monoide (cuyo elemento neutro es la función identidad) vía la composición y $\operatorname{Aut} G$ 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 1.58. *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 1.59. *Dados 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 1.60. *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 1.61. *El determinante* $\det\colon \mathrm{GL}(n,k) \to k^{\times}$ *es un morfismo sobreyectivo de grupos.*

Ejemplo 1.62. *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 1.63. *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 1.64. *La aplicación* $\varsigma\colon \mathbb{C}^{\times} \to \mathbb{R}_{>0}$*, definida por* $\varsigma(x) = |x|$*, es un morfismo sobreyectivo.*

Ejemplo 1.65. *La aplicación* $\varsigma\colon \mathbb{Z}[X] \to \mathbb{Q}_{>0}$, *definida por*

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

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

Ejemplo 1.66. *Fijemos una raíz* $w \in \mathbb{C}$ *de orden* n *de la unidad (por ejemplo, podemos tomar* $w = \cos(2\pi/n) + i\operatorname{sen}(2\pi/n)$*). La aplicación* $\varphi\colon \mathbb{Z}_n \to \mathrm{G}_n$, *definida por* $\varphi(n) = w^n$, *es un isomorfismo de grupos.*

Ejemplo 1.67. *Dado* $n > 1$, *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* $a^n = 1$, $b^2 = 1$ *y* $bab^{-1} = a^{-1}$ *y los* $2n$ *elementos* $1, a \dots, a^{n-1}, b, ab, \dots, a^{n-1}b$ *son todos distintos. En consecuencia, 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 1.28, es un isomorfismo.*

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 1.68. *Si* G' *es abeliano, entonces* $\mathrm{Hom}(G, G')$ *es un grupo abeliano vía* $(\varphi + \psi)(g) := \varphi(g) + \psi(g)$. *El neutro 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 las igualdades

$$\big(\varphi + (\psi + \zeta)\big)(g) = \varphi(g) + \big(\psi(g) + \zeta(g)\big) = \big(\varphi(g) + \psi(g)\big) + \zeta(g) = \big((\varphi + \psi) + \zeta\big)(g)$$

y

$$(\varphi + \psi)(g) = \varphi(g) + \psi(g) = \psi(g) + \varphi(g) = (\psi + \varphi)(g)$$

muestran que

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

Además, de la definición se sigue inmediatamente que

$$\varphi + 0_{GG'} = \varphi \quad \text{para todo } \varphi \in \operatorname{Hom}(G, G').$$

Dejamos al lector la tarea de probar que $-\varphi$ es un morfismo de grupos si $\varphi\colon G \to G'$ lo es, y que $\varphi + (-\varphi) = 0_{GG'}$. □

Observación 1.69. *De la misma manera puede probarse que si M y M' son monoides y M' es abeliano, entonces $\operatorname{Hom}(M, M')$ es un monoide abeliano.*

Proposición 1.70. *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*

$$\varphi_*\colon \operatorname{Hom}(G, G') \to \operatorname{Hom}(H, G') \quad y \quad \psi^*\colon \operatorname{Hom}(G, G') \to Hom(G, H'),$$

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

Demostración. La función $\varphi_*(\alpha)$ es un morfismo de grupos para cada $\alpha \in \operatorname{Hom}(G, G')$, porque los morfismos son cerrados bajo composición. Además,

$$\varphi_*(\alpha + \beta)(g) = (\alpha + \beta)\big(\varphi(g)\big) = \alpha\big(\varphi(g)\big) + \beta\big(\varphi(g)\big) = \varphi_*(\alpha)(g) + \varphi_*(\beta)(g)$$

para todo $\alpha, \beta \in \operatorname{Hom}(G, G')$ y $g \in G$. Esto prueba que la afirmación es verdadera para φ_*, y una cuenta similar demuestra que también lo es para φ^*. □

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 fácil ver que $\ker \varphi \lhd G$ e $\operatorname{Im} \varphi \leq G'$, pero ambos hechos también son consecuencias inmediatas del siguiente resultado.

Proposición 1.71. *La imagen bajo un morfismo de grupos $\varphi\colon G \to G'$, de un subgrupo H de G, es un subgrupo de G', que es normal en $\varphi(G)$ si H es normal en G, y la preimagen de un subgrupo H' de G' es un subgrupo de G, que es normal si lo es H'.*

Demostración. El conjunto $\varphi(H)$ es un subgrupo de G' porque es un conjunto no vacío y

$$\varphi(h)\varphi(l)^{-1} = \varphi(hl^{-1}) \in H \quad \text{para todo } h, l \in H,$$

y es normal en $\varphi(G)$ si H es normal, porque bajo esta hipótesis

$$\varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(ghg^{-1}) \in H \quad \text{para todo } g \in G \text{ y } h \in H.$$

Por otra parte, para ver que $\varphi^{-1}(H')$ es un subgrupo de G es suficiente notar que es no vacío porque $0 \in \varphi^{-1}(H')$ y que si $h, l \in \varphi^{-1}(H')$, entonces

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

Además, si H' es normal y $h \in \varphi^{-1}(H')$, entonces

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} \in H' \quad \text{para todo } g \in G,$$

y, por lo tanto, $\varphi^{-1}(H')$ es normal. □

Observación 1.72. *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*:*

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

$$\begin{tikzcd} H \arrow[r, "\psi"] \arrow[d, "\psi'"] & G \arrow[r, "\varphi"] & G' \\ \ker\varphi \arrow[ur, "\iota"'] & & \end{tikzcd}$$

conmuta.

En efecto, ambas se siguen de inmediato de la definición de núcleo de un morfismo. La primera dice, con otras palabras, que $\varphi(g) = 1$ *para todo* $g \in \ker\varphi$*, y la segunda, que si* $\varphi\circ\psi = 1_{HG'}$*, entonces* $\operatorname{Im}\varphi \subseteq \ker\varphi$*.*

Proposición 1.73. *Si* $\varphi\colon G \to G'$ *es un morfismo de grupos, entonces dos elementos* $g, h \in G$ *tienen la misma imagen bajo* φ *si y sólo si* $g\ker\varphi = h\ker\varphi$*.*

Demostración. En efecto,

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

como afirmamos. □

Corolario 1.74. *Un morfismo de grupos* $\varphi\colon G \to G'$ *es inyectivo si y sólo si* $\ker\varphi = 1$*.*

Ejemplo 1.75. *El núcleo del determinante* $\det\colon \mathrm{GL}(n,k) \to k^\times$ *es el* grupo lineal especial $\mathrm{SL}(n,k)$*.*

Ejemplo 1.76. *El núcleo de la función exponencial*

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

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

Ejemplo 1.77. *El núcleo del morfismo* $\varsigma\colon \mathbb{C}^\times \to \mathbb{R}_{>0}$*, definido por* $\varsigma(x) = |x|$*, es el círculo unidad.*

13. Cocientes de grupos

Consideremos una relación de equivalencia $\simeq$ definida en el conjunto subyacente de un monoide S. Dado $s \in S$ denotemos con $[s]$ a la clase de equivalencia de s en el conjunto cociente $S/\simeq$.

Proposición 1.78. $S/\simeq$ *tiene una (única) estructura de monoide tal que la proyección canónica* $\pi\colon S \to S/\simeq$ *es un morfismo si y sólo si* $\simeq$ *satisface la siguiente condición:*

$$s \simeq s' \text{ y } t \simeq t' \Rightarrow st \simeq s't'. \tag{10}$$

Este monoide es conmutativo si lo es S*.*

Demostración. La definición del producto en $S/\simeq$,

$$[s][s'] = [ss'],$$

esta forzada por el requerimiento de que π sea un morfismo. Esta operación es asociativa porque lo es el producto de S y la función π es sobreyectiva. En efecto, usando estos hechos se ve inmediatamente que

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

para todo $s, s', s'' \in M$. El mismo argumento prueba que el neutro de $S/\simeq$ es la clase $[1]$, del neutro 1 de S, y que $S/\simeq$ es conmutativo si S es conmutativo. $\square$

Notemos que si $s \in S$ es inversible, entonces $[s]$ es inversible y $[s]^{-1} = [s^{-1}]$. 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.

Decimos que una relación de equivalencia $\simeq$, definida sobre un monoide S es *compatible con la estructura de monoide de* S, si satisface la condición (10), requerida en el enunciado de la proposición anterior.

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

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

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

$$\{h \in G : h \simeq g\} = gN = Ng$$

para todo $g \in N$. Recíprocamente, si N es un subgrupo normal de G, entonces por la Proposición 1.46 las relaciones de equivalencia

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

coinciden y son compatibles con la operación de G, porque

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

De ahora en más, dado un 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*. Por ejemplo, $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Recién vimos que el núcleo de $\pi\colon G \to G/N$ es N. En realidad este morfismo es inicial entre aquellos con dominio G, cuyos núcleos incluyen a N. En otras palabras, $\pi\colon G \to G/N$ tiene la siguiente propiedad universal, llamada en forma habitual *propiedad universal del cociente*:

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

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] & G' \\ G/N \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$

conmuta.

Para comprobarlo, notemos que si $g \simeq h$ entonces $gh^{-1} \in N \subseteq \operatorname{Ker}\varphi$, por lo cual $\varphi(g) = \varphi(h)$, lo que permite definir $\bar{\varphi}([g]) = \varphi(g)$. Como $\pi(g) = [g]$, el triángulo conmuta. Adicionalmente, $\bar{\varphi}$ es un morfismo de grupos porque

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

para todo $g, h \in G$.

Observación 1.79. *El núcleo de $\bar{\varphi}$ es $\ker\varphi/N$ y su imagen es la imagen de φ. En particular, $\bar{\varphi}$ 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 $\bar{\varphi}\circ\pi = \varphi$, la clase en G/N de un elemento g de G pertenece a $\ker\bar{\varphi}$ si y sólo si $g \in \ker\varphi$ y, por consiguiente,*

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

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

Demostración. Esto es una consecuencia inmediata de la propiedad universal del cociente y la Observación 1.79. □

Teorema 1.81 (Segundo teorema de isomorfismo). *Si $L \subseteq N$ son subgrupos normales de un grupo G, entonces $N/L \lhd G/L$ y $G/N \approx (G/L)/(N/L)$.*

Demostración. Por la propiedad universal de π_L hay único morfismo $\tilde{\pi}\colon G/L \to G/N$ tal que el triángulo

$$\begin{tikzcd} G \arrow[r, "\pi_N"] \arrow[d, "\pi_L"'] & G/N \\ G/L \arrow[ur, "\tilde{\pi}"'] & \end{tikzcd},$$

donde $\pi_L\colon G \to G/L$ y $\pi_N\colon G \to G/N$ son las proyecciones canónicas, conmuta. Es fácil ver que $\tilde{\pi}$ es sobreyectivo y que $\ker\tilde{\pi} = N/L$. En consecuencia, nuevamente por la propiedad universal del cociente, $\tilde{\pi}$ induce un isomorfismo $\bar{\pi}\colon (G/L)/(N/L) \to G/N$. □

Teorema 1.82 (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 $L/L \cap N \approx NL/N$.*

Demostración. Consideremos el morfismo $\tilde{\iota}\colon L \to G/N$ obtenido componiendo la inclusión canónica $\iota\colon L \to G$ con la proyección canónica $\pi_N\colon G \to G/N$. Por la propiedad universal del cociente sabemos que hay un único monomorfismo $\bar{\iota}\colon L/\ker\tilde{\iota} \to G/N$ tal que el triángulo

$$\begin{tikzcd} L \arrow[r, "\tilde{\iota}"] \arrow[d, "\pi_L"'] & G/N \\ L/\ker\tilde{\iota} \arrow[ur, "\bar{\iota}"'] & \end{tikzcd}$$

conmuta. Es fácil ver que $\ker \tilde{\iota} = L \cap N$ e $\operatorname{Im} \tilde{\iota} = NL/N$. Así, $\bar{\iota}$ induce por correstricción el isomorfismo deseado de $L/L \cap N$ en NL/N. □

TEOREMA 1.83. *Si* $\varphi\colon G \to G'$ *es un morfismo de grupos finitos, 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 1.84. *Consideremos un morfismo de grupos finitos* $\varphi\colon G \to G'$. *Por el Teorema de Lagrange, sabemos que* $|\operatorname{Im} \varphi|$ *divide a* $|G'|$, *y por el Teorema 1.83, que divide a* $|G|$. *Por lo tanto,* $|\operatorname{Im} \varphi|$ *divide a* $(|G| : |G'|)$. *En particular, si* $|G|$ *y* $|G'|$ *son coprimos, entonces* φ *es el morfismo nulo.*

EJEMPLO 1.85. *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. Un elemento $x \in X$ es una *cota inferior* de un subconjunto $Y \subseteq X$ si $x \leq y$ para todo $y \in Y$, y es una *cota superior* si $x \geq y$ para todo $y \in Y$. Decimos que Y es *acotado inferiormente* si tiene cotas inferiores, que es *acotado superiormente* si tiene cotas superiores y que es *acotado* si lo es superior e inferiormente. Un *elemento mínimo* de Y es una cota inferior que pertenece a Y, y un *elemento máximo* es una cota superior que pertenece a Y. Es evidente que cada subconjunto Y de X puede tener a lo sumo un mínimo y un máximo. El *supremo* de una familia $(x_i)_{i\in I}$ de elementos de X, es un elemento $y \in X$, que satisface:

- $x_j \leq y$ para todo $j \in I$,
- Si $x_j \leq x$ para todo $j \in I$, entonces $y \leq x$,

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

- $z \leq x_j$ para todo $j \in I$,
- Si $x \leq x_j$ para todo $j \in I$, entonces $x \leq z$.

Dicho de otro modo, el supremo es una cota inferior máxima y el ínfimo una cota inferior mínima. Si existen, el supremo y el ínfimo de $(x_i)_{i\in I}$ son únicos, y se los denota $\bigvee_{i\in I} x_i$ y $\bigwedge_{i\in I} x_i$, respectivamente. Un conjunto ordenado X es un *reticulado completo* si toda familia de subconjuntos de X tiene supremo e ínfimo. Por ejemplo, el conjunto $\operatorname{Sub}_H G$, 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 $\operatorname{Sub} G$ en lugar de $\operatorname{Sub}_1 G$.

PROPOSICIÓN 1.86. *Para cada conjunto ordenado* X *son equivalentes:*

1. X *es un reticulado completo.*
2. *Toda familia de elementos de* X *tiene supremo.*
3. *Toda familia de elementos de* X *tiene ínfimo.*

Demostración. Es claro que 1) ⇒ 2) y 1) ⇒ 3). Veamos que 2) ⇒ 1). Notemos primero que el supremo de la familia vacía es el mínimo de X. En consecuencia toda familia $(x_i)_{i\in I}$ de elementos de X tiene cotas inferiores. Es fácil ver ahora que el supremo de las cotas inferiores de los x_i's es el ínfimo de $(x_i)_{i\in I}$. Un razonamiento similar prueba que 3) ⇒ 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:

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

El reticulado completo X es el dominio, e Y el codominio. Las condiciones pedidas son redundantes. De hecho, cualquiera de las dos últimas implican la primera. Por ejemplo, supongamos que vale la segunda y que $x_1 \le x_2$. Entonces

$$f(x_2) = f(x_1 \vee x_2) = f(x_1) \vee f(x_2),$$

y, por lo tanto, $f(x_1) \le f(x_2)$. 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 $f\circ f^{-1} = \mathrm{id}_{X'}$.

Proposición 1.87. *Si X e Y son reticulados completos y $f\colon X \to Y$ es una función creciente biyectiva que preserva supremos o ínfimos, entonces f es un isomorfismo.*

Demostración. Supongamos que $f\colon X \to Y$ preserva supremos. Entonces

$$f^{-1}\Big(\bigvee_{j\in J} y_j\Big) = \bigvee_{j\in J} f^{-1}(y_j)$$

para cada familia $(y_j)_{j\in J}$ de elementos de Y, porque

$$f\left(f^{-1}\left(\bigvee_{j\in J} y_j\right)\right) = \bigvee_{j\in J} y_j = \bigvee_{j\in J} f\big(f^{-1}(y_j)\big) = f\left(\bigvee_{j\in J} f^{-1}(y_j)\right).$$

Así, f y f^{-1} son funciones crecientes y biyectivas que preservan supremos. Pero entonces también preservan ínfimos, porque el ínfimo de cada familia de elementos de un reticulado completo es el supremo de las cotas inferiores. El caso en que f preserva ínfimos se puede tratar en forma similar, o deducir del anterior reemplazando los órdenes dados por los opuestos (definidos por $z \preceq z'$ si $z' \le z$), tanto en X como en Y. □

Ejercicio 1.88. *Exhiba reticulados X e Y y una función biyectiva $f\colon X \to Y$, que preserva el orden y no es un isomorfismo.*

Volvamos a nuestro asunto principal, que en este momento es la teoría de grupos.

Teorema 1.89 (Teorema de la correspondencia). *Si $\varphi\colon G \to G'$ es un morfismo sobreyectivo de grupos, entonces las funciones*

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

son isomorfismos de reticulados, inversos uno del otro. Esta correspondencia tiene las siguientes propiedades: para cada $H, L \in \mathrm{Sub}_{\ker\varphi} G$ con $H \le L$,

- *Si H tiene índice finito en L, entonces $\varphi(H)$ es un subgrupo de índice finito de $\varphi(L)$ y $|L:H| = |\varphi(L):\varphi(H)|$,*
- *$H \triangleleft L$ si y sólo si $\varphi(H) \triangleleft \varphi(L)$, y entonces $L/H \approx \varphi(L)/\varphi(H)$.*

Demostración. Es claro que si $\ker\varphi \le H \le L$, entonces $\varphi(H) \le \varphi(L)$. Como φ es sobreyectiva,

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

para todo subconjunto H' de G'. Adicionalmente,

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

para cada $H \le G$, 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 $g \in G$. Además la segunda de las aplicaciones preserva ínfimos porque tomar imagen inversa se comporta bien con intersecciones. Por la Proposición 1.87, esto es suficiente para probar que vale la primera afirmación.

Para concluir que si $\ker\varphi \le H \le L$ y H tiene índice finito en L, entonces vale la igualdad $|L:H| = |\varphi(L):\varphi(H)|$, es suficiente probar que la correspondencia $lH \mapsto \varphi(l)H$, 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

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

Finalmente, los resultados obtenidos al comienzo de la Sección 12 muestran en particular que $H \triangleleft L$ si y sólo si $\varphi(H) \triangleleft \varphi(L)$ y, por la propiedad universal de cociente y el Segundo teorema del isomorfismo,

$$\frac{\varphi(L)}{\varphi(H)} \approx \frac{L/\ker\varphi}{H/\ker\varphi} \approx \frac{L}{H},$$

como deseamos. □

Definición 1.90. *Un grupo G es* simple *si $G \neq 1$ y $H \triangleleft G \Rightarrow H = 1$ o $H = G$.*

Definición 1.91. *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 1.92. *$H \triangleleft G$ 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 $\bar\varphi\colon G/H \to G'/H'$ tal que el cuadrado

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] & G' \arrow[d, "\pi'"] \\ G/H \arrow[r, "\bar\varphi"] & G'/H', \end{tikzcd}$$

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 entonces se deduce de inmediato que

$$\operatorname{Im}\bar\varphi = \pi'(\operatorname{Im}\varphi) \qquad \text{y} \qquad \ker\bar\varphi = \varphi^{-1}(H')/H.$$

Proposición 1.93. *La construcción anterior tiene las siguientes propiedades:*

1. *Para todo $H \triangleleft G$, 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

$$\begin{tikzcd} G \arrow[r, "\mathrm{id}"] \arrow[d, "\pi"] & G \arrow[d, "\pi"] \\ G/H \arrow[r, "\mathrm{id}"] & G/H \end{tikzcd}$$

y el rectángulo exterior del diagrama

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] & G' \arrow[r, "\psi"] \arrow[d, "\pi'"] & G'' \arrow[d, "\pi''"] \\ G/H \arrow[r, "\bar{\varphi}"] & G'/H' \arrow[r, "\bar{\psi}"] & G''/H'' \end{tikzcd}$$

conmutan. □

Ejercicio 1.94. *Pruebe que si $\varphi\colon G \to G'$ es un morfismo de grupos y $H' \triangleleft G'$, entonces $\varphi^{-1}(H') \triangleleft G$ y existe un único morfismo inyectivo $\bar{\varphi}\colon G/\varphi^{-1}(H') \to G'/H'$ de grupos, tal que el diagrama*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] & G' \arrow[d, "\pi'"] \\ G/\varphi^{-1}(H') \arrow[r, "\bar{\varphi}"] & G'/H', \end{tikzcd}$$

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

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 diedral y cuaterniónico. Para ello necesitamos primero introducir los grupos libres, los cuales, a grosso 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

Dado un 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

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

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 proximo objetivo será definir el *producto* w_1w_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

$$x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n} x_{\beta_1}^{\delta_1} \cdots x_{\beta_m}^{\delta_m}. \tag{11}$$

Si esta es una palabra reducida, entonces ponemos

$$w_1w_2 := x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n} x_{\beta_1}^{\delta_1} \cdots x_{\beta_m}^{\delta_m}.$$

Si no, primero eliminamos de (11) sucesivamente pares de símbolos asociados, hasta obtener una que lo sea.

Teorema 1.95. *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

$$w_1(w_2w_3) = (w_1w_2)w_3$$

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 $l(w_2) \le n$ 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 1.96. *Dada una 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*

$$\begin{tikzcd} X \arrow[r, "j"] \arrow[d, "\iota"] & G \\ L(X) \arrow[ur, "\varphi"'] & \end{tikzcd}$$

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 1.96, 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 1.97. *Si (G,j) es un grupo libre sobre X, $l\colon Y\to X$ es una función biyectiva 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 1.98. *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 único morfismo $\varphi\colon L(X)\to G$ tal que $\varphi\circ\iota = j$, es un isomorfismo. En consecuencia, j es inyectivo.*

DEMOSTRACIÓN. Por la Observación 1.97, sabemos que si φ es un isomorfismo, entonces (G,j) también lo es. Recíprocamente, si (G,j) es libre, entonces hay un único morfismo $\psi\colon G\to L(X)$ tal que el triángulo

$$\begin{tikzcd} X \arrow[r, "j"] \arrow[d, "\iota"] & G \arrow[dl, "\psi"] \\ L(X) & \end{tikzcd}$$

conmuta. Como $\psi\circ\varphi\circ\iota = \iota$ y $\varphi\circ\psi\circ j = j$, por las propiedades universales de $(L(X),\iota)$ y (G,j), debe ser $\psi\circ\varphi = \mathrm{id}_{L(X)}$ y $\varphi\circ\psi = \mathrm{id}_G$. □

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, es un grupo libre. Por la Proposición 1.98, esto ocurre si y sólo si el morfismo de $L(X)$ en G inducido por ι_X es biyectivo. Un argumento sencillo muestra que si un par (G,j) es libre, entonces $\operatorname{Im} j$ es una base de G. Así, un grupo tiene una base si y sólo si existen un conjunto X y una función $j\colon X\to G$ tales que (G,j) es libre. El siguiente teorema será probado más adelante.

Teorema 1.99. *Dos grupos libres $L(X)$ y $L(Y)$ son isomorfos si y sólo si $|X| = |Y|$. Equivalentemente, todos 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 1.100. *Todo grupo es isomorfo a un cociente de un grupo libre.*

Demostración. Dado un conjunto de generadores X de G, el único morfismo

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

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

14.2. Presentaciones

Dado un cociente $G = L(X)/N$, 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 1.100, 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 $\langle x_1,\dots,x_n|p_1,\dots,p_m\rangle$ en lugar de $\langle\{x_1,\dots,x_n\}|\{p_1,\dots,p_m\}\rangle$. Si $G = \langle x_1,\dots,x_n|p_1,\dots,p_m\rangle$, entonces también decimos que G es el *grupo con generadores $x_1,\dots,x_n$ sujetos a las relaciones $p_1 = 1,\dots,p_m = 1$*. Recordemos que dados un grupo cociente G/N de un grupo G y un elemento $g \in G$, el símbolo $[g]$ denota a la clase de g en G/N.

Ejemplo 1.101. $\langle x|\emptyset\rangle \approx \mathbb{Z}$.

Ejemplo 1.102. *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. Como 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 1.103. *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 $(0,1)$. Como

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

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

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

En particular, $|\langle x_1, x_2 | x_1^{n_1}, x_2^{n_2}, x_1x_2x_1^{-1}x_2^{-1}\rangle| \le n_1n_2$. *Como* p *es un morfismo sobreyectivo y* $|\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}| = n_1n_2$, *esto implica que* $\langle x_1, x_2 | x_1^{n_1}, x_2^{n_2}, x_1x_2x_1^{-1}x_2^{-1}\rangle \approx \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$.

Ejemplo 1.104. *Recordemos para cada* $n > 1$, *el grupo diedral* D_n *es el subgrupo de* $\mathrm{GL}(2,\mathbb{R})$ *generado por las matrices*

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

donde $\theta = 2\pi/n$. *En el Ejemplo 1.28 vimos que* x *e* y *satisfacen las relaciones* $x^n = 1$, $y^2 = 1$ *e* $yxy^{-1} = x^{-1}$. *Por lo tanto 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*

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

En particular,

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

Como $|D_n| = 2n$ *y* p *es sobreyectivo, esto implica que* $\langle x_1, x_2 | x_1^n, x_2^2, x_2x_1x_2^{-1}x_1\rangle \approx D_n$.

Ejemplo 1.105. *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 *es una raíz de la unidad de orden* $2n$. *Como* $x^n = y^2$ *e* $yxy^{-1} = x^{-1}$, *hay un único morfismo*

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

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 1.30, se comprueba que $[x_1]^{2n} = 1$. *En consecuencia, 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*

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

y, por lo tanto,

$$|\langle x_1, x_2 | x_1^n x_2^{-2}, x_2x_1x_2^{-1}x_1\rangle| \le 4n.$$

Así, como $|H_n| = 4n$ *y el morfismo* p *es sobreyectivo,* $\langle x_1, x_2 | x_1^n x_2^{-2}, x_2x_1x_2^{-1}x_1\rangle \approx H_n$.

Observación 1.106. *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* $2n$ *con dos generadores* x, y *que satisfacen* $x^n = 1$, $y^2 = 1$ *e* $yxy^{-1} = x^{-1}$ *es isomorfo a* $\langle x_1, x_2 | x_1^n, x_2^2, x_2x_1x_2^{-1}x_1\rangle$, *y todo grupo de orden* $4n$ *con dos generadores* x, y *que satisfacen* $x^n = y^2$ *e* $yxy^{-1} = x^{-1}$ *es isomorfo a* $\langle x_1, x_2 | x_1^n x_2^{-2}, x_2x_1x_2^{-1}x_1\rangle$.

EJEMPLO 1.107. *Volviendo al Ejemplo 1.104, el subgrupo $\langle x^r\rangle$ de D_n es normal para todo r. 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

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

Si r divide a n, entonces el cociente $D_n/\langle x^r\rangle$ tiene orden $2r$ y es trivial que tiene generadores $[x],[y]$ que satisfacen las relaciones $[x]^r = 1$, $[y]^2 = 1$ e $[y][x][y]^{-1} = [x]^{-1}$. Por lo tanto es isomorfo a D_r.

EJEMPLO 1.108. *Razonando como en el ejemplo anterior se comprueba que el subgrupo $\langle x^r\rangle$ del grupo cuaterniónico generalizado H_n es normal para todo r, y que si $r|n$, entonces $H_n/\langle x^r\rangle \approx D_r$.*

OBSERVACIÓN 1.109 (Descripción de Conjuntos de morfismos). *Por el Teorema 1.96, para cada grupo G y cada conjunto X, la aplicación*

$$\theta\colon \operatorname{Hom}(L(X), G) \to G^X, \tag{12}$$

que cada morfismo φ le asigna su restricción $\varphi_{|X}$ a X, es biyectiva. Por ejemplo, como los grupos cíclicos infinitos son libres, y cada uno de sus generadores mónicos es una base, si $\langle x\rangle$ es un grupo cíclico infinito, entonces

$$\theta\colon \operatorname{Hom}(\langle x\rangle, G) \to G^{\{x\}} \approx G,$$

es la función biyectiva dada por $\theta(\varphi) = \varphi(x)$.

Consideremos ahora el caso, más general, en el que el dominio es un grupo $\langle X|R\rangle$, dado por una presentación. Recordemos que $\langle X|R\rangle$ es el cociente $L(X)/\overline{\langle R\rangle}$, del grupo libre $L(X)$ por el subgrupo normal generado por X, y denotemos con π a la proyección canónica de $L(X)$ sobre $\langle X|R\rangle$. Cada morfismo de grupos

$$\varphi\colon \langle X|R\rangle \to G,$$

determina, por composición, un morfismo $\pi^*(\varphi)\colon L(X) \to G$. Por supuesto, salvo cuando $R = 1$, no todo morfismo $\psi\colon L(X) \to G$ es de este tipo. Para que lo sea es necesario y suficiente que se anule sobre $\overline{\langle R\rangle}$, o, lo que es igual, sobre R. Así, la imagen de la función

$$\pi^*\colon \operatorname{Hom}\big(\langle X|R\rangle, G\big) \to \operatorname{Hom}\big(L(X), G\big),$$

es el conjunto de los morfismos de $L(X)$ en G, que se anulan en R. Además, es evidente que π^* es una aplicación inyectiva. Componiendo π^* con la biyección eqnu5 introducida antes, obtenemos una función inyectiva

$$\bar\theta\colon \operatorname{Hom}(\langle X|R\rangle, G) \to G^X,$$

cuya imagen es el conjunto de las funciones $h\colon X \to G$, tales que para cada $r \in R$, reemplazando en r cada $x \in X$ por $h(x)$, se obtiene el elemento neutro de G. Por último un cálculo directo muestra que $\bar\theta(f)(x) = f([x])$. Antes de dar agunos ejemplos notemos que este razonamiento se aplica perfectamente a morfismos cuyo dominio es un grupo arbitrario H, siempre y cuando dispongamos de una presentación de H. Esto es, de un isomorfismo explícito $\langle X|R\rangle \approx H$. Por ejemplo, si $\langle x\rangle$ es un grupo cíclico de orden n, entonces

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

Similarmente,

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

y

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

Terminamos este apartado dando otra caracterización de los grupos diedrales.

TEOREMA 1.110. *Si G es un grupo finito y $x, y \in G$ tienen orden 2, entonces $\langle x, y\rangle \approx D_n$, donde n es el orden de yx.*

DEMOSTRACIÓN. Escribamos $s = yx$. Por la Observación 1.106, como

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

basta probar que $|\langle x, y\rangle| = 2n$ o, equivalentemente, que $\langle s\rangle$ es un subgrupo propio de $\langle x, y\rangle$ y $\langle x, y\rangle = \langle s\rangle \cup y\langle s\rangle$. Lo primero es un consecuencia inmediata de que un grupo cíclico no puede tener dos elementos de orden 2. Como $\langle s\rangle \cup y\langle s\rangle \subseteq \langle x, y\rangle$ y $x, y \in y\langle s\rangle$, para probar lo último es suficiente ver que $\langle s\rangle \cup y\langle s\rangle$ es un grupo. Pero esto es cierto porque claramente

$$ys^is^j = ys^{i+j},$$

porque un cálculo directo, en el que se usa que $y^2 = 1$ para probar la segunda igualdad, y que $xy = s^{-1}$ para probar la tercera, muestra que

$$ys^iys^j = y(yx)^iys^j = (xy)^is^j = s^{-i}s^j = s^{j-i},$$

y porque

$$s^iys^j = y^2s^iys^j = ys^{j-i}$$

debido a que $y^2 = 1$ e $ys = s^{-1}y$. □

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 las relaciones con el producto directo interno.

15.1. Producto directo interno

Dado un grupo G y subgrupos $G_1, \dots, G_n$ de G, decimos que G es *producto directo interno de* $G_1, \dots, G_n$ si cada $g \in G$ se escribe de manera única como un producto

$$g = g_1 \cdots g_n$$

con $g_1 \in G_1, \dots, g_n \in G_n$ (en particular $G = G_1 \cdots G_n$) y

$$(g_1 \cdots g_n)(g_1' \cdots g_n') = g_1g_1' \cdots g_ng_n' \tag{13}$$

para todo $g_1, g_1' \in G_1, \dots, g_n, g_n' \in G_n$. Es claro que si G es producto directo interno de $G_1, \cdots, G_n$ entonces $g_ig_j = g_jg_i$ para cada $g_i \in G_i$ y $g_j \in G_j$, con $i \neq j$. En consecuencia G es producto directo interno de $G_{\sigma_1}, \dots, G_{\sigma_n}$ para todo $\sigma \in \mathrm{S}_n$ y $G_i \triangleleft G$ para todo i. Notemos también que las inclusiones canónicas $\iota_i\colon G_i \to G$ y las aplicaciones $\pi_i\colon G \to G_i$, 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 1.111. *Consideremos un grupo G y subgrupos normales $G_1,\dots,G_n$ de G tales que $G = G_1\cdots G_n$. Por brevedad, denotemos con $G_{\hat{\imath}}$ a $G_1\cdots\widehat{G_i}\cdots G_n$. Son equivalentes:*

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

Demostración. 1) $\Rightarrow$ 2) Por 1), sabemos que todo elemento $g \in G$ se escribe de manera única en la forma $g = g_1\cdots g_n$, con $g_i \in G$. Si $g \in G_{\hat{\imath}}$, entonces $g_i = 1$, y si esto es cierto para todo i, entonces $g = 1$.

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

3) $\Rightarrow$ 4) Porque $G_1\cdots G_{i-1} \subseteq G_{\hat{\imath}}$.

4) $\Rightarrow$ 5) Supongamos que el item 5) es falso. Entonces hay un mínimo $j > 1$ tal que existen $g_1 \in G_1,\cdots,g_j \in G_j$ con $g_j^{-1} = g_1\cdots g_{j-1} \neq 1$. Pero esto contradice 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 $1 = xx^{-1} \in G_iG_j$, debido a lo cual, por hipótesis, $x = 1$. Notemos ahora que $g_ig_j = g_jg_i$ para cada $g_i \in G_i$ y $g_j \in G_j$ con $i \neq j$, porque

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

Pero entonces

$$g_1\cdots g_n = h_1\cdots h_n \Rightarrow g_1h_1^{-1}\cdots g_nh_n^{-1} = 1 \Rightarrow g_1 = h_1,\dots,g_n = h_n$$

para todo $g_1,h_1 \in G_1,\dots,g_n,h_n \in G_n$, y además, la multiplicación de G está dada por la fórmula (13). □

15.2. Producto directo

Dada una familia de grupos $(G_i)_{i\in I}$, el producto directo $\prod_{i\in I} G_i$ es un grupo, llamado *producto directo de* $(G_i)_{i\in I}$, vía la multiplicación coordenada a coordenada. Esta operación está definida adrede para que las proyecciones canónicas $\pi_j\colon \prod_{i\in I} G_i \to G_j$ $(j \in I)$ 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:

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

(14)
$$\begin{tikzcd} G \arrow[d, "\overrightarrow{(\varphi_i)}"'] \arrow[dr, "\varphi_j"] & \\ \prod G_i \arrow[r, "\pi_j"] & G_j \end{tikzcd}$$

conmuta.

En efecto, el requisito de que los diagramas (14) conmuten, sólo lo satisface la función $\overrightarrow{(\varphi_i)}$ definida por
$$\overrightarrow{(\varphi_i)}(g) := (\varphi_i(g))_{i\in I},$$
y un cálculo directo muestra que esta función es un morfismo de grupos. Notemos asimismo que $\ker \overrightarrow{(\varphi_i)} = \bigcap \ker \varphi_i$.

Observación 1.112. *Una manera equivalente de formular la propiedad universal anterior es diciendo que para cada grupo G la correspondencia*
$$\begin{aligned} \operatorname{Hom}(G, \textstyle\prod G_i) &\xrightarrow{\Psi} \textstyle\prod \operatorname{Hom}(G, G_i) \\ \varphi &\longmapsto (\pi_i \circ \varphi)_{i\in I} \end{aligned}$$
es biyectiva. Es fácil ver que si los G_i's son conmutativos, entonces Ψ también es un morfismo de grupos.

Observación 1.113. *Consideremos subgrupos normales $G_1, \dots, G_n$ de un grupo G. Como en el Teorema 1.111, escribamos $G_{\hat{\imath}} = G_1 \cdots \widehat{G_i} \cdots G_n$. Por la propiedad universal del producto, las proyecciones canónicas $\pi_{\hat{\imath}}\colon G \to G/G_{\hat{\imath}}$ inducen un morfismo*
$$G \xrightarrow{\overrightarrow{(\pi_{\hat{1}},\dots,\pi_{\hat{n}})}} G/G_{\hat{1}} \times \cdots \times G/G_{\hat{n}}\ ,$$
cuyo núcleo es $\bigcap_{i=1}^n G_{\hat{\imath}}$. Afirmamos que $\overrightarrow{(\pi_{\hat{1}}, \dots, \pi_{\hat{n}})}$ es sobreyectivo si y sólo si $G_1 \cdots G_n = G$. En efecto, si se satisface esta condición, entonces dado $([g_1], \dots, [g_n]) \in G/G_{\hat{1}} \times \cdots \times G/G_{\hat{n}}$, existen $g_{ij} \in G_i$ $(1 \le i, j \le n)$ tales que $g_i = g_{1i} \cdots g_{ni}$ para todo i. En consecuencia,
$$\overrightarrow{(\pi_{\hat{1}}, \dots, \pi_{\hat{n}})}(g_{11} \cdots g_{nn}) = (\pi_{\hat{1}}(g_{11}), \dots, \pi_{\hat{n}}(g_{nn})) = ([g_1], \dots, [g_n]),$$
porque
$$\pi_{\hat{1}}(g_{ii}) = \pi_{\hat{\imath}}(g_{1i} \cdots g_{ni}) = [g_i] \quad \text{para todo } i.$$
Recíprocamente, si $\overrightarrow{(\pi_{\hat{1}}, \dots, \pi_{\hat{n}})}$ es sobreyectivo, entonces dado $g \in G$ hay un $x \in G$ tal que
$$\overrightarrow{(\pi_{\hat{1}}, \dots, \pi_{\hat{n}})}(x) = ([g], 1, \cdots, 1).$$
En particular $xg^{-1} \in G_{\hat{1}}$ y $x \in G_{\hat{2}}$ y, por lo tanto, existen
$$g_2 \in G_2, \dots, g_n \in G_n \quad y \quad g'_1 \in G_1, g'_3 \in G_3, \dots, g'_n \in G_n$$
tales que $g = xg_2 \cdots g_n$ 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 $G_i G_j = G_j G_i$ para todo i, j, debido a la Observación 1.49.

COROLARIO 1.114. $\overrightarrow{(\pi_{\widehat{1}}, \dots, \pi_{\widehat{n}})}$ *es un isomorfismo si y sólo si G es producto directo interno de $G_1, \dots, G_n$.*

DEMOSTRACIÓN. Esto es una consecuencia inmediata del Teorema 1.111 y la Observación 1.113. □

PROPOSICIÓN 1.115. *Dada una familia $(\varphi_i \colon H_i \to G_i)_{i \in I}$ de morfismos de grupos, existe un único morfismo*

$$\prod_{i \in I} \varphi_i \colon \prod H_i \to \prod G_i$$

tal que los diagramas

$$\begin{tikzcd} \prod H_i \arrow[r, "\prod \varphi_i"] \arrow[d, "\pi_j"] & \prod G_i \arrow[d, "\pi_j"] \\ H_j \arrow[r, "\varphi_j"] & G_j \end{tikzcd} \qquad (j \in I)$$

conmutan.

DEMOSTRACIÓN. Por la propiedad universal de $\prod G_i$ los morfismos $\varphi_j \circ \pi_j$ inducen la flecha $\prod \varphi_i$ requerida, y esta es única. □

Es fácil ver que

$$(15) \quad \Big(\prod \varphi_i\Big)((h_i)_{i \in I}) = (\varphi_i(h_i))_{i \in I}, \quad \ker\Big(\prod \varphi_i\Big) = \prod \ker \varphi_i \quad \text{e} \quad \operatorname{Im}\Big(\prod \varphi_i\Big) = \prod \operatorname{Im} \varphi_i.$$

OBSERVACIÓN 1.116. *La correspondencia introducida en la Proposición 1.115 tiene las siguientes propiedades:*

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

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

Esto puede comprobarse mediante un cálculo directo usando la fórmula (15), *o argumentando como en la Proposición 1.93.*

OBSERVACIÓN 1.117. *Por la Proposición 1.115, sabemos que dados una familia $(G_i)_{i \in I}$ de grupos y subgrupos normales $H_i \triangleleft G_i$, las proyecciones canónicas $\pi_i \colon G_i \to G_i/H_i$ inducen un morfismo sobreyectivo*

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

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

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

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:

$$\bigsqcup G_i := \left\{ g = (g_i)_{i \in I} \in \prod G_i : g_i = 1 \text{ salvo para finitos índices } i \in I \right\}.$$

Así, $\bigsqcup G_i = \prod G_i$ si y sólo si i es finito. 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

- $\pi_i(\iota_i(g)) = g$ para todo $i \in I$ y $g \in G_i$,
- $\iota_i(g_i)\iota_j(g_j) = \iota_j(g_j)\iota_i(g_i)$ para todo $i, j \in I$ con $i \neq j$, $g_i \in G_i$ 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:

- Dada una familia morfismos de grupos $(\varphi_i \colon G_i \to G)_{i \in I}$ con la propiedad de que para todo $i, j \in I$ con $i \neq j$,

  $$\varphi_i(g_i)\varphi_j(g_j) = \varphi_j(g_j)\varphi_i(g_i) \text{ para cada } g_i \in G_i \text{ y } g_j \in G_j,$$

  existe un único morfismo de grupos $\overleftarrow{(\varphi_i)}_{i \in I} \colon \bigsqcup G_i \to G$, tal que para cada $j \in I$ el diagrama

  $$\begin{tikzcd} & G \\ G_j \arrow[ur, "\varphi_j"] \arrow[r, "\iota_j"] & \bigsqcup G_i \arrow[u, "\overleftarrow{(\varphi_i)}"'] \end{tikzcd}$$

  conmuta.

En efecto, si $\overleftarrow{(\varphi_i)}$ existe, entonces forzosamente

$$\overleftarrow{(\varphi_i)}(g) = \overleftarrow{(\varphi_i)} \left(\prod \iota_j \circ \pi_j(g) \right) = \prod \overleftarrow{(\varphi_i)}(\iota_j \circ \pi_j(g)) = \prod \varphi_j(\pi_j(g)),$$

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

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

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

$$\overleftarrow{(\varphi_i)}{\circ}\iota_j(g) = \prod \varphi_i(\pi_i{\circ}\iota_j(g)) = \varphi_j(g)$$

para cada $g \in G_j$.

Observación 1.118. *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, además, en este caso, es un isomorfismo de grupos.

Proposición 1.119. *Dada una 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

$$\begin{tikzcd} H_j \arrow[r, "\varphi_j"] \arrow[d, "\iota_j"] & G_j \arrow[d, "\iota_j"] \\ \bigsqcup H_i \arrow[r, "\bigsqcup \varphi_i"] & \bigsqcup G_i \end{tikzcd}$$

conmutan.

Demostración. Por la propiedad universal de $\bigsqcup H_i$ los morfismos $\iota_j{\circ}\varphi_j$ inducen la flecha requerida, y esta es única. □

Es obvio que $\big(\bigsqcup \varphi_i\big)((g_i)_{i\in I}) = (\varphi_i(g_i))_{i\in I}$, $\ker\big(\bigsqcup \varphi_i\big) = \bigsqcup \ker \varphi_i$ e $\operatorname{Im}\big(\bigsqcup \varphi_i\big) = \bigsqcup \operatorname{Im} \varphi_i$.

Observación 1.120. *La correspondencia introducida en la Proposición 1.119 tiene las siguientes propiedades:*

1. $\bigsqcup \mathrm{id}_{H_i} = \mathrm{id}_{\bigsqcup H_i}$.

2. *Dadas 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 1.121. *Si* $H_i \lhd G_i$ *para todo* $i \in I$, *entonces las proyecciones canónicas* $\pi_i\colon G_i \to G_i/H_i$ *inducen un morfismo sobreyectivo*

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

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

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

EJERCICIO 1.122. *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 múltiplo común de los ordenes de sus coordenadas.*

OBSERVACIÓN 1.123. *Supongamos que* $G_1,\dots,G_n$ *son subgrupos de un grupo* G *y que los elementos de* G_i *conmutan con los de* G_j *siempre que* $i \neq j$. *Entonces la función*

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

es un morfismo de grupos. Recíprocamente, si ς *es un morfismo de grupos, entonces*

$$gh = \varsigma\big(\iota_i(g)\big)\varsigma\big(\iota_j(h)\big) = \varsigma\big(\iota_i(g)\iota_j(h)\big) = \varsigma\big(\iota_j(h)\iota_i(g)\big) = \varsigma\big(\iota_j(h)\big)\varsigma\big(\iota_i(g)\big) = hg$$

para todo $g \in G_i$ *y* $h \in G_j$, *con* $i \neq j$. *Es obvio que* $\operatorname{Im}\varsigma = G_1\cdots G_n$, *y que si es un morfismo de grupos, entonces*

$$\ker\varsigma = \{(g_1,\dots,g_n) \in G_1 \times \cdots \times G_n : g_1\cdots g_n = 1\}.$$

PROPOSICIÓN 1.124. *Si* $G_1,\dots,G_n$ *son subgrupos de* G, *entonces son equivalentes:*

1. $G_1\cdots G_n$ *es un subgrupo de* G *y es producto directo interno de* $G_1,\dots,G_n$.
2. *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.*

DEMOSTRACIÓN. Si se satisfacen las condiciones del item 1), entonces para cada par de índices i y j distintos, los elementos de G_i conmutan con los de G_j. En consecuencia, la función ς definida en la Observación 1.123 es un morfismo, que además es inyectiva por la definición de producto directo interno y la caracterización de $\ker\varsigma$ dada en la misma observación. Recíprocamente, si ς es un morfismo inyectivo, entonces cada $g \in G_1\cdots G_n$ se escribe de manera única como producto

$$g = g_1\cdots g_n \quad \text{con } g_i \in G_i,$$

y la multiplicación de dos elementos de este tipo está dada por

$$(g_1\cdots g_n)(g_1'\cdots g_n') = \varsigma(g_1,\cdots,g_n)\varsigma(g_1',\dots,g_n') = \varsigma(g_1g_1',\dots,g_ng_n') = g_1g_1'\cdots g_ng_n',$$

que son las condiciones requeridas en la definición de producto directo interno. □

Bajo las hipótesis de la Proposición 1.124, es evidente que ς es un isomorfismo si y sólo si G es producto directo interno de $G_1,\dots,G_n$. En este caso la composición $\overrightarrow{(\pi_{\hat{1}},\dots,\pi_{\hat{n}})}\circ\varsigma$, del isomorfismo $\overrightarrow{(\pi_{\hat{1}},\dots,\pi_{\hat{n}})}$ introducido en la Observación 1.113, con ς, identifica al subgrupo $\iota_i(G_i)$ de $G_1\times\cdots\times G_n$ con el subgrupo $\iota_i(G/G_{\hat{i}})$ de $(G/G_{\hat{1}})\times\cdots\times(G/G_{\hat{n}})$.

COROLARIO 1.125. *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. Por la Proposición 1.43 sabemos que

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

y, por lo tanto, es coprimo con $|G_i|$. En consecuencia $G_i\cap(G_1\cdots G_{i-1})=1$. Por los Teoremas 1.111 y 1.124, esto implica que el morfismo ς es inyectivo. Ahora es obvio que es sobreyectivo si y sólo si $|G|=|G_1|\cdots|G_n|$. □

COROLARIO 1.126. *La función $\phi\colon\mathbb{N}\to\mathbb{N}$ de Euler tiene la siguiente propiedad: 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 1.125, la aplicación

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

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 1.127. *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 $G\approx H\times L$.*

15.4. Morfismos entre productos directos finitos de grupos

Para cada par $\mathbf{H}=(H_1,\dots,H_r)$ y $\mathbf{K}=(K_1,\dots,K_s)$ de familias finitas de grupos, denotamos con el símbolo $\mathrm{M}_{s\times r}\bigl(\mathrm{Hom}(\mathbf{H},\mathbf{K})\bigr)$ 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

$$\varsigma_{ij}(h)\varsigma_{ij'}(h')=\varsigma_{ij'}(h')\varsigma_{ij}(h)$$

para todo i, $j<j'$, $h\in H_j$ y $h'\in H_{j'}$.

Proposición 1.128. *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

$$\theta(\varsigma_{ij})(h_1,\dots,h_r) = \Big(\prod_l \varsigma_{1l}(h_l),\dots,\prod_l \varsigma_{sl}(h_l)\Big),$$

es biyectiva

Demostración. Primero veamos que $\theta(\varsigma_{ij}) \in \mathrm{Hom}(H_1\times\cdots\times H_r, K_1\times\cdots\times K_s)$. Por la propiedad universal del producto, para ello será suficiente comprobar que las aplicaciones

$$\begin{aligned} H_1\times\cdots\times H_r &\longrightarrow K_i\\ (h_1,\dots,h_r) &\longmapsto \textstyle\prod_l \varsigma_{il}(h_l)\end{aligned}$$

son morfismos. Pero esto se sigue inmediatamente de la propiedad universal del producto directo restringido. Así, θ es una función bien definida. Resta probar que es biyectiva, y quizás la manera más fácil de hacerlo es notar que es inversible, y que su inversa es la función definida por

$$\theta^{-1}(\varsigma) = (\pi_i\circ\varsigma\circ\iota_j),$$

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

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

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

$$\begin{pmatrix}\varsigma_{11} & \dots & \varsigma_{1r}\\ \vdots & \ddots & \vdots\\ \varsigma_{s1} & \dots & \varsigma_{sr}\end{pmatrix}\begin{pmatrix}h_1\\ \vdots\\ h_r\end{pmatrix} := \begin{pmatrix}\varsigma_{11}(h_1)\cdots\varsigma_{1r}(h_r)\\ \vdots\\ \varsigma_{s1}(h_1)\cdots\varsigma_{sr}(h_r)\end{pmatrix}. \tag{16}$$

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. Consideremos ahora otra matriz

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

donde $\mathbf{L} = (L_1,\dots,L_t)$ es otra familia finita de grupos. Afirmamos que la composición $\theta(\varphi_{ij})\circ\theta(\varsigma_{ij})$ se transforma vía θ^{-1} en el producto de matrices

$$\begin{pmatrix}\varphi_{11} & \dots & \varphi_{1s}\\ \vdots & \ddots & \vdots\\ \varphi_{t1} & \dots & \varphi_{ts}\end{pmatrix}\begin{pmatrix}\varsigma_{11} & \dots & \varsigma_{1r}\\ \vdots & \ddots & \vdots\\ \varsigma_{s1} & \dots & \varsigma_{sr}\end{pmatrix} = \begin{pmatrix}\psi_{11} & \dots & \psi_{1r}\\ \vdots & \ddots & \vdots\\ \psi_{t1} & \dots & \psi_{tr}\end{pmatrix}, \tag{17}$$

donde $\psi_{ij}\colon H_j \to L_i$ es el morfismo definido por $\psi_{ij}(h) := (\varphi_{i1}\circ\varsigma_{1j})(h)\cdots(\varphi_{is}\circ\varsigma_{sj})(h)$. En efecto, un cálculo directo muestra que la l-ésima coordenada $\theta(\varphi_{ij})\circ\theta(\varsigma_{ij})(h_1,\dots,h_r)_l$ de $\theta(\varphi_{ij})\circ\theta(\varsigma_{ij})(h_1,\dots,h_r)$ es

$$\begin{aligned}
\theta(\varphi_{ij})\circ\theta(\varsigma_{ij})(h_1,\dots,h_r)_l &= \varphi_{l1}\bigl(\varsigma_{11}(h_1)\cdots\varsigma_{1r}(h_r)\bigr)\cdots\varphi_{ls}\bigl(\varsigma_{s1}(h_1)\cdots\varsigma_{sr}(h_r)\bigr)\\
&= \varphi_{l1}(\varsigma_{11}(h_1))\cdots\varphi_{l1}(\varsigma_{1r}(h_r))\cdots\varphi_{ls}(\varsigma_{s1}(h_1))\cdots\varphi_{ls}(\varsigma_{sr}(h_r))\\
&= \varphi_{l1}(\varsigma_{11}(h_1))\cdots\varphi_{ls}(\varsigma_{s1}(h_1))\cdots\varphi_{l1}(\varsigma_{1r}(h_r))\cdots\varphi_{ls}(\varsigma_{sr}(h_r))\\
&= \psi_{l1}(h_1)\cdots\psi_{lr}(h_r)\\
&= \theta(\psi_{ij})(h_1,\dots,h_r)_l.
\end{aligned}$$

donde la tercera igualdad vale porque $\varphi_{lj}(\varsigma_{jk}(h_k))$ conmuta con $\varphi_{lj'}(\varsigma_{j'k'}(h'_{k'}))$ si $k'\neq k$ o $j'\neq j$.

Si los L_i son grupos abelianos y denotamos aditivamente la operación de cada uno de ellos, entonces los productos de matrices (16) y (17) toman el aspecto habitual. Manteniendo estas asunciones, la suma de morfismos introducida en la Proposición 1.68 se corresponde, vía θ^{-1}, con la suma de matrices. En particular, si G es un grupo conmutativo y su operación es denotada aditivamente, entonces $\operatorname{End}(G^n)\approx \mathrm{M}_n(\operatorname{End} G)$ y este isomorfismo respeta tanto la suma como la composición.

16. Producto semidirecto

Por el Teorema 1.111 de la Sección 15, 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, introducimos la noción de producto semidirecto, y estudiamos algunas de sus propiedades y las relaciones con la versión interna.

16.1. Producto semidirecto interno

Dados un grupo G y subgrupos N y H de G, decimos que G es *producto semidirecto interno* de N con H si $N\triangleleft G$ 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, $hn'h^{-1}\in N$, por lo que la fórmula

$$(nh)(n'h') = nhn'h^{-1}hh' \tag{18}$$

da la expresión deseada. De esta igualdad se sigue inmediatamente que la función $\pi_H\colon G\to H$, definida por $\pi_H(nh)=h$, es un morfismo cuyo núcleo es la inclusión canónica $\iota_N\colon N\to G$. Además, la inclusión canónica $\iota_H\colon H\to G$ es una sección de π_H.

Teorema 1.129. *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. *$N\triangleleft G$ y $N\cap H=1$.*

3. $N \triangleleft G$ *y si* $1 = nh$*, con* $n \in N$ *y* $h \in H$*, entonces* $n = h = 1$.

Demostración. Si G es producto semidirecto interno de N con H, entonces aparentemente cada $x \in N \cap H$ tiene dos escrituras,

$$x = 1x \quad \text{y} \quad x = x1,$$

como producto de un elemento de N con uno de H. Como en realidad tal escritura es única, inevitablemente $N \cap H = 1$. Así, 1) $\Rightarrow$ 2). Por otra parte, si vale 2) y $1 = nh$ con $n \in N$ y $h \in H$, entonces

$$n = h^{-1} \in N \cap H = 1$$

y, por lo tanto, $n = h = 1$. Esto prueba que 2) $\Rightarrow$ 3). Veamos que 3) $\Rightarrow$ 1). Si $nh = n'h'$, entonces

$$n^{-1}n'h'h^{-1} = 1$$

y, por consiguiente, $n^{-1}n' = h'h^{-1} = 1$. $\square$

Notemos que si G se descompone como producto semidirecto interno en la forma $G = NH$, entonces la aplicación

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

es un automorfismo, para cada $h \in H$. Además, la función $\varsigma\colon H \to \operatorname{Aut} N$ obtenida de este modo es un morfismo. Además, con estas notaciones, la fórmula (18) 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

$$\varsigma\colon H \to \operatorname{Aut} N,$$

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 para todo h, 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 1.130. *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 dados (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 1.12, para terminar la demostración es suficiente ver que $(1,1)$ es neutro a izquierda de $N\times_\varsigma H$ 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. □

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

PROPOSICIÓN 1.131. *El producto semidirecto tiene las siguientes propiedades:*

1. *Las funciones*

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

   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* $N\times_\varsigma H$ *y la función*

$$\begin{array}{c} N\xrightarrow{\ \iota\ } N\times 1\\ n\longmapsto (n,1)\end{array}$$

   es un isomorfismo.

3. $1\times H$ *es un subgrupo de* $N\times_\varsigma H$
4. $(1,h)(n,1)(1,h)^{-1}=(h\cdot n,1)$ *para todo* $h\in H$ *y* $n\in N$.
5. $(N\times 1)\cap(1\times H)=1$ *y* $(N\times 1)(1\times H)=N\times_\varsigma H$.

DEMOSTRACIÓN. Un cálculo directo muestra que π y s son morfismos. Además es claro que $\pi\circ s=\mathrm{id}_H$, $\ker\pi=N\times 1$ y $(N\times 1)\cap(1\times H)=1$. En consecuencia $N\times 1\lhd N\times_\varsigma H$ y $1\times H\le N\times_\varsigma H$. por otra parte, como

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

también ι es un morfismo de grupos, y se comprueba si dificultad ver que

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

Por último, de la igualdad

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

se sigue que $(N\times 1)(1\times H)=N\times_\varsigma H$. □

COROLARIO 1.132. $N\times_\varsigma H$ *es producto semidirecto interno de* $N\times 1$ *con* $1\times H$.

Proposición 1.133. *Si un grupo G es producto semidirecto interno de un subgrupo normal N con un subgrupo H, entonces la función*

$$\begin{aligned} N \times_{\varsigma} H &\xrightarrow{\zeta} G \ , \\ (n,h) &\longmapsto nh \end{aligned}$$

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

Demostración. Las igualdades

$$\zeta\big((n,h)(n',h')\big) = \zeta(nhn'h^{-1}, hh') = nhn'h' = \zeta(n,h)\zeta(n',h')$$

muestra que ζ es un morfismo de grupos. Como $G = NH$, este morfismo es sobreyectivo, y como $N \cap H = 1$, es inyectivo. $\square$

Ejemplo 1.134. *Dado un grupo abeliano G consideremos el morfismo*

$$\varsigma \colon C_2 \to \operatorname{Aut} G,$$

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 $G \times_{\varsigma} C_2$ es el grupo con conjunto subyacente $G \times C_2$ y multiplicación

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

Es fácil ver que cuando G es un grupo cíclico de orden n, esta construcción da un grupo isomorfo al grupo diedral D_n.

Ejemplo 1.135. *Consideremos dos grupos cíclicos $C_m = \langle x \rangle$ y $C_n = \langle y \rangle$ de orden m y n, respectivamente. Por la Observación 1.109, para cada $i \geq 0$ hay un morfismo*

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

tal que $\upsilon_i(y) = y^i$. Como $\upsilon_i(y^j) = y^{ji} = 1$ si y sólo si ji es múltiplo de n, el núcleo de υ_i es $\langle y^{n/(n:i)} \rangle$, donde, como en el Ejemplo 1.28, 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. Notemos que $\upsilon_i^m(y) = y^{(i^m)}$, de manera que $\upsilon_i^m = \mathrm{id}$ si y sólo si $i^m \cong 1 \pmod{n}$, lo cual implica que i y n son coprimos. En consecuencia, nuevamente por la Observación 1.109, existe un morfismo

$$\varsigma \colon C_m \to \operatorname{Aut} C_n$$

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

Ejemplo 1.136. *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_m tienen orden par. En consecuencia, por la Observación 1.35 todos tienen elementos de orden 2. Pero como vimos en el Ejemplo 1.30, 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 1.137. *Consideremos productos semidirectos* $N_1 \times_{\varsigma_1} H_1$ *y* $N_2 \times_{\varsigma_2} H_2$ *y morfismos* $\gamma\colon H_1 \to H_2$ *y* $\xi\colon N_1 \to N_2$*. Si el diagrama*

$$\begin{tikzcd} H_1 \arrow[r, "\varsigma_1"] \arrow[dd, "\gamma"] & \operatorname{Aut} N_1 \arrow[dr, "\xi_*"] & \\ & & \operatorname{Hom}(N_1, N_2) \\ H_2 \arrow[r, "\varsigma_2"] & \operatorname{Aut} N_2 \arrow[ur, "\xi^*"] & \end{tikzcd} ,$$

donde ξ_* *y* ξ^* *están definidos por* $\xi_*(\zeta) = \xi\circ\zeta$ *y* $\xi^*(\zeta) = \zeta\circ\xi$*, conmuta, entonces la función*

$$\chi\colon N_1 \times_{\varsigma_1} H_1 \to N_2 \times_{\varsigma_2} H_2,$$

definida por $\chi(n,h) = (\xi(n), \gamma(h))$*, es un morfismo de grupos, que es biyectivo si y sólo si* ξ *y* γ *lo son.*

Demostración. Por la conmutatividad del diagrama del enunciado,

$$\xi(h \cdot_{\varsigma_1} n') = \xi(\varsigma_1(h)(n')) = \xi_*(\varsigma_1(h))(n') = \xi^*(\varsigma_2\circ\gamma(h))(n') = \varsigma_2(\gamma(h))(\xi(n')) = \gamma(h) \cdot_{\varsigma_2} \xi(n'),$$

para cada $h \in H$ y $n' \in N$. En consecuencia

$$\begin{aligned} \chi((n,h)(n',h')) &= \chi(n(h \cdot_{\varsigma_1} n'), hh') \\ &= (\xi(n)\xi(h \cdot_{\varsigma_1} n'), \gamma(h)\gamma(h')) \\ &= (\xi(n)(\gamma(h) \cdot_{\varsigma_2} \xi(n')), \gamma(h)\gamma(h')) \\ &= (\xi(n), \gamma(h))(\xi(n'), \gamma(h')) \\ &= \chi(n,h)\chi(n',h'), \end{aligned}$$

lo cual prueba que χ es un morfismo. Además, es evidente que la segunda afirmación es verdadera. $\square$

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 es un epimorfismo. De la definición se sigue inmediatamente que una sucesión de morfismos

$$1 \longrightarrow G' \xrightarrow{\varphi} G \xrightarrow{\psi} G'' \longrightarrow 1 \tag{19}$$

es exacta si y sólo si φ es inyectiva, ψ es sobreyectiva e $\operatorname{Im}\varphi = \ker\psi$. Una *sucesión exacta corta* es una sucesión exacta de esta forma. Decimos que la sucesión exacta corta (19) es escindida a derecha si ψ es una retracción y a izquierda si φ es una sección. Dados grupos G, G' y G'', decimos que G es una *extensión de G' por G''* si hay un sucesión exacta corta como (19).

Ejemplo 1.138. *Si $N \times_\varsigma H$ es un producto semidirecto, entonces*

$$1 \longrightarrow N \xrightarrow{\iota_N} N \times_\varsigma H \xrightarrow{\pi_H} H \longrightarrow 1\ , \tag{20}$$

donde ι_N y π_H son la inclusión y la proyección canónica, respectivamente, es una sucesión exacta corta escindida a derecha. Si $\varsigma\colon H \to \operatorname{Aut} N$ es el morfismo trivial (esto es, si $N \times_\varsigma H$ es el producto directo de N con H) entonces la sucesión también es escindida a izquierda.

Ejemplo 1.139. *La sucesión de morfismos*

$$1 \longrightarrow \mathbb{Z}_2 \xrightarrow{\iota} \mathbb{Z}_4 \xrightarrow{\pi} \mathbb{Z}_2 \longrightarrow 1\ ,$$

donde ι y π son los morfismos definidos por $\iota(1) = 2$ y $\pi(1) = 1$, es una sucesión exacta corta no escindida.

Diremos que la sucesión exacta corta (19) es *equivalente* a la sucesión exacta corta

$$1 \longrightarrow G' \xrightarrow{\iota} L \xrightarrow{\pi} G'' \longrightarrow 1\ , \tag{21}$$

si existe un morfismo $\alpha\colon G \to L$ tal que el diagrama

$$\begin{tikzcd}
1 \arrow[r] & G' \arrow[r, "\varphi"] \arrow[d, "\mathrm{id}_{G'}"] & G \arrow[r, "\psi"] \arrow[d, "\alpha"] & G'' \arrow[r] \arrow[d, "\mathrm{id}_{G''}"] & 1 \\
1 \arrow[r] & G' \arrow[r, "\iota"] & L \arrow[r, "\pi"] & G'' \arrow[r] & 1
\end{tikzcd}$$

conmuta. Afirmamos que entonces α es necesariamente un isomorfismo. Para probarlo notemos primero que

$$\begin{aligned}
\alpha(g) = 1 &\Rightarrow \exists\, g' \in G' \text{ tal que } \varphi(g') = g && \text{porque } \psi(g) = \pi\circ\alpha(g) = 1 \text{ y (19) es exacta}\\
&\Rightarrow g' = 1 && \text{porque } \iota(g') = \alpha(g) = 1 \text{ y (21) es exacta}\\
&\Rightarrow g = \varphi(g') = 1,
\end{aligned}$$

y, por lo tanto, α es inyectivo. Nos queda ahora la tarea de probar que es sobreyectiva. Como ψ lo es, dado $l \in L$ existe $g \in G$ tal que $\psi(g) = \pi(l)$, por lo cual

$$\pi(\alpha(g^{-1})l) = \pi(\alpha(g^{-1}))\pi(l) = \psi(g^{-1})\pi(l) = 1.$$

En consecuencia, debido a la exactitud de (21), hay un $g' \in G'$ tal que $\iota(g') = \alpha(g^{-1})l$ y así,

$$l = \alpha(g)\iota(g') = \alpha(g)\alpha(\varphi(g')) = \alpha(g\varphi(g')).$$

Por la misma definición de equivalencia de sucesiones exactas cortas, es evidente que esta relación es reflexiva y transitiva. Ahora es claro que también es simétrica. Notemos que si dos sucesiones como las (19) y (21) son equivalentes, entonces una de ellas es escindida a un lado si y sólo si la otra lo es. Por ejemplo, si s es una sección de ψ, entonces $\alpha\circ s$ es una sección de π. En el Ejemplo 1.138 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 1.140. *Si una sucesión exacta corta*

$$1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow 1 \tag{22}$$

es escindida a derecha, entonces existe un producto semidirecto $N \times_\varsigma H$ tal que las sucesiones exactas cortas (20) *y* (22)*, son equivalentes.*

Demostración. Fijemos una sección s de π. 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

$$\begin{aligned} G &\xrightarrow{\Phi_{s(h)}} G\\ g &\longmapsto s(h)gs(h)^{-1} \end{aligned}$$

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

$$\pi\big(s(h)gs(h)^{-1}\big) = h\pi(g)h^{-1} = 1$$

para cada $g \in \iota(N)$. Por lo tanto, la aplicación $\varsigma\colon H \to \operatorname{Aut} N$ dada por

$$\iota(\varsigma(h)(n)) = s(h)\iota(n)s(h)^{-1}$$

está bien definida. Además es un morfismo de grupos, porque

$$\begin{aligned} \iota(\varsigma(hh')(n)) &= s(hh')\iota(n)s(hh')^{-1}\\ &= s(h)s(h')\iota(n)s(h')^{-1}s(h)^{-1}\\ &= s(h)\iota(\varsigma(h')(n))s(h)^{-1}\\ &= \iota(\varsigma(h)\circ\varsigma(h')(n)). \end{aligned}$$

Entonces tiene sentido considerar el producto semidirecto $N \times_\varsigma H$. Para terminar la prueba será suficiente mostrar que la aplicación $\alpha\colon N \times_\varsigma H \to G$, definida por $\alpha(n,h) = \iota(n)s(h)$ es un morfismo de grupos, y que el diagrama

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota_N"] \arrow[d, "\mathrm{id}_N"] & N \times_\varsigma H \arrow[r, "\pi_H"] \arrow[d, "\alpha"] & H \arrow[r] \arrow[d, "\mathrm{id}_H"] & 1\\ 1 \arrow[r] & N \arrow[r, "\iota"] & G \arrow[r, "\pi"] & H \arrow[r] & 1 \end{tikzcd}$$

conmuta. Pero las igualdades

$$\alpha\circ\iota_N(n) = \alpha(n,1) = \iota(n) \qquad \text{y} \qquad \pi\circ\alpha(n,h) = \pi(\iota(n)s(n)) = \pi\circ\iota(n)\pi\circ s(h) = h$$

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 1.141. *En la demostración del Teorema 1.140 no sólo probamos que la sucesión exacta corta (22) 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 1.142. *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 es definido por $\pi(nh) = h$ es una sucesión exacta corta. Por el Teorema 1.140, como la inclusión canónica de H en G es una sección de π, el diagrama

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota_N"] \arrow[d, "\mathrm{id}_N"] & N\times_{\varsigma} H \arrow[r, "\pi_H"] \arrow[d, "\alpha"] & H \arrow[r] \arrow[d, "\mathrm{id}_H"] & 1 \\ 1 \arrow[r] & N \arrow[r, "\iota"] & G \arrow[r, "\pi"] & H \arrow[r] & 1 \end{tikzcd},$$

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 1.133.

PROPOSICIÓN 1.143. *Las sucesiones exactas cortas asociadas a dos productos semidirectos $N\times_{\varsigma_1} H$ y $N\times_{\varsigma_2} H$ son equivalentes si y sólo si existe una función $\varpi\colon H\to N$ que satisface:*

$$\varpi(hh') = \varpi(h)\bigl(h\cdot_{\varsigma_2}\varpi(h')\bigr) \qquad y \qquad (h\cdot_{\varsigma_1} n)\varpi(h) = \varpi(h)(h\cdot_{\varsigma_2} n), \tag{23}$$

para todo $h,h'\in H$ y $n\in N$.

DEMOSTRACIÓN. Supongamos que un diagrama de la forma

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota_N"] \arrow[d, "\mathrm{id}_N"] & N\times_{\varsigma_1} H \arrow[r, "\pi_H"] \arrow[d, "\chi"] & H \arrow[r] \arrow[d, "\mathrm{id}_H"] & 1 \\ 1 \arrow[r] & N \arrow[r, "\iota_N"] & N\times_{\varsigma_2} H \arrow[r, "\pi_H"] & H \arrow[r] & 1 \end{tikzcd}$$

conmuta y $\chi\bigl((n,1)(1,h)\bigr) = \chi(n,1)\chi(1,h)$ para todo $n\in N$ y $h\in H$. Entonces, como

$$\pi_H\circ\chi = \pi_H \qquad \text{y} \qquad \chi\circ\iota_N = \iota_N, \tag{24}$$

existe una única función $\varpi\colon H\to N$ tal que

$$\chi(n,h) = \chi(n,1)\chi(1,h) = (n,1)\bigl(\varpi(h),h\bigr) = \bigl(n\varpi(h),h\bigr).$$

En consecuencia,

$$\chi\big((n,1)(n',h)\big) = \chi(nn',h) = \big(nn'\varpi(h),h\big) = (n,1)\big(n'\varpi(h),h\big) = \chi(n,1)\chi(n',h) \tag{25}$$

para todo $n, n' \in N$ y $h \in H$. Recíprocamente, dada cualquier función $\varpi\colon H \to N$, la función

$$\chi\colon N \times_{\varsigma_1} H \to N \times_{\varsigma_2} H,$$

definida por $\chi(n,h) := (n\varpi(h),h)$, satisface las condiciones (24) y (25). Afirmamos que χ es un morfismo si y sólo si

$$\chi\big((1,h)(n,1)\big) = \chi(1,h)\chi(n,1) \qquad \text{y} \qquad \chi\big((1,h)(1,h')\big) = \chi(1,h)\chi(1,h') \tag{26}$$

para todo $h,h' \in H$ y $n \in N$. En efecto, es claro que si χ es un morfismo, entonces las igualdades (26) se satisfacen. Recíprocamente, si estas igualdades valen, entonces

$$\begin{aligned}
\chi\big((n,h)(n',h')\big) &= \chi\big((n,1)(1,h)(n',h')\big) \\
&= \chi(n,1)\chi\big((1,h)(n',h')\big) && \text{por (25)} \\
&= \chi(n,1)\chi(h \cdot_{\varsigma_1} n', hh') \\
&= \chi(n,1)\chi(h \cdot_{\varsigma_1} n', 1)\chi(1,hh') \\
&= \chi(n,1)\chi(h \cdot_{\varsigma_1} n', 1)\chi(1,h)\chi(1,h') && \text{por (26)} \\
&= \chi(n,1)\chi(h \cdot_{\varsigma_1} n', h)\chi(1,h') \\
&= \chi(n,1)\chi\big((1,h)(n',1)\big)\chi(1,h') \\
&= \chi(n,1)\chi(1,h)\chi(n',1)\chi(1,h') && \text{por (26)} \\
&= \chi(n,h)\chi(n',h'),
\end{aligned}$$

para todo $(n,h),(n',h') \in N \times_{\varsigma_1} H$ y, por lo tanto, χ es un morfismo, como queríamos. Para terminar la prueba basta observar que como

$$\begin{aligned}
&\chi\big((1,h)(n,1)\big) = \big((h \cdot_{\varsigma_1} n)\varpi(h),h\big), && \chi(1,h)\chi(n,1) = \big(\varpi(h)h \cdot_{\varsigma_2} n),h\big),\\
&\chi\big((1,h)(1,h')\big) = \big(\varpi(hh'),hh'\big), && \chi(1,h)\chi(1,h') = \big(\varpi(h)(h \cdot_{\varsigma_2} \varpi(h')),hh'\big),
\end{aligned}$$

las condiciones (23) y (26) son equivalentes. □

Teorema 1.144. *Si una sucesión exacta corta*

$$1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow 1 \tag{27}$$

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 $(\gamma,\pi)\circ\iota(n) = (n,1)$ y $\pi_H\circ(\gamma,\pi)(g) = \pi(g)$ para todo $n \in N$ y $g \in G$, el diagrama

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "\iota"] \arrow[d, "\mathrm{id}_N"] & G \arrow[r, "\pi"] \arrow[d, "(\gamma,\pi)"] & H \arrow[r] \arrow[d, "\mathrm{id}_H"] & 1 \\
1 \arrow[r] & N \arrow[r, "\iota_N"] & N \times H \arrow[r, "\pi_H"] & H \arrow[r] & 1
\end{tikzcd}$$

conmuta, lo que prueba el resultado. □

18. Automorfismos interiores y subgrupos característicos

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.

Dado $g \in G$, 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 las igualdades

$$\Phi_g(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = \Phi_g(h)\Phi_g(k)$$

muestran que, de hecho, es un automorfismo, llamado *el automorfismo interior* de G *asociado a* g. Además, como

$$\Phi_{gh}(k) = ghkh^{-1}g^{-1} = \Phi_g\bigl(\Phi_h(k)\bigr),$$

la aplicación

$$\begin{aligned} G &\xrightarrow{\Psi} \operatorname{Aut} G \\ g &\longmapsto \Phi_g \end{aligned}$$

es un morfismo de grupos. Es claro que su imagen es el conjunto $\operatorname{Int} G$, de los automorfismos interiores de G, y su 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 1.140. Aunque sencillo, el siguiente es el primer resultado escencialmente nuevo.

Proposición 1.145. *La igualdad* $\varphi\circ\Phi_g\circ\varphi^{-1} = \Phi_{\varphi(g)}$ *vale para cada* $\varphi \in \operatorname{Aut} G$ *y* $g \in G$. *En particular,* $\operatorname{Int} G \lhd \operatorname{Aut} G$.

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 $h \in G$. □

Al grupo cociente $\operatorname{Out} G := \operatorname{Aut} G/\operatorname{Int} G$ se lo conoce como el grupo de *automorfismos exteriores* de G (aunque sus elementos no son automorfismos). Es obvio que la sucesión

$$1 \longrightarrow \mathrm{Z}\,G \xrightarrow{\iota} G \xrightarrow{\Psi} \operatorname{Aut} G \xrightarrow{\pi} \operatorname{Out} G \longrightarrow 1\,,$$

donde ι es la inclusión canónica y π la proyección al cociente, es exacta.

Observación 1.146. $\mathrm{Z}\bigl(\prod G_i\bigr) = \prod \mathrm{Z}(G_i)$ *y* $\mathrm{Z}\bigl(\bigsqcup G_i\bigr) = \bigsqcup \mathrm{Z}(G_i)$ *para toda familia* $(G_i)_{i\in I}$ *de grupos.*

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 1.147. *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 $(gk^{-1})k = g$. □

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 H 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 $\mathrm{Z}\, G$ es un subgrupo característico de G. Para probarlo debemos mostrar que si $g \in \mathrm{Z}\, G$ y $\varphi \in \operatorname{Aut} G$, entonces $\varphi(g) \in \mathrm{Z}\, G$. 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 1.148. *Recordemos que el grupo diedral D_n ($n \geq 2$) está generado por dos elementos x, y sujetos a las relaciones $x^n = 1$, $y^2 = 1$ e $yxy^{-1}x = 1$, y que*

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

Queremos determinar su centro. Para empezar, D_2 es conmutativo. Supongamos entonces que $n > 2$. Como

$$x(x^i y)x^{-1} = x^{i+2}y \qquad \text{y} \qquad x^2 \neq 1,$$

$x^i y \notin \mathrm{Z}\, D_n$ para ningún i, y como

$$yx^i y^{-1} = x^{-i} \quad \text{y} \quad x^i \text{ conmuta con } x,$$

$x^i \in \mathrm{Z}\, D_n$ si y sólo si $i = n/2$. Así,

$$\mathrm{Z}\, D_n = \begin{cases} D_n & \text{si } n = 2, \\ 1 & \text{si } n \text{ es impar,} \\ \{1, x^{n/2}\} & \text{si } n \text{ es par y } n > 2. \end{cases}$$

Consideremos ahora el grupo cuaterniónico generalizado H_n ($n \geq 2$). Recordemos 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

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

De la igualdad $x(x^i y)x^{-1} = x^{i+2}y$ se sigue que $x^i y \notin \mathrm{Z}\, H_n$ para ningún i, y puesto que $yx^i y^{-1} = x^{-i}$ y x^i 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 1.149. *Pruebe que todos los subgrupos de H_2 son normales.*

EJERCICIO 1.150. *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 1.151. *Pruebe que si $f \colon G \to G'$ es un morfismo sobreyectivo de grupos, entonces $f(\mathrm{Z}\, G) \subseteq \mathrm{Z}\, G'$.*

EJERCICIO 1.152. *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 $N \subseteq \mathrm{Z}(H \times L)$.

PROPOSICIÓN 1.153. *Si $G/\mathrm{Z}\, G$ es cíclico, entonces G es abeliano.*

Demostración. Por hipótesis existe $g \in G$ tal que $G = \langle g \rangle \, \mathrm{Z}\, G$. Como

$$(g^m h)(g^n k) = g^m g^n hk = g^n g^m kh = (g^n k)(g^m h)$$

para todo $m, n \in \mathbb{Z}$ y todo $h, k \in \mathrm{Z}\, G$, esto implica que G es conmutativo. □

Observación 1.154. *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, dado $g \in G$ arbitrario, como $L \lhd G$, 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 es cierto 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 1.150 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 1.155. *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 1.156. *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. Primero notemos que $\Phi_g(L) \supseteq \Phi_g(H) = H$ para cada $g \in G$. Entonces, como $\Phi_{[g]}(L/H) = \Phi_g(L)/H$, donde $[g]$ denota a la clase de g en G/H, y L/H es normal en G/H,

$$\Phi_g(L)/H = L/H,$$

lo que, por el Teorema de la correspondencia, 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. □

18.1. 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 $g,h \in G$. 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. El cociente $G/[G,G]$ es llamado 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

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] & G' \\ G/[G,G] \arrow[ur, "\varphi'"'] & \end{tikzcd},$$

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 1.93, dado un morfismo de grupos

$$\varphi\colon G \to G'$$

existe un único morfismo $\bar{\varphi}\colon \frac{G}{[G,G]} \to \frac{G'}{[G',G']}$ tal que el diagrama

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] & G' \arrow[d, "\pi'"] \\ G/[G,G] \arrow[r, "\bar{\varphi}"] & G'/[G',G'] \end{tikzcd},$$

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 $\overline{\psi\circ\varphi} = \bar{\psi}\circ\bar{\varphi}$.

Ejemplo 1.157. *Consideremos el grupo diedral D_n, presentado como en el Ejemplo 1.148. Vamos a determinar su subgrupo conmutador. Puesto que*

$$[x,y] = xyx^{-1}y^{-1} = x^2,$$

el subgrupo $\langle x^2\rangle$ de D_n está incluído en $[D_n,D_n]$. Pero por el Ejemplo 1.107 sabemos que $\langle x^2\rangle$ es un subgrupo normal de D_n y que $D_n/\langle x^2\rangle \approx D_2$, un grupo conmutativo. Así también vale la inclusión recíproca y $[D_n,D_n] = \langle x^2\rangle$. Consideremos ahora el grupo cuaterniónico generalizado, también con la presentación dada en el Ejemplo 1.148. Como

$$[x,y] = xyx^{-1}y^{-1} = x^2,$$

el subgrupo de H_n generado por x^2 es normal porque

$$yx^2y^{-1} = x^{-2},$$

y el cociente $H_n/\langle x^2\rangle$ es conmutativo (por ejemplo, porque $[x,y]=x^2$), el subgrupo conmutador de H_n es $\langle x^2\rangle$.

18.2. 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 1.158. *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 $g\in G$, porque

$$\Phi_g([h,l])=\Phi_g(hlh^{-1}l^{-1})=\Phi_g(h)\Phi_g(l)\Phi_g(h)^{-1}\Phi_g(l)^{-1}\quad \text{para todo } h,l\in G.$$

Esto prueba que $[H,L]$ es un subgrupo normal de G. Los otros casos pueden tratarse de manera similar. □

OBSERVACIÓN 1.159. *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 clases de los elementos de L. En particular $[G,L]\subseteq K$ si y sólo si la imagen LK/K, de L en G/K, está incluída en el centro de $Z(G/K)$. Denotemos con $\bar{H}$, $\bar{L}$ y $\overline{[H,L]}$ a los mínimos subgrupos normales de G que contienen a H, L y $[H,L]$ respectivamente. Obviamente, el mínimo subgrupo normal K de G, tal que $[H,L]\subseteq K$, es $\overline{[H,L]}$. Como $[H,L]\subseteq[\bar{H},\bar{L}]$ y, por la Proposición 1.158, el subgrupo $[\bar{H},\bar{L}]$ de G es normal, $\overline{[H,L]}$ está incluído en $[\bar{H},\bar{L}]$.*

Supongamos que H y L son subgrupos normales de un grupo G. Por la propiedad universal del cociente, 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

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] & G' \\ G/[H,L] \arrow[ur, "\varphi'"'] & \end{tikzcd}$$

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 1.93, si $\varphi(H)\subseteq H'$ y $\varphi(L)\subseteq L'$, entonces existe un único morfismo $\bar{\varphi}\colon \frac{G}{[H,L]}\to\frac{G'}{[H',L']}$ tal que el diagrama

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] & G' \arrow[d, "\pi'"] \\ G/[H,L] \arrow[r, "\bar{\varphi}"] & G'/[H',L'] \end{tikzcd},$$

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 $\overline{\psi\circ\varphi} = \bar{\psi}\circ\bar{\varphi}$.

OBSERVACIÓN 1.160. *Dadas familias de grupos $(H_i)_{i\in I}$, $(L_i)_{i\in I}$ y $(G_i)_{i\in I}$, con $H_i, L_i \le G_i$ para todo i,*

$$\Big[\prod H_i, \prod L_i\Big] = \prod [H_i, L_i] \qquad y \qquad \Big[\coprod H_i, \coprod L_i\Big] = \coprod [H_i, L_i].$$

EJERCICIO 1.161. *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).*

18.3. Subgrupos conjugados

Dos subgrupos L y H de un grupo G son *conjugados* si $L = gHg^{-1} = \Phi_g(H)$ para algún $g \in G$. Es evidente que si $L \le G$ es finito y H es conjugado a L, entonces H es finito y tiene el mismo orden que L. Además, por el Teorema 1.89, si L tiene índice finito, entonces el índice de H también es finito y coincide con el de L. 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 maximal 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 $h \in H$.

18.4. 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, $\mathrm{C}_G(H) \triangleleft \mathrm{N}_G(H)$. De las definiciones se sigue que:

1. $\mathrm{C}_G(H) = \bigcap_{h\in H} \mathrm{C}_G(h)$.
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 el máximo subgrupo de G en el que H es normal.

Observación 1.162. *Dadas familias de grupos $(H_i)_{i\in I}$ y $(G_i)_{i\in I}$ con $H_i \leq G_i$,*

$$N_{\prod G_i}\Bigl(\prod H_i\Bigr) = \prod N_{G_i}(H_i), \qquad N_{\coprod G_i}\Bigl(\coprod H_i\Bigr) = \coprod N_{G_i}(H_i),$$
$$C_{\prod G_i}\Bigl(\prod H_i\Bigr) = \prod C_{G_i}(H_i) \qquad y \qquad C_{\coprod G_i}\Bigl(\coprod H_i\Bigr) = \coprod C_{G_i}(H_i).$$

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 $H/(H\cap L) \approx HL/H$, porque $H \triangleleft HL$.

Observación 1.163. *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 1.164. *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 $(n \geq 2)$. 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 $n!$. Recordemos también que, al menos en este apunte, el resultado del producto $\sigma\tau$ de dos permutaciones, es la permutación obtenida aplicando primero τ y luego σ. Una forma bastante usual (pero que nosotros no utilizaremos nunca) de describir una permutación σ es escribiendo:

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

Para abreviar, denotaremos con $\mathbb{I}_n$ al conjunto $\{1,\dots,n\}$, de modo que $\mathrm{S}_n = \mathrm{S}_{\mathbb{I}_n}$. Dado $\sigma \in \mathrm{S}_n$ y $j \in \mathbb{I}_n$ decimos que σ *fija* j si $\sigma(j) = j$ y que lo *mueve* si $\sigma(j) \neq j$. 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 $\sigma\tau$ es la permutación definida por

$$\sigma\tau(j) = \begin{cases} \sigma(j) & \text{si } \tau \text{ fija } j, \\ \tau(j) & \text{si } \tau \text{ no fija } j. \end{cases}$$

Es evidente que si σ se escribe como un producto $\sigma = \sigma_1 \cdots \sigma_s$ 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 $(i_1,\dots,i_r)$ para denotar a este r-ciclo. Esta escritura no es única. Los sinónimos de $(i_1,\dots,i_r)$ son

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

Así, cada r-ciclo es determinado por r funciones inyectivas de $\mathbb{I}_r$ en $\mathbb{I}_n$. Por lo tanto hay

$$\frac{1}{r}n(n-1)\cdots(n-r+1)$$

r-ciclos en S_n. El único 1-ciclo es el permutación identidad. A los 2 ciclos también se los llama *trasposiciones*. 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. Un cálculo directo muestra que componiendo j veces consigo mismo el r ciclo $(i_1,\dots,i_r)$, se obtiene la permutación que fija los elementos de $\mathbb{I}_n\setminus\{i_1,\dots,i_r\}$ y aplica cada i_l en i_{l+j}, donde la suma $i+j$ es hecha módulo r. En consecuencia, el orden de cada r-ciclo es r.

TEOREMA 2.1. *Toda permutación $\sigma\in\mathrm{S}_n$ se escribe como un producto $\sigma=\sigma_1\cdots\sigma_r$ 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 múltiplo común 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 $i_{r+1}\in\{i_1,\dots,i_r\}$. Puesto que σ es inyectiva, forzosamente debe ser $i_{r+1}=i_1$. Consideremos el r-ciclo σ_1 definido por

$$\sigma_1(i_1)=i_2,\ \sigma_1(i_2)=i_3,\ \dots,\ \sigma_1(i_{r-1})=i_r\quad\text{y}\quad\sigma_1(i_r)=i_1.$$

Como el conjunto de puntos fijados por $\sigma_1^{-1}\sigma$ es la unión disjunta de $\{i_1,\dots,i_r\}$ y el de los fijados por σ, por la hipótesis inductiva existen ciclos disjuntos $\sigma_2,\dots,\sigma_s$ tales que

$$\sigma_1^{-1}\sigma=\sigma_2\cdots\sigma_s.$$

Puesto que $\{i_1,\dots,i_r\}$ es dejado fijo por cada uno de los ciclos $\sigma_2,\dots,\sigma_s$, la expresión $\sigma=\sigma_1\cdots\sigma_s$ es un producto de ciclos disjuntos dos a dos.

Consideremos la unicidad. Supongamos que

$$\sigma=\sigma_1\cdots\sigma_s=\sigma_1'\cdots\sigma_{s'}'.$$

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 $i=1$. Tomando ahora potencias de todos los órdenes, y evaluando en i_1, obtenemos que

$$\sigma_1^k(i_1)=\sigma_1^k\sigma_2^k\cdots\sigma_s^k(i_1)=\sigma^k(i_1)={\sigma_1'}^k{\sigma_2'}^k\cdots{\sigma_{s'}'}^k(i_1)={\sigma_1'}^k(i_1),$$

para todo $k\in\mathbb{N}$, donde la primera igualdad vale porque los σ_j's con $j\geq 2$ fijan i_1, la segunda porque los σ_j's conmutan dos a dos, y la tercera y cuarta por las mismas razones, referidas a los σ_j''s. Pero entonces $\sigma_1=\sigma_1'$ porque

$$\sigma_1(i_k)=\sigma_1^k(i_1)=\sigma_2^k(i_1)=\sigma_2(i_k)\quad\text{para todo } k,$$

y, por lo tanto,

$$\sigma_2 \cdots \sigma_s = \sigma_2 \cdots \sigma_{s'}.$$

Un argumento inductivo muestra ahora que $s' = s$ y $\{\sigma_2, \dots, \sigma_s\} = \{\sigma'_2, \dots, \sigma'_{s'}\}$.

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 $\sigma^r = \sigma_1^r \cdots \sigma_s^r = \mathrm{id}$. 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

$$\sigma = \sigma_1 \cdots \sigma_s.$$

Denotemos con r_j al orden de σ_j, donde $1 \le j \le s$. Podemos suponer que $2 \le r_1 \le \cdots \le r_s$. Claramente

$$r_1 + \cdots + r_s \le n \qquad \text{y} \qquad n - r_1 - \cdots - r_s$$

es la cantidad de puntos fijos de σ. Denotemos con α_1 a este número y con α_j, para $1 < j \le n$, a la cantidad de j-ciclos que aparecen en $\{\sigma_1, \dots, \sigma_s\}$. En otras palabras $\alpha_j = |\{i : r_i = j\}|$. Es claro $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n$ y que hay una correspondencia biyectiva entre el conjunto de los números naturales $r_1 \le r_2 \le \cdots \le r_s$ con $r_1 \ge 2$ tales que $r_1 + \cdots + r_s \le n$ y el de los enteros $\alpha_1, \dots, \alpha_n \ge 0$ tales que $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n$. A la sucesión $[\alpha_1, \dots, \alpha_n]$ la llamamos la *estructura cíclica* de σ.

PROPOSICIÓN 2.2 (Fórmula de Cauchy). *Para cada n-upla $(\alpha_1, \dots, \alpha_n)$, de n enteros no negativos tales que $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n$, hay*

$$\frac{n!}{1^{\alpha_1}\alpha_1! 2^{\alpha_2}\alpha_2! \dots n^{\alpha_n}\alpha_n!} \tag{28}$$

permutaciones con estructura cíclica $[\alpha_1, \dots, \alpha_n]$ en S_n.

DEMOSTRACIÓN. Consideremos una sucesión $i_1, \dots, i_n$, formada por los primeros n-números naturales. Intercalando en forma alternada paréntesis de apertura (y de cierre) en la sucesión, de modo que de izquierda a derecha haya primero α_1 configuraciones del tipo $(\dots)$ envolviendo a un sólo número cada una, luego α_2 envolviendo 2, luego α_3 envolviendo 3, etcétera, se obtiene una permutación con estructura cíclica $[\alpha_1, \dots, \alpha_n]$. Por ejemplo, si

Esto se sigue de que cada j-ciclo se puede obtener de j formas distintas

$$(i_1, \dots, i_j) = (i_2, \dots, i_j, i_1) = \cdots = (i_j, i_1, \dots, i_{j-1})$$

y de que si permutamos entre si los α_j ciclos de orden j obtenemos la misma permutación de S_n. □

TEOREMA 2.3. *Dos permutaciones de S_n son conjugadas en si y sólo si tienen la misma estructura cíclica. Además, si*

$$\sigma = (i_1, \dots, i_{r_1})(i_{r_1+1}, \dots, i_{r_2}) \cdots (i_{r_{s-1}+1}, \dots, i_{r_s})$$

y τ es una permutación arbitraria, entonces

$$\tau\sigma\tau^{-1} = \big(\tau(i_1), \dots, \tau(i_{r_1})\big)\big(\tau(i_{r_1+1}), \dots, \tau(i_{r_2})\big) \cdots \big(\tau(i_{r_{s-1}+1}), \dots, \tau(i_{r_s})\big).$$

DEMOSTRACIÓN. Un cálculo sencillo muestra que

$$\tau(i_1,\dots,i_r)\tau^{-1} = (\tau(i_1),\dots,\tau(i_r))$$

para cada permutación τ y cada r-ciclo $(i_1,\dots,i_r)$. En consecuencia, si σ se escribe en la forma $\sigma = \sigma_1\cdots\sigma_s$, como un producto de ciclos disjuntos dos a dos, entonces

$$\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1})\cdots(\tau\sigma_s\tau^{-1})$$

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

$$\sigma = (i_1,\dots,i_{r_1})(i_{r_1+1},\dots,i_{r_2})\cdots(i_{r_{s-1}+1},\dots,i_{r_s})$$

y

$$\sigma' = (i'_1,\dots,i'_{r_1})(i'_{r_1+1},\dots,i'_{r_2})\cdots(i'_{r_{s-1}+1},\dots,i'_{r_s}).$$

Entonces la permutación $\tau \in \mathrm{S}_n$ definida por

$$\tau(i) = \begin{cases} i'_j & \text{si } i = i_j \text{ con } 1 \le j \le r_s, \\ \varphi(i) & \text{si } i \in \mathbb{I}_n \setminus \{i_1,\dots,i_{r_s}\}, \end{cases}$$

donde $\varphi\colon \mathbb{I}_n \setminus \{i_1,\dots,i_{r_s}\} \to \mathbb{I}_n \setminus \{i'_1,\dots,i'_{r_s}\}$ es una función biyectiva arbitraria, satisface $\tau\sigma\tau^{-1} = \sigma'$. □

COROLARIO 2.4. *La fórmula* (28) *da la cantidad de elementos que tiene la clase de conjugación asociada a la estructura cíclica* $[\alpha_1,\dots,\alpha_n]$.

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 $\alpha_1,\dots,\alpha_n \ge 0$ que satisfacen

$$\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n.$$

Dada una de esta sucesiones, consideremos los números $\mu_j = \alpha_j + \cdots + \alpha_n$. Por su misma definición

$$\mu_1 \ge \mu_2 \ge \cdots \ge \mu_n \qquad \text{y} \qquad \mu_1 + \cdots + \mu_n = n. \tag{29}$$

Las sucesiones de énteros no negativos que satisfacen (29) 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 $\mu_1 \ge \mu_2 \ge \cdots \ge \mu_n$ 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

$$\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = \mu_1 + \cdots + \mu_n = n.$$

Como estas correspondencias son inversa una de la otra, hay tantas clases de conjugación de S_n como particiones de n.

EJEMPLO 2.5. *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.*

Observación 2.6. *El Teorema 2.3 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* $\Phi_\tau \alpha$*, donde* Φ_τ *es la conjugación por la trasposición* 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* $h \in K$*. Entonces, por la segunda afirmación del Teorema 2.3*

$$\beta(h) = \Phi_\tau(\alpha(h)) = \alpha(h)$$

si y sólo si $h \in K$*, que es más que lo que necesitábamos probar.*

2. Generadores de $\mathrm{S_n}$

Un cálculo directo muestra que

$$(i_1, \dots, i_r) = (i_1, i_r)(i_1, i_{r-1}) \cdots (i_1, i_2) \quad \text{y} \quad (1, i_1)(1, i_j)(1, i_1) = (i_1, i_j) \text{ si } i_i, i_j \neq 1.$$

Como cada permutación es producto de ciclos se sigue que

$$\mathrm{S}_n = \langle (1,2), (1,3), \dots, (1,n) \rangle.$$

Como además $(i, i+1)(1, i)(i, i+1) = (1, i+1)$ para todo $i < n$, es claro que también

$$\mathrm{S}_n = \langle (1,2), (2,3), \dots, (n-1,n) \rangle.$$

Por último, usando la igualdad $(1, \dots, n)^{i-1}(1,2)(1, \dots, n)^{-i+1} = (i, i+1)$, válida para $i < n$, concluímos que

$$\mathrm{S}_n = \langle (1,2), (1, \dots, n) \rangle.$$

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 $\operatorname{Des}(\sigma)$ al conjunto de descensos de σ. Por definición el *signo* de σ es el número $\operatorname{sg}(\sigma) := (-1)^{|\operatorname{Des}(\sigma)|}$. La propiedad más importante de la función $\operatorname{sg}\colon \mathrm{S}_n \to \{-1, 1\}$ es que, como establecemos en el Teorema 2.9 abajo, es un morfismo sobreyectivo de grupos.

Lema 2.7. *Para cada permutación* $\sigma \in \mathrm{S}_n$ *y cada* $k < n$*, la cantidad de descensos de* $\sigma(k, k+1)$ *difiere en* ± 1 *de la de* σ*.*

Demostración. Es evidente que:

- Si $i < j \leq n$ y $\{k, k+1\} \cap \{i, j\} = \emptyset$, entonces (i,j) es un descenso de $\sigma(k, k+1)$ si y sólo si lo es de σ.
- Si $i < k$, entonces $(i, k) \in \operatorname{Des}(\sigma(k, k+1))$ si y sólo si $(i, k+1) \in \operatorname{Des}(\sigma)$.
- Si $i < k$, entonces $(i, k+1) \in \operatorname{Des}(\sigma(k, k+1))$ si y sólo si $(i, k) \in \operatorname{Des}(\sigma)$.

- Si $k+1<j$, entonces $(k,j)\in \mathrm{Des}(\sigma(k,k+1))$ si y sólo si $(k+1,j)\in \mathrm{Des}(\sigma)$.
- Si $k+1<j$, entonces $(k+1,j)\in \mathrm{Des}(\sigma(k,k+1))$ si y sólo si $(k,j)\in \mathrm{Des}(\sigma)$.
- El par $(k,k+1)\in \mathrm{Des}(\sigma(k,k+1))$ si y sólo si no es un descenso de σ.

El resultado se sigue fácilmente de estas observaciones. □

COROLARIO 2.8. *Si $\sigma=\sigma_1\cdots\sigma_s$, donde las σ_i's son trasposiciones, entonces s es congruente a* $\mathrm{Des}(\sigma)$ *módulo* 2.

DEMOSTRACIÓN. Esto es una consecuencia inmediata de la Proposición 2.7. □

TEOREMA 2.9. *La función* $\mathrm{sg}\colon \mathrm{S}\to\{-1,1\}$ *es un morfismo sobreyectivo*

DEMOSTRACIÓN. Por el Corolario 2.8, si $\sigma=\sigma_1\cdots\sigma_s$, donde las σ_i's son trasposiciones, 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 2.10. *Si $\sigma\in \mathrm{S}_n$ tiene estructura cíclica $[\alpha_1,\dots,\alpha_n]$, entonces*

$$\mathrm{sg}(\sigma)=(-1)^{n-s},$$

donde $s=\alpha_1+\cdots+\alpha_n$.

DEMOSTRACIÓN. Si σ es un r-ciclo $(i_1,\dots,i_r)$, entonces $\mathrm{sg}(\sigma)=(-1)^{r-1}$, porque

$$\sigma=(i_1,i_r)(i_1,i_{r-1})\cdots(i_1,i_2).$$

En el caso general hay una factorización $\sigma=\sigma_1\cdots\sigma_s$, 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 consiguiente

$$\mathrm{sg}(\sigma)=\mathrm{sg}(\sigma_1)\cdots\mathrm{sg}(\sigma_s)=(-1)^{\sum_{j=2}^n\alpha_j(j-1)}=(-1)^{\sum_{j=1}^n\alpha_j j-\sum_{j=1}^n\alpha_j}=(-1)^{n-s},$$

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 es $n!/2$ de S_n.

OBSERVACIÓN 2.11. *La aplicación $\theta\colon \mathrm{S}_n\to \mathrm{A}_{n+2}$, definida por*

$$\theta(\sigma)=\begin{cases}\sigma & \text{si } \sigma \text{ es par,}\\ \sigma(n+1,n+2) & \text{si } \sigma \text{ es impar,}\end{cases}$$

es un morfismo inyectivo de grupos.

PROPOSICIÓN 2.12. *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 $\{\mathrm{id},\sigma\}$. En particular S_n es el producto semidirecto de A_n y $\{\mathrm{id},(1,2)\}$.*

DEMOSTRACIÓN. Tomemos $\sigma\in H\setminus \mathrm{A}_n$. Como la función

$$\begin{aligned} H\cap \mathrm{A}_n &\longrightarrow H\setminus \mathrm{A}_n\\ \tau &\longmapsto \tau\sigma\end{aligned}$$

es biyectiva, $H \cap \mathrm{A}_n$ es un subgrupo de índice 2 de H, lo cual implica que 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 $\{\mathrm{id}, \sigma\}$. □

4. Generadores de $\mathrm{A_n}$

Como cada elemento de A_n es producto de un número par de trasposiciones y

$$(a,b)(a,c) = (a,b,c)^2 \qquad \text{y} \qquad (a,b)(c,d) = (a,c,b,d)^2,$$

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 y los 4-ciclos. Dado que $(a,b,c) = (a,c,b)^2$, el resultado que sigue dice que en realidad los cuadrados de $(1,3,2),(1,4,2),\dots,(1,n,2)$ bastan.

Teorema 2.13. *Para todo $n \in \mathbb{N}$,*

$$\mathrm{A}_n = \langle (1,2,3),(1,2,4),\dots,(1,2,n)\rangle.$$

Demostración. Cuando $n < 3$ el resultado es trivial. Supongamos que $n \geq 3$. De las igualdades

$$(a,b)(a,c) = (a,b,c)^2 \qquad \text{y} \qquad (a,b)(c,d) = (a,b,c)(b,c,d)$$

se sigue que A_n está generado por los 3-ciclos. Como

$$(a,b,c) = (1,c,b)(1,a,b)(1,a,c)$$

para cada terna a,b,c de elementos de $\mathbb{I}_n$ distintos de 1, para concluir la demostración es 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 cierto, porque

$$(1,a,2) = (1,2,a)^2 \qquad \text{y} \qquad (1,a,b) = (1,2,b)^2(1,2,a)(1,2,b)$$

para cada par a,b de elementos de $\mathbb{I}_n$ distintos de 1 y 2. □

Teorema 2.14. *para todo $n \in \mathbb{N}$,*

$$\begin{aligned}\mathrm{A}_n &= \langle (1,2)(2,3),(1,2)(3,4),\dots,(1,2)(n-1,n)\rangle\\ &= \langle (2,3)(1,2),(3,4)(1,2),\dots,(n-1,n)(1,2)\rangle.\end{aligned}$$

Demostración. Como $(1,2)(2,3) = (2,3)(1,2)(2,3)(1,2)$ y $(1,2)(j,j+1) = (j,j+1)(1,2)$ cuando $j > 2$ es suficiente probar la primera igualdad. Por el teorema anterior, para ello es suficiente verificar que el subgrupo de A_n generado por $(1,2)(2,3),\dots,(1,2)(n-1,n)$ contiene a los 3-ciclos $(1,2,3),\dots,(1,2,n)$, lo que se sigue por inducción en j, usando que $(1,2,3) = (1,2)(2,3)$ y

$$\big((1,2)(j,j+1)(1,2,j)(1,2)(j,j+1)\big)^2 = (1,j+1,2)^2 = (1,2,j+1),$$

para todo $j \geq 3$. □

5. El conmutador y el centro de $\mathrm{S_n}$ y $\mathrm{A_n}$

El objetivo de esta sección es determinar el subgrupo conmutador y el centro de los grupos S_n y A_n.

TEOREMA 2.15. $[\mathrm{S}_n, \mathrm{S}_n] = \mathrm{A}_n$ *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

$$\operatorname{sg}([\sigma, \tau]) = \operatorname{sg}(\sigma)\operatorname{sg}(\tau)\operatorname{sg}(\sigma^{-1})\operatorname{sg}(\tau^{-1}) = 1$$

para todo $\sigma, \tau \in \mathrm{S}_n$, debido a que $\operatorname{sg}(\sigma) = \operatorname{sg}(\sigma^{-1})$ y $\operatorname{sg}(\tau) = \operatorname{sg}(\tau^{-1})$. Por el Teorema 2.13, para probar que vale la inclusión opuesta es suficiente mostrar que los 3-ciclos son conmutadores, lo cual es cierto, porque de hecho,

$$(a, b, c) = (a, b)(a, c)(a, b)(a, c)$$

para toda terna a, b, c de elementos de $\mathbb{I}_n$. Para probar que $[\mathrm{A}_n, \mathrm{A}_n] = \mathrm{A}_n$ cuando $n \geq 5$, es suficiente observar que fijado un 3-ciclo (a, b, c) existen $d, e \in \mathbb{I}_n$, distintos de a, b, c, y que

$$(a, b, c) = [(a, c, d), (a, d, e)][(a, d, e), (a, b, d)],$$

lo que se comprueba por cálculo directo. □

OBSERVACIÓN 2.16. *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*

$$H = \{\mathrm{id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

de A_4 *es normal y* A_4/H *es abeliano,* $[\mathrm{A}_4, \mathrm{A}_4] \subseteq H$. *Por otro lado, las igualdades*

$$\begin{aligned}(1, 2)(3, 4) &= [(1, 2, 3), (1, 3, 4)],\\ (1, 3)(2, 4) &= [(1, 3, 2), (1, 2, 4)],\\ (1, 4)(2, 3) &= [(1, 4, 2), (1, 2, 3)],\end{aligned}$$

muestran que la inclusión opuesta también vale.

TEOREMA 2.17. *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,

$$\sigma = (i_1, i_2, \dots, i_{r_1})(j_1, j_2, \dots, j_{r_2}) \cdots,$$

entonces tomando $\tau = (i_1, j_1, j_2)$ obtenemos

$$\tau\sigma\tau^{-1} = (j_1, i_2, \dots, i_{r_1})(j_2, i_1, j_3, \dots, j_{r_2}) \cdots \neq \sigma.$$

Si σ es un ciclo $(i_1, i_2, i_3, \dots i_r)$ de longitud al menos 3, entonces tomando $\tau = (i_1, i_2)$ obtenemos

$$\tau\sigma\tau^{-1} = (i_2, i_1, i_3, \dots i_r) \neq \sigma.$$

Finalmente, si σ es una trasposición (i_1, i_2), entonces existe $i_3 \in \mathbb{I}_n$ distinto de i_1 e i_2, y tomando $\tau = (i_1, i_3)$ obtenemos

$$\tau\sigma\tau^{-1} = (i_3, i_2) \neq \sigma.$$

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 $(i_1, i_2, i_3, i_4, \dots, i_r)$ de longitud al menos 5, entonces tomando $\tau = (i_1, i_2)(i_3, i_4)$ obtenemos

$$\tau\sigma\tau^{-1} = (i_2, i_1, i_4, i_3, i_5, \dots, i_r) \neq \sigma.$$

Finalmente, si σ es un 3-ciclo (i_1, i_2, i_3), entonces existe $i_4 \in X$ distinto de i_1, i_2 e i_3 y tomando $\tau = (i_1, i_2)(i_3, i_4)$ obtenemos

$$\tau\sigma\tau^{-1} = (i_2, i_1, i_4) \neq \sigma,$$

lo que termina la demostración. □

Observación 2.18. *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 $\mathrm{A_n}$

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 2.19. *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. Para probarlo vamos a usar el argumento desarrollado en la demostración del Teorema 2.17. Fijemos $\sigma \in H$ distinto de la identidad.

1. Si $\sigma = (i_1, i_2, \dots, i_{r_1})(j_1, j_2, \dots, j_{r_2}) \cdots$ tiene dos ciclos no triviales en su descomposición cíclica, entonces tomando $\tau = (i_1, j_1, j_2)$, obtenemos

   $$\varrho = \tau\sigma\tau^{-1}\sigma^{-1} = (i_1, j_1, j_2)(j_3, j_2, i_2) = (j_3, i_1, j_1, j_2, i_2),$$

   si $r_2 > 2$ y

   $$\varrho = \tau\sigma\tau^{-1}\sigma^{-1} = (i_1, j_1, j_2)(j_1, j_2, i_2) = (j_1, i_1)(j_2, i_2),$$

   si $r_2 = 2$.
2. Si σ es un ciclo $(i_1, i_2, i_3, i_4, i_5, \dots, i_r)$ de longitud al menos 5, entonces tomando $\tau = (i_1, i_2)(i_3, i_4)$ obtenemos

   $$\varrho = \tau\sigma\tau^{-1}\sigma^{-1} = (i_1, i_2)(i_3, i_4)(i_2, i_3)(i_4, i_5) = (i_1, i_2, i_4, i_5, i_3).$$

3. Si σ es un 3-ciclo (i_1, i_2, i_3) tomamos $\varrho = \sigma$.

De modo que tenemos tres casos:

- $\varrho = (i_1, i_2)(i_3, i_4)$ es un producto de dos 2-ciclos,
- $\varrho = (i_1, i_2, i_3, i_4, i_5)$ es un 5-ciclo,
- $\varrho = (i_1, i_2, i_3)$ es un 3-ciclo.

En el primero existe $i_5 \notin \{i_1, i_2, i_3, i_4\}$, y tomando $u = (i_2, i_5, i_3)$ obtenemos

$$u\varrho u^{-1}\varrho = (i_1, i_5)(i_2, i_4)(i_1, i_2)(i_3, i_4) = (i_1, i_4, i_3, i_2, i_5),$$

lo que nos reduce al segundo. En este, tomando $u = (i_2, i_3, i_4)$ obtenemos

$$u\varrho^{-1}u^{-1}\varrho = (i_5, i_2, i_4, i_3, i_1)(i_1, i_2, i_3, i_4, i_5) = (i_1, i_4, i_2),$$

y así 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 2.3, existe $t \in \mathrm{S}_n$ tal que $(j_1, j_2, j_3) = t(i_1, i_2, i_3)t^{-1}$. Si $t \in \mathrm{A}_n$ entonces $(j_1, j_2, j_3) \in H$ por definición. Si no, podemos tomar $k_1, k_2 \in X \setminus \{j_1, j_2, j_3\}$ distintos, y entonces

$$(j_1, j_2, j_3) = (k_1, k_2)(j_1, j_2, j_3)(k_1, k_2)^{-1} = (k_1, k_2)t(i_1, i_2, i_3)\big((k_1, k_2)\circ t\big)^{-1}.$$

Como $(k_1, k_2)t \in \mathrm{A}_n$, esto implica que $(j_1, j_2, j_3) \in H$. □

Teorema 2.20. *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 2.12, existe $\tau \in \mathrm{S}_n$ tal que $H = \{\mathrm{id}, \tau\}$. Como τ tiene orden 2, es un producto de 2-ciclos disjuntos y, en consecuencia, por el Teorema 2.3, su clase de conjugación tiene más de un elemento, lo que es imposible porque $H = \{\tau, \mathrm{id}\}$ es normal. □

Debido a que todo subgrupo de índice 2 de un grupo es invariante, del Teorema 2.19 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 2.21. *El grupo A_4 tiene las siguiente 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 $\tau \in \mathrm{A}_4$ (la clase de τ^2 en A_4/H es 1). Puesto 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 2.12, el subgrupo $H \cap \mathrm{A}_4$ de A_4 tiene orden 6, lo que contradice el item 1). □

6. Presentaciones de $\mathrm{S_n}$ y $\mathrm{A_n}$

El objetivo de esta sección es dar presentaciones de S_n y A_n. Comenzamos con el grupo simétrico.

TEOREMA 2.22. *Para cada $n \geq 2$, el grupo simétrico S_n es canónicamente isomorfo al grupo con generadores $s_1, \dots, s_{n-1}$ 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 $s_1, \dots, s_{n-1}$ sujeto 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 $s_1, \dots, s_{n-2}$ es un cociente del grupo con generadores $s_1, \dots, s_{n-2}$, 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 $C_1, \dots, C_n$ 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, para empezar,

$$C_j s_j = G' s_{n-1} s_{n-2} \cdots s_{j+1} s_j s_j = G' s_{n-1} s_{n-2} \cdots s_{j+1} = C_{j+1}$$

y

$$C_{j+1} s_j = G' s_{n-1} s_{n-2} \cdots s_{j+1} s_j = C_j,$$

para todo j. 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 penúltima igualdad se sigue de que $s_j \in G'$ porque $j < n-1$. Finalmente, si $i < j$,

$$
\begin{aligned}
C_i s_j &= G' s_{n-1} s_{n-2} \cdots s_{j+1} s_j s_{j-1} \cdots s_{i+1} s_i s_j\\
&= G' s_{n-1} s_{n-2} \cdots s_{j+1} s_j s_{j-1} s_j \cdots s_{i+1} s_i\\
&= G' s_{n-1} s_{n-2} \cdots s_{j+1} s_{j-1} s_j s_{j-1} \cdots s_{i+1} s_i\\
&= G' s_{j-1} s_{n-1} s_{n-2} \cdots s_{j+1} s_j s_{j-1} \cdots s_{i+1} s_i\\
&= G' s_{n-1} s_{n-2} \cdots s_{j+1} s_j s_{j-1} \cdots s_{i+1} s_i\\
&= C_i,
\end{aligned}
$$

donde la anteúltima igualdad se sigue de que $s_{j-1} \in G'$, porque $j-1 < n-1$. En consecuencia, cualquiera sea $s \in G$, para cada $i \leq n$ existe $i' \leq n$ tal que $C_i s = C_{i'}$, puesto que s es producto de s_j's. Dado que $1 \in G' = C_n$, en particular obtenemos 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 2.23. *Las relaciones que satisfacen $s_1,\dots,s_{n-1}$ pueden expresarse en la forma*

$$
\begin{aligned}
&s_i^2=1, &&\textit{para todo } i,\\
&(s_is_j)^2=1, &&\textit{si } j-i\ge 2,\\
&(s_is_{i+1})^3=1, &&\textit{para } i<n-1,
\end{aligned}
$$

que fue la utilizada al definir la noción general de presentación.

Teorema 2.24. *Para cada $n\ge 3$, el grupo alternado A_n es canónicamente isomorfo al grupo con generadores $t_1,\dots,t_{n-2}$ sujetos a las relaciones*

$$
\begin{aligned}
&t_1^3=1,\\
&t_i^2=1, &&\textit{para } i>1,\\
&(t_it_j)^2=1, &&\textit{si } j-i\ge 2,\\
&(t_it_{i+1})^3=1, &&\textit{para } i<n-2.
\end{aligned}
$$

Demostración. Consideremos el grupo G con generadores $t_1,\dots,t_{n-2}$ sujetos a las relaciones mencionadas arriba. Es evidente que la función

$$
\begin{aligned}
\{t_1,\dots,t_{n-2}\} &\longrightarrow \mathrm{A}_n\\
t_i &\longmapsto (i+1,i+2)(1,2)
\end{aligned},
$$

se extiende univocamente a un morfismo $\psi\colon G\to \mathrm{A}_n$. Como, por el Teorema 2.14, este morfismo es sobreyectivo, para terminar la demostración será suficiente ver que $|G|\le n!/2$. Probaremos esto mostrando que hay un producto semidirecto $G\times_\vartheta \mathbb{Z}_2$ y un morfismo sobreyectivo $\mathrm{S}_n\to G\times_\vartheta\mathbb{Z}_2$. Para empezar, es fácil ver que la función $\vartheta\colon \mathbb{Z}_2\to \operatorname{Aut} G$, dada por $\vartheta(1)(t_i)=t_i^{-1}$, es un morfismo bien definido. Por ejemplo, la relación $(t_1t_2)^3=1$ se transforma por $\vartheta(1)$ en la relación $(t_1^2t_2)^3=1$, la cual vale porque

$$t_1t_2t_1t_2t_1t_2=1\Rightarrow t_2t_1^2t_2t_1^2t_2t_1^2=1\Rightarrow t_1^2t_2t_1^2t_2t_1^2t_2=1.$$

Podemos considerar entonces el producto cruzado $G\times_\vartheta\mathbb{Z}_2$. Llamemos G' al grupo generado por los elementos $s_1,t_1,\dots,t_{n-2}$, sujetos a las relaciones

$$
\begin{aligned}
&s_1^2=t_1^3=1,\\
&s_1t_is_1=t_i^{-1} &&\text{para todo } i,\\
&t_i^2=1, &&\text{para } i>1,\\
&(t_it_j)^2=1, &&\text{si } j-i\ge 2,\\
&(t_it_{i+1})^3=1, &&\text{para } i<n-2,
\end{aligned}
$$

y escribamos $s_{i+1}=t_is_1$ para $1\le i<n-1$. La relaciones dadas arriba para $s_1,t_1,\dots,t_{n-2}$ son equivalentes a las dadas en la Observación 2.23 para $s_1,\dots,s_{n-1}$. Por lo tanto,

$$G'=\langle s_1,t_1,\dots,t_{n-2}\rangle=\langle s_1,\dots,s_{n-1}\rangle\approx \mathrm{S}_n\,.$$

Por consiguiente, para terminar la demostración es suficiente notar que existe un morfismo de grupos $\varphi\colon G'\to G\times_\vartheta\mathbb{Z}_2$, tal que $\varphi(t_i)=(t_i,0)$ y $\varphi(s_1)=(0,1)$, 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 practica 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 $\tilde\rho\colon G\to \mathrm{Fun}(X,X)$. Dicho en forma más precisa, la correspondencia

$$\begin{aligned}\mathrm{Fun}(G\times X,X) &\longrightarrow \mathrm{Fun}(G,\mathrm{Fun}(X,X))\\ \rho &\longmapsto \tilde\rho\end{aligned},$$

donde $\tilde\rho$ es la función dada por $\tilde\rho(g)(x)=\rho(g,x)$, es biunívoca. Es claro que las condiciones requeridas a ρ en la definición de acción se satisfacen si y sólo si

$$\tilde\rho(gh)=\tilde\rho(g)\circ\tilde\rho(h)\ \text{ para todo } g,h\in G \quad \text{y} \quad \tilde\rho(1)=\mathrm{id}\,.$$

En particular

$$\tilde\rho(g^{-1})\circ\tilde\rho(g)=\tilde\rho(1)=\mathrm{id}\ \text{ para todo } g,h\in G.$$

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

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

$$\tilde\rho\colon G\to \mathrm{S}_X$$

asociado a ρ. Una acción es *fiel* si su núcleo es 1. En este caso el morfismo asociado $\tilde\rho\colon G\to\mathrm{S}_X$ es inyectivo y, por lo tanto, G es isomorfo a un subgrupo de S_X. Dada una acción

$$\rho\colon G\times X\to X$$

la fórmula $[g]\cdot x = g\cdot x$ define una acción fiel $\bar\rho$ de $G/\ker\rho$ en X. La definición no depende del representante elegido, porque si $h\in\ker\rho$, entonces

$$(gh)\cdot x = g\cdot(h\cdot x) = g\cdot x \quad \text{para todo } x\in X.$$

Como

$$\tilde{\bar\rho}([g])(x)=[g]\cdot x = g\cdot x=\tilde\rho(g)(x) \quad \text{para todo } g\in G \text{ y } x\in X,$$

el triángulo

$$\begin{tikzcd} G \arrow[r, "\tilde\rho"] \arrow[d, "\pi"'] & \mathrm{S}_X \\ \frac{G}{\ker\rho} \arrow[ur, "\tilde{\bar\rho}"'] & \end{tikzcd},$$

donde π es la proyección al cociente, conmuta. Esto muestra que $\tilde{\bar\rho}$ es el morfismo inducido por $\tilde\rho$ gracias la propiedad universal del cociente, y da un método alternativo para obtener $\bar\rho$, con el cual es innecesario comprobar la buena definición.

EJEMPLO 3.1. *Todo grupo G actúa por traslaciones a izquierda sobre el conjunto G/L, de las coclases a izquierda de cada subgrupo L de G. Así, $h\cdot(gL)=hgL$. Puesto que*

$$h\cdot gL = gL \Leftrightarrow hg\in gL \Leftrightarrow h\in gLg^{-1},$$

el núcleo de esta acción es el máximo subgrupo

$$N = \bigcap_{g\in G} gLg^{-1}$$

de L que es normal en G. De ahora en más siempre consideraremos a G/L provisto de esta estructura de G-espacio.

Recordemos que para cada magma S y cada elemento $s \in S$, el símbolo l_s denota a la permutación de S definida por $l_s(t) = st$.

TEOREMA 3.2 (Cayley). *La función*

$$\begin{aligned} G &\longrightarrow \mathrm{S}_G \\ g &\longmapsto l_g \end{aligned}$$

es un morfismo inyectivo.

DEMOSTRACIÓN. Tómese $L = 1$ en el ejemplo anterior. La función del enunciado es el morfismo $\tilde{\rho}\colon G \to \mathrm{S}_G$, asociado a la acción obtenida. □

COROLARIO 3.3. *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 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 $(1,\dots,n)$. □

COROLARIO 3.4. *Todo grupo finito G es subgrupo de un grupo finito simple.*

DEMOSTRACIÓN. Por el Teorema de Cayley y la Observación 2.11, sabemos que G es isomorfo a un subgrupo de A_n, para un $n \geq 5$. Para terminar la demostración basta recordar que, por el Teorema 2.19, 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 $(1,2,\dots,n)$ generan S_n puede reformularse como sigue: dada una numeración $j_1,\dots,j_n$ de $\mathbb{I}_n$, los ciclos (j_1,j_2) y $(j_1,j_2,\dots,j_n)$ 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 3.5. *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 $2^{k'}m'$, cada uno de la forma $(x, gx, \dots, g^{|g|-1})$. Como estos ciclos son permutaciones impares si y sólo si $k' > 0$ y $2^{k-k'}m/m'$ es impar si y sólo si $k' = k$, el signo de l_g es -1 si y sólo si $k' = k \geq 1$. □

COROLARIO 3.6. *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 3.5, 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 2.12. $\square$

Ejercicio 3.7. *Pruebe que 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.*

Volvamos a la situación considerada en el Ejemplo 3.1. Supongamos que L tiene índice finito. Entonces el morfismo

$$\begin{aligned} G &\longrightarrow \mathrm{S}_{G/L}\,, \\ g &\longmapsto \tilde{\rho}(g) \end{aligned}$$

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 $N = \bigcap_{g\in G} gLg^{-1}$. 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 3.8. *Si L es un subgrupo de índice $n < \infty$ de un grupo G, entonces L contiene un subgrupo normal N de G cuyo índice en G es nh, con h un divisor de $(n-1)!$. Además, puede tomarse como N el núcleo del morfismo de G en $\mathrm{S}_{G/L}$ que manda g en $\tilde{\rho}(g)$.*

El Teorema 3.8 generaliza la Proposición 1.50, porque cuando $n = 2$, entonces $h = 1$ y $N = L$.

Corolario 3.9. *Si un grupo simple G tiene un subgrupo de índice finito $n > 1$, entonces hay un morfismo inyectivo de G en S_n. En consecuencia $|G| \le n!$.*

Demostración. Por el Teorema 3.8, si L es un subgrupo de índice n de G, entonces hay un morfismo $\varphi\colon G \to \mathrm{S}_{G/L}$, con $\ker\varphi \subseteq L$. Como L es propio y G es simple, φ es inyectivo y, en consecuencia, $|G| \le |\,\mathrm{S}_{G/L}\,| = n!$, como queríamos. $\square$

Corolario 3.10. *Los grupos infinitos simples no tienen subgrupos propios de índice finito.*

Corolario 3.11. *Supongamos que G es un grupo finito simple y que $|G| = nm$ con $n > 1$. Si G tiene subgrupo L de índice n, entonces m divide a $(n-1)!$.*

Demostración. Por la simplicidad de G, el subgrupo normal de índice nh de G, con h un divisor de $(n-1)!$, cuya existencia está garantizada por el Teorema 3.8, es uno de los subgrupos triviales 1 o G. Como $n > 1$ el segundo caso no puede darse y, así, $m = h$. $\square$

Corolario 3.12. *Supongamos que G es un grupo finito y que $|G| = mn$. Todo subgrupo L de índice n de G contiene a un subgrupo $N \triangleleft G$ cuyo índice en G es nh, con h un divisor de $((n-1)! : m)$. En particular si todos los primos que dividen a m son mayores o iguales que el máximo primo menor que n, entonces todo subgrupo de índice n de G es normal.*

Demostración. Por el Teorema 3.8, 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 $(n-1)!$. Como $[G : N]$ divide a $|G|$, también m es divisible por h. Esto implica que $h = 1$ si ningún primo menor que n divide a m, porque en este caso $(n-1)!$ y m son coprimos. $\square$

Corolario 3.13. *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 3.14. *Pruebe que si $n \ne 4$, entonces S_n no tiene subgrupos de índice t con $2 < t < n$. Pruebe también que esto es falso si $n = 4$.*

2.1. Subconjuntos estables y morfismos

Decimos que un subconjunto Y de un G-espacio X es *estable bajo la acción de* G o simplemente que es *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 que satisface

$$\varphi(g \cdot x) = g \cdot \varphi(x) \quad \text{para todo } g \in G \text{ y } x \in X.$$

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 identicas 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 sección es inyectiva, todo morfismo inyectivo es un monomorfismo, y todo morfismo sobreyectivo es un epimorfismo. Un morfismo $\varphi\colon G \to G'$ 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.

2.2. 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 3.15. *Cada conjunto X es un G-espacio vía la* acción trivial $g \cdot x = x$.

Ejemplo 3.16. *G actúa sobre si mismo por conjugación. Esto es, $g \cdot h := ghg^{-1}$. Más generalmente, G actúa por conjugación sobre cada subgrupo normal N.*

Ejemplo 3.17. *Si H y K son subgrupos de un grupo G y $K \subseteq \mathrm{N}_G(H)$, entonces K actúa sobre H por conjugación.*

Ejemplo 3.18. *Todo subgrupo H de un grupo G actúa sobre G por traslaciones a izquierda. En símbolos, $h \cdot g := hg$ para todo $h \in H$ y $g \in G$.*

Ejemplo 3.19. *G actúa sobre el conjunto $\mathrm{P}\,G$, de partes de G, por conjugación. Esto es, $g \cdot X := gXg^{-1}$.*

Ejemplo 3.20. *El conjunto* $\mathrm{Sub}\,G$*, de los subgrupos de G, es estable bajo la acción del ejemplo anterior y, así, G también actúa sobre* $\mathrm{Sub}\,G$ *por conjugación.*

Ejemplo 3.21. *G actúa sobre $\mathrm{P}\,G$ vía $g \cdot X := gX$. Esto es, por traslaciones a izquierda.*

Ejemplo 3.22. *La clase de conjugación de un subgrupo L de G es un G-espacio via $g \cdot hLh^{-1} = ghLh^{-1}g^{-1}$.*

Ejemplo 3.23. *G actúa sobre el conjunto $G\backslash L$, de las coclases a derecha de cada uno de sus subgrupos L, vía $g \cdot (Lh) = Lhg^{-1}$.*

Ejemplo 3.24. *S_n actúa sobre el anillo $k[X_1, \dots, X_n]$ de polinomios en n variables con coeficientes en un cuerpo k, via*

$$\sigma \cdot P(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

Ejemplo 3.25. *Cada subgrupo G de $\mathrm{GL}(V)$ actúa sobre V vía $g \cdot v := g(v)$. Esta es la* acción natural de G sobre V.

Ejemplo 3.26. *El grupo ortogonal $O(\mathbb{R}^n)$ actúa sobre la esfera*

$$S^{n-1} = \{x \in \mathbb{R}^n : \|x\| = 1\},$$

via $g \cdot x = g(x)$.

Ejemplo 3.27. *La* acción natural de S_X sobre X *es la definida por $\sigma \cdot x = \sigma(x)$.*

Observación 3.28. *Los núcleos de las acciones consideradas en los ejemplos anteriores son G, $\mathrm{C}_G(N)$, $K \cap \mathrm{C}_G(H)$, 1, $\mathrm{Z}\,G$, $\bigcap_{H \in \operatorname{Sub} G} N_G(H)$, 1, $\bigcap_{h \in G} \mathrm{N}_G(hLh^{-1})$, $\bigcap_{h \in G} hLh^{-1}$, 1, 1, 1 y 1, respectivamente.*

2.3. Órbitas, puntos fijos y estabilizadores

Decimos que dos elementos x e y de un G-espacio X son *conjugados* si existe $g \in G$ tal que $g \cdot x = y$. Por ejemplo, dos elementos de G son conjugados bajo la acción de G sobre si mismo introducida en el Ejemplo 3.16, si y sólo si lo son en el sentido usual, y dos subgrupos H y L de G son conjugatos (también en el sentido usual) si lo son como elementos del conjunto $\operatorname{Sub} G$, provisto de la acción de G dada en el Ejemplo 3.20. Por los axiomas de acción a izquierda, la relación $\sim$, definida por $x \sim y$ si x e y son conjugados, es transitiva y reflexiva. Como

$$y = g \cdot x \Leftrightarrow g^{-1} \cdot y = x,$$

también es simétrica. Entonces es una relación de equivalencia y, por lo tanto, 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 $\mathcal{O}X$ al conjunto de todas las órbitas. 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. Decimos que $x \in X$ es un *punto fijo* si $g \cdot x = x$ para todo $g \in G$, es decir 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 $X' \cap \mathcal{O}_x$ es un conjunto de un elemento. Notemos que el conjunto $\operatorname{PF} X$, de los puntos fijos de X, está incluído en X'. Como X' tiene exáctamente un punto de cada órbita, si X es finito, entonces

$$|X| = \sum_{x \in X'} |\mathcal{O}_x| = |\operatorname{PF} X| + \sum_{x \in X' \setminus \operatorname{PF} X} |\mathcal{O}_x|. \tag{30}$$

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 definición, 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 y que el núcleo de la acción de G sobre X es la intersección de los estabilizadores de todos los elementos de X.

PROPOSICIÓN 3.29. *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 3.30. *Si x e y están en la misma órbita, entonces sus estabilizadores son isomorfos.*

OBSERVACIÓN 3.31. *Supongamos que X es un G-espacio y tomemos $x \in X$. Por la Proposición 3.29, para cada H conjugado a G_x existe $y \in \mathcal{O}_x$ tal que $G_y = H$. En consecuencia, por los comentarios hechos en la Sección 18.3,*

$$N = \bigcap_{y \in \mathcal{O}_x} G_y$$

es el máximo subgrupo normal de G_x.

TEOREMA 3.32. *Para cada G-espacio X y cada $x \in X$, la aplicación $\Phi\colon G/G_x \to \mathcal{O}_x$, definida por $\Phi(gG_x) = g \cdot x$, es un isomorfismo de G-espacios (recuerdese que G/G_x tiene una estructura canónica de G-espacio).*

DEMOSTRACIÓN. En primer lugar, Φ está bien definida pues

$$gG_x = g'G_x \Rightarrow \text{existe } l \in G_x \text{ tal que } g' = gl \Rightarrow g' \cdot x = g \cdot (l \cdot x) = g \cdot x.$$

Además es un morfismo de G-espacios porque

$$\Phi(h \cdot gG_x) = \Phi(hgG_x) = hg \cdot x = h \cdot (g \cdot x) = h \cdot \Phi(gG_x) \quad \text{para todo } h, g \in G,$$

y es evidente que es sobreyectivo. Por último, también es inyectivo porque si $g \cdot x = g' \cdot x$, entonces $g^{-1}g' \in G_x$ y, por lo tanto, $gG_x = g'G_x$. □

COROLARIO 3.33. *Para cada G-espacio X y cada $x \in X$, si la órbita $\mathcal{O}_x$ es finita, entonces G_x tiene índice finito y*

$$|\mathcal{O}_x| = |G : G_x|.$$

Como aplicación de este resultado obtenemos la siguiente

PROPOSICIÓN 3.34. *Si k es un cuerpo finito con q elementos, entonces*

$$\begin{aligned} |\operatorname{GL}(n,k)| &= (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) \\ &= q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1). \end{aligned}$$

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 ${}^tk^{n+1}$ al espacio de los vectores columna de $n+1$ coordenadas y con e_1 al primer elemento de la base canónica de ${}^tk^{n+1}$. Como la acción natural de $\mathrm{GL}(n+1,k)$ sobre ${}^tk^{n+1}\setminus\{0\}$ es transitiva, por el Corolario 3.33,

$$q^{n+1}-1=|k^{n+1}\setminus\{0\}|=\frac{|\mathrm{GL}(n+1,k)|}{|\mathrm{GL}(n+1,k)_{e_1}|}.$$

Como el resultado de la acción de una matriz inversible arbitraria sobre e_1 es la primera columna de la matriz, $\mathrm{GL}(n+1,k)_{e_1}$ es el conjunto de las matrices cuya primera columna es e_1. Dicho de otro modo, una matriz está en $\mathrm{GL}(n+1,k)_{e_1}$ si y sólo si tiene la forma

$$\left(\begin{array}{c:ccc} 1 & \star & \cdots & \star \\ \hdashline 0 & & & \\ \vdots & & \mathrm{A} & \\ 0 & & & \end{array}\right),$$

con los $\star$'s elementos arbitrarios de k y $\mathrm{A}\in\mathrm{GL}(n,k)$. Por lo tanto

$$|\mathrm{GL}(n+1,k)_{e_1}|=q^n|\mathrm{GL}(n,k)|.$$

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. □

Combinando el Corolario 3.33 con la fórmula (30), obtenemos que, si X es finito,

$$|X|=|\mathrm{PF}\,X|+\sum_{x\in X'\setminus\mathrm{PF}\,X}|G:G_x|, \tag{31}$$

donde X' es un conjunto de representantes de las órbitas de X. Una observación que será útil más adelante es que 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. Por supuesto, en todos los casos considerados asumimos que el G espacio en cuestión es finito.

Acción de G sobre si mismo por conjugación: En este caso la fórmula (31) da la llamada *ecuación de las clases*

$$|G|=|\mathrm{Z}\,G|+\sum_{g\in X'\setminus\mathrm{Z}\,G}|G:\mathrm{C}_G(g)|,$$

en la cual X' es un conjunto de representantes de las clases de conjugación de G. Para comprobarlo basta notar que $\mathrm{PF}\,G=\mathrm{Z}\,G$ y $G_g=\mathrm{C}_G(g)$ para todo $g\in G$.

Acción de G sobre un subgrupo normal N por conjugación: En este se reduce a la igualdad

$$|G|=|\mathrm{Z}\,G\cap N|+\sum_{g\in X'\setminus\mathrm{Z}\,G}|G:\mathrm{C}_G(g)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de G incluídas en N.

Acción de G sobre SubG por conjugación: En este caso, como PF Sub G es el conjunto SubN G de los subgrupos normales de G y $G_H = \mathrm{N}_G(H)$ para todo subgrupo H de G, la fórmula (31) deviene

$$|\operatorname{Sub} G| = |\operatorname{SubN} G| + \sum_{H \in X' \setminus \operatorname{SubN} G} |G : \mathrm{N}_G(H)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de Sub G.

Acción de G sobre PG por conjugación: En este se transforma en

$$2^{|G|} = |\operatorname{PaN} G| + \sum_{S \in X' \setminus \operatorname{PaN} G} |G : \mathrm{N}_G(S)|,$$

donde X' es un conjunto de representantes de las órbitas de P G y PaN G es el conjunto de los subconjuntos S de G tales que $gSg^{-1} = S$ para todo $g \in G$.

Veamos otra aplicación del Corolario 3.33.

OBSERVACIÓN 3.35. *Fijemos un elemento g de un grupo G. Es obvio que $\langle g \rangle \subseteq \mathrm{C}_G(g)$. Además, si G es finito, entonces por el Corolario 3.33,*

$$|\mathrm{C}_G(g)| = \frac{|G|}{|\{hgh^{-1} : h \in G\}|}.$$

Por ejemplo, esta fórmula combinada con la fórmula (28) *(ver Proposición 2.2), nos dice que*

$$|\mathrm{C}_{\mathrm{S}_n}(\sigma)| = 1^{\alpha_1}\alpha_1! 2^{\alpha_2}\alpha_2! \cdots n^{\alpha_n}\alpha_n! \quad \text{para cada permutación } \sigma, \tag{32}$$

donde $(\alpha_1, \dots, \alpha_n)$ 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 (32)*, 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 3.36. *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.*

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 dados subconjuntos $\{x_1, \dots, x_k\}$ e $\{y_1, \dots, y_k\}$ de k elementos de X, existe $g \in G$ tal que $g \cdot x_1 = y_1, \dots, g \cdot x_k = y_k$.

EJEMPLO 3.37. *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, dados subconjuntos $\{x_1, \dots, x_{n-2}\}$ e $\{y_1, \dots, y_{n-2}\}$ 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 $z_1, z_2 \in \mathbb{I}_n \setminus \{y_1, \dots, y_{n-2}\}$ y considerando $\sigma' = (z_1, z_2)\sigma$, obtenemos una permutación par σ' que también satisface $\sigma'(x_i) = y_i$.*

PROPOSICIÓN 3.38. *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) $\Rightarrow$ 2) No hay duda de que G opera transitivamente sobre X. Tomemos $x \in X$. Por hipótesis, dados subconjuntos $\{x_1, \dots, x_{k-1}\}$ e $\{y_1, \dots, y_{k-1}\}$ de $k-1$ elementos de $X \setminus \{x\}$, existe $g \in G$ tal que $g \cdot x = x$ y $g \cdot x_1 = y_1, \dots, g \cdot x_{k-1} = y_{k-1}$. Esto muestra que G_x opera $(k-1)$-transitivamente sobre $X \setminus \{x\}$.

2) $\Rightarrow$ 1) Tomemos subconjuntos $\{x_1, \dots, x_k\}$ e $\{y_1, \dots, y_k\}$ 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 $h \cdot x_2 = g \cdot y_2, \dots, h \cdot x_{k-1} = g \cdot y_{k-1}$. Pero entonces $(g^{-1}h) \cdot x_1 = y_1, \dots, (g^{-1}h) \cdot x_k = y_k$. □

2.4. Contando órbitas

Para cada G-espacio X y cada elemento g de G, designamos con $\operatorname{PF}_g X$ al conjunto $\{x \in X : g \cdot x = x\}$, de los puntos de X fijados por g. Recordemos que el símbolo $\mathcal{O}X$ denota al conjunto de órbitas de la acción. El siguiente resultado es conocido como lema de Burnside, quizás debido a que Burnside lo citó en su libro “On the Theory of Groups of Finite Order”, atribuyéndoselo a Frobenius, pero en realidad ya era conocido por Cauchy.

Teorema 3.39. *Para cada G-espacio finito X, los cardinales de los conjuntos* $\operatorname{PF}_g X$ *y* $\mathcal{O}X$ *están relacionados por la siguiente igualdad:*

$$|\mathcal{O}X||G| = \sum_{g \in G} |\operatorname{PF}_g X|.$$

Demostración. En $\sum_{g \in G} |\operatorname{PF}_g X|$ cada $x \in X$ es contado $|G_x|$ veces (pues G_x consiste de todos los $g \in G$ tales que $x \in \operatorname{PF}_g X$). 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 $|\mathcal{O}X||G| = \sum_{g \in G} |\operatorname{PF}_g X|$, como queremos. □

Ejemplo 3.40. *La cantidad de clases de conjugación de un grupo finito G es igual a*

$$\frac{1}{|G|} \sum_{g \in G} |\operatorname{C}_G(g)|,$$

En efecto, para la acción de G sobre si mismo vía conjugación,

$$\operatorname{PF}_g G = \{h \in G : ghg^{-1} = h\} = \{h \in G : h^{-1}gh = g\} = \operatorname{C}_G(g).$$

Corolario 3.41. *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* $\operatorname{PF}_g X = \emptyset$.

Demostración. Como X es transitivo, tiene una sóla órbita. En consecuencia, por el Teorema 3.39,

$$|G| = \sum_{g \in G} |\operatorname{PF}_g X|$$

y, como $|\operatorname{PF}_1 X| = |X| > 1$, debe existir $g \in G$ tal que $\operatorname{PF}_g X = \emptyset$. □

Lema 3.42. *Fijemos $n \in \mathbb{N}$ y $q \in \mathbb{Q}$. Existe sólo una cantidad finita de n-uplas* $(i_1, \dots, i_n)$ *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 $(i_1, \dots, i_n)$ de números naturales tales que $i_1 \le \cdots \le i_n$ y $q = \sum_{j=1}^{n} 1/i_j$. Pero esto es cierto, porque en cada una de estas n-uplas $i_1 \le n/q$ y, por la hipótesis inductiva, para cada número natural $k \le n/q$ sólo hay una cantidad finita de $(n-1)$-uplas $(i_2, \dots, i_n)$ que satisfacen $q - 1/k = \sum_{j=2}^{n} 1/i_j$. □

Teorema 3.43. *Para cada $n \ge 1$, sólo hay una cantidad finita de clases de isomorfismos de grupos finitos con 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 $\{g_1, \dots, g_n\}$ 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 $g_j \in \mathrm{Z}\, G$. Por otra parte, por el Lema 3.42, dicho valor está acotado por un $M > 0$. En consecuencia $|G| \le M$, y para concluir la demostración basta notar que sólo hay finitos grupos no isomorfos de orden menor o igual que M. □

Ejercicio 3.44. *Pruebe que si un grupo G contiene un elemento de orden $n > 1$ y dos clases de conjugación, entonces $|G| = 2$.*

3. 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 3.45 (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 $(g_1, \dots, g_p)$ tales que $g_1 \cdots g_p = 1$. El grupo cíclico $\mathbb{Z}_p$ actúa sobre X vía

$$i \cdot (g_1, \dots, g_p) = (g_{1+i}, \dots, g_n, g_1, \dots, g_i).$$

Los puntos fijos de X son las p-uplas constantes $(g, \dots, g)$ 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 (30) 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 abajo indica la manera correcta de hacerlo.

Corolario 3.46. *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 sólo usaremos que el Teorema de Cauchy vale cuando G es abeliano. Bajo esta hipótesis es posible probar el 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 3.47. *Supongamos que P es un p-subgrupo de Sylow de G y que H 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. Entonces, por el Tercer teorema del isomorfismo,

$$H \cap P \lhd H \quad \text{y} \quad HP/P \approx H/H \cap P,$$

de lo cual se sigue que

$$|HP| = [HP : P]|P| = [H : H \cap P]|P|$$

es una potencia de p. En consecuencia, como $P \cup H \subseteq HP$, y P es un p-grupo maximal, $H \leq P$. $\square$

Dado un grupo finito G, designamos con el símbolo $\mathrm{Syl}_p\, G$ al conjunto de los p-subgrupos de Sylow de G.

Teorema 3.48 (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 mostraremos 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 es cierto cuando $|G|/p < n$ y que $|G|/p = n$. 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. Bajo esta hipótesis, de la ecuación de las clases

$$|G| = |\,\mathrm{Z}\, G| + \sum_{g \in X' \setminus \mathrm{Z}\, G} |G : \mathrm{C}_G(g)|,$$

se sigue que p divide a $|\,\mathrm{Z}\, G|$. En consecuencia, por el Lema 3.45, el centro de G tiene un elemento g de orden p. Como g es central, $\langle g\rangle \lhd G$. Además p divide al orden de $G/\langle g\rangle$, 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

$$|P| = |g||P'| = p|P'|$$

demuestra que P es un p-subgrupo de Sylow de G. Ahora tomemos $P\in \operatorname{Syl}_p G$ y llamemos X a su clase de conjugación. Cada p-subgrupo H de G actúa por conjugación sobre X. Denotemos con $\operatorname{PF}_H X$ al conjunto de los puntos fijos de X bajo esta acción. Por el Lema 3.47,

$$\operatorname{PF}_H X = \{gPg^{-1} : H\subseteq \mathrm{N}_G(gPg^{-1})\} = \{gPg^{-1} : H\subseteq gPg^{-1}\}.$$

Por otra parte

$$|\operatorname{PF}_H X| \cong |X| \pmod{p},$$

puesto que $X\setminus \operatorname{PF}_H X$ es una unión disjunta de órbitas no triviales y, por el Corolario 3.33, el cardinal de cada órbita no trivial de X es una potencia positiva de p. Así,

$$|\{gPg^{-1} : H\subseteq gPg^{-1}\}| \cong |X| \pmod{p}.$$

Como $\{gPg^{-1} : P\subseteq gPg^{-1}\} = \{P\}$, tomando $H=P$ en esta igualdad, concluímos que $|X|\cong 1 \pmod{p}$ y, en consecuencia, que

$$|\{gPg^{-1} : H\subseteq gPg^{-1}\}| \cong 1 \pmod{p}.$$

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 $H=1$. □

Corolario 3.49. *Supongamos que G es un grupo finito y que p es un primo que divide a $|G|$. La cantidad de p-subgrupos de Sylow de G es $|G:\mathrm{N}_G(P)|$, donde $P\in\operatorname{Syl}_p G$ es arbitrario.*

Demostración. Dado que la acción de G sobre $\operatorname{Syl}_p G$ por conjugación es transitiva, $|\operatorname{Syl}_p G| = |G:G_P| = |G:\mathrm{N}_G(P)|$. □

Corolario 3.50. *Si G es un grupo de orden $p^r m$ con p primo y m coprimo con p, entonces $|\operatorname{Syl}_p G|$ divide a m.*

Demostración. Es una consecuencia inmediata del Corolario 3.49. □

Corolario 3.51. *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) ⇒ 2) Es trivial.

2) ⇒ 3) Por el item 2) del Teorema 3.48.

3) ⇒ 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 3.48, está incluído en G. □

Proposición 3.52. *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 $P_i \le G'$, 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 $G' = G$. $\square$

Observación 3.53. *Dados un subgrupo L de un grupo finito G y un divisor primo p de $|L|$, consideremos el conjunto $\operatorname{Syl}_p^L G$, de todos los p-subgrupos de Sylow de G que incluyen a un p-subgrupo de Sylow de L. Si $P \in \operatorname{Syl}_p^L G$, entonces $P \cap L \in \operatorname{Syl}_p H$, simplemente porque es un p-subgrupo de L que incluye a un p-subgrupo de Sylow P', y, por lo tanto, coincide con P'. Esto prueba que la función*

$$\begin{aligned} \operatorname{Syl}_p^L G &\longrightarrow \operatorname{Syl}_p L\ , \\ P &\longmapsto P_L \end{aligned}$$

donde $P_L := P \cap L$, está bien definida. Además es sobreyectiva, porque, por el item 3) del Teorema 3.48, todo subgrupo de Sylow de L está incluído en un subgrupo de Sylow de G. En consecuencia,

$$|\operatorname{Syl}_p L| \le |\operatorname{Syl}_p G|.$$

Ahora fijemos $P \in \operatorname{Syl}_p^L G$ y tomemos $P' \in \operatorname{Syl}_p G$ arbitrario. Por el item 2) del Teorema 3.48 sabemos que existe $g \in G$ tal que $P' = gPg^{-1}$, de lo cual se sigue que

$$gP_Lg^{-1} = P' \cap gLg^{-1}.$$

Por consiguiente, si L es normal, entonces $\operatorname{Syl}_p^L G = \operatorname{Syl}_p G$ (en particular, cada p-subgrupo normal de G está incluído en todos los p-subgrupos de Sylow de G). Además

$$PL/L \in \operatorname{Syl}_p(G/L),$$

porque $|PL/L| = |P/(P\cap L)|$ es una potencia de p y

$$|G/L : PL/L| = |G : PL|$$

es coprimo con p. Por último, como todos los elementos de $\operatorname{Syl}_p(G/L)$ son conjugados a PL/L, todos los subgrupos de Sylow de G/L son de la forma QL/L, con $Q \in \operatorname{Syl}_p G$.

Proposición 3.54. *Si N es un subgrupo normal de un grupo finito G y p es un primo que divide a $|N|$, entonces $|\operatorname{Syl}_p N|$ divide a $|\operatorname{Syl}_p G|$. Además*

$$\frac{|\operatorname{Syl}_p G|}{|\operatorname{Syl}_p N|} = \frac{|\mathrm{N}_G(P_N)|}{|\mathrm{N}_G(P)|} = \frac{|G:N||\mathrm{N}_N(P_N)|}{|\mathrm{N}_G(P)|},$$

donde P_N y P son p-subgrupos de Sylow arbitrarios de N y P, respectivamente.

Demostración. G actúa sobre $\operatorname{Syl}_p N$ por conjugación, porque

$$gP_Ng^{-1} \subseteq gNg^{-1} = N \qquad \text{para todo } P_N \in \operatorname{Syl}_p N \text{ y } g \in G.$$

Además, esta acción es transitiva debido a que lo es su restricción a N y, dado que $\mathrm{N}_G(P_N)$ es el estabilizador de P_N para la acción de G,

$$|\operatorname{Syl}_p N| = |G : \mathrm{N}_G(P_N)|.$$

Fijemos P_N y tomemos $P \in \operatorname{Syl}_p G$ tal que $P \cap N = P_N$. Como

$$gP_Ng^{-1} = g(P\cap N)g^{-1} = gPg^{-1} \cap gNg^{-1} = gPg^{-1} \cap N = P \cap N = P_N$$

para todo $g \in \mathrm{N}_G(P)$, el grupo $\mathrm{N}_G(P)$ está incluído en $\mathrm{N}_G(P_N)$. En consecuencia,

$$|\operatorname{Syl}_p N| = |G : \mathrm{N}_G(P_N)| \quad \text{divide a} \quad |G : \mathrm{N}_G(P)| = |\operatorname{Syl}_p G|.$$

Finalmente

$$\frac{|\operatorname{Syl}_p G|}{|\operatorname{Syl}_p N|} = \frac{|G:\mathrm{N}_G(P)|}{|G:\mathrm{N}_G(P_N)|} = \frac{|\mathrm{N}_G(P_N)|}{|\mathrm{N}_G(P)|} = \frac{|G:N||\mathrm{N}_N(P_N)|}{|\mathrm{N}_G(P)|},$$

donde la última igualdad se sigue de que $|N:\mathrm{N}_N(P_N)| = |\operatorname{Syl}_p N| = |G:\mathrm{N}_G(P_N)|$. □

PROPOSICIÓN 3.55. *Si N es un subgrupo normal de un grupo finito G y p es un primo que divide a $|G/N|$, entonces $|\operatorname{Syl}_p(G/N)|$ divide a $|\operatorname{Syl}_p G|$.*

DEMOSTRACIÓN. Es evidente que G actúa sobre $\{PN/N : P \in \operatorname{Syl}_p G\}$ por conjugación y que esta acción es transitiva. Entonces, puesto que $\mathrm{N}_G(P)$ está incluído en el estabilizador $G_{\frac{PN}{N}}$ de PN/N y que, por la Observación 3.53,

$$|\operatorname{Syl}_p(G/N)| = |\{PN/N : P \in \operatorname{Syl}_p G\}| = |G : G_{\frac{PN}{N}}|,$$

el cardinal de $\operatorname{Syl}_p(G/N)$ divide a $|G:\mathrm{N}_G(P)| = |\operatorname{Syl}_p G|$. □

TEOREMA 3.56 (Frattini). *Si N es un subgrupo normal de un grupo finito G y P es un p-subgrupo de Sylow de N, entonces $G = N\,\mathrm{N}_G(P)$. En consecuencia, P es un subgrupo normal de N si y sólo si es un subgrupo normal de G.*

DEMOSTRACIÓN. Tomemos $g \in G$. Como N es normal, $gPg^{-1} \subseteq gNg^{-1} = N$. Por lo tanto, por el item 2) del Teorema de Sylow, existe $n \in N$ tal que $ngPg^{-1}n^{-1} = P$. Así, $g = n^{-1}ng \in N\,\mathrm{N}_G(P)$. □

COROLARIO 3.57. *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 3.63, 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. □

3.1. Algunos ejemplos

El objetivo de esta subsección es determinar los subgrupos de Sylow de algunos grupos finitos.

EJEMPLO 3.58. *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 3.59. *Consideremos ahora el grupo simétrico S_4. Dado que es 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. Como 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 el subgrupo

$$N := \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

de S_4 es invariante, está incluído en todos los 2-subgrupos de Sylow de S_4. Por lo tanto, estos son los subgrupos $P_\sigma := \langle\sigma, N\rangle$, con $\sigma \in \mathrm{S}_4 \setminus N$ un elemento cuyo orden es una potencia de 2. Por ejemplo, podemos tomar como σ a un 4-ciclo. Más aún, por el Teorema 2.3 y el item 2) del Teorema de Sylow, es claro que en todos los 2-subgrupos de Sylow de S_4, y no sólo en *algunos, σ es un 4-ciclo. 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*

$$P_{(1,2,3,4)} = \{\mathrm{id}, (1,3), (2,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,2,3,4), (1,4,3,2)\},$$
$$P_{(1,2,4,3)} = \{\mathrm{id}, (1,4), (2,3), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,2,4,3), (1,3,4,2)\}$$

y

$$P_{(1,3,2,4)} = \{\mathrm{id}, (1,2), (3,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,3,2,4), (1,4,2,3)\}.$$

Finalmente, como $P_{(1,2,3,4)}$ está generado por las permutaciones

$$\sigma = (1,2,3,4) \quad y \quad \tau = (1,4)(2,3),$$

y $\sigma^4 = \tau^2 = \tau\sigma\tau^{-1}\sigma = \mathrm{id}$, los grupos $P_{(1,2,3,4)}$, $P_{(1,2,4,3)}$ y $P_{(1,3,2,4)}$ son isomorfos a D_4.

EJEMPLO 3.60. *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 $N \approx \mathbb{Z}_2 \times \mathbb{Z}_2$ es su único 2-subgrupo de Sylow.

EJEMPLO 3.61. *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

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

Recordemos también que

- *Los elementos x^iy 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.*
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 $\langle x^t\rangle \lhd D_n$ 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 $K_i := \langle x^iy, x^t\rangle = \langle x^t\rangle\langle x^iy\rangle$, donde la última igualdad vale porque $\langle x^t\rangle$ es normal. De hecho, como

$$|\langle x^t\rangle\langle x^iy\rangle| = \frac{|\langle x^t\rangle||\langle x^iy\rangle|}{|\langle x^t\rangle \cap \langle x^iy\rangle|} = \frac{2^m \times 2}{1} = 2^{m+1},$$

todos los K_i son, efectivamente, 2-subgrupos de Sylow. Puesto que

$$K_i = \langle x^iy, x^t\rangle = \{x^{tj+i}y, x^{tj} : 0 \leq j < 2^m\},$$

es claro que $K_i = K_{i'}$ si y sólo si $i' \cong i \pmod{t}$. Así, los 2-subgrupos de Sylow de D_n son exactamente $K_0, \dots, K_{t-1}$. Para ver que K_i es isomorfo a D_{2^m} es suficiente notar que tiene orden 2^{m+1} y que los elementos x^iy y x^t generan K_i y satisfacen

$$(x^t)^{2^m} = 1, \quad (x^iy)^2 = 1 \quad y \quad (x^iy)x^t(x^iy)^{-1} = x^{-t}.$$

Ejemplo 3.62. *Recordemos que el grupo cuaterniónico generalizado H_n está generado por dos elementos x e y sujetos a las relaciones*

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

y que

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

Recordemos también que

- *Los elementos x^iy 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 $n = 2^mt$ 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 (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 $t = p^uv$ con v coprimo con p, entonces $\langle x^{2^{m+1}v} \rangle$ tiene orden p^u y es invariante. Consideremos 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 2-subgrupos de Sylow de H_n son algunos de los subgrupos $L_i := \langle x^iy, x^t \rangle = \langle x^t \rangle \langle x^iy \rangle$, donde la última igualdad vale porque $\langle x^t \rangle$ es invariante. Para ver cuales de estos lo son, observemos que $\langle x^iy \rangle \cap \langle x^t \rangle = \{1, x^n\}$ porque

$$(x^iy)^2 = x^iyx^iy^{-1}y^2 = y^2 = x^n, \quad (x^iy)^3 = x^{n+i}y \quad y \quad (x^iy)^4 = x^{2n} = 1.$$

Por consiguiente,

$$|\langle x^t \rangle \langle x^iy \rangle| = \frac{|\langle x^t \rangle||\langle x^iy \rangle|}{|\langle x^t \rangle \cap \langle x^iy \rangle|} = \frac{2^{m+1} \times 4}{2} = 2^{m+2},$$

lo cual muestra que, de hecho, todos los L_i son 2-subgrupos de Sylow. Puesto que

$$L_i = \langle x^iy, x^t \rangle = \{x^{tj+i}y, x^{tj} : 0 \le j < 2^{m+1}\},$$

es claro que $L_i = L_{i'}$ si y sólo si $i' \cong i \pmod{t}$. 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_{2m} es suficiente notar que tiene orden 2^{m+2} y que x^iy y x^t generan L_i y satisfacen

$$(x^t)^{2^m}(x^iy)^{-2} = 1 \quad y \quad (x^iy)x^t(x^iy)^{-1}x^t = 1.$$

Ejemplo 3.63. *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. Veamos cuantos hay. Como*

- *Los grupos cíclicos de orden p tienen $p - 1$ generadores,*
- *Por el Teorema 2.1, los únicos elementos de orden p de S_p son los p ciclos, y*

- S_p *tiene* $(p-1)!$ *p-ciclos (como fué probado al comienzo de la Sección 1 del Capítulo 2), en* S_p *hay*

$$(p-2)! = \frac{(p-1)!}{p-1}$$

p-subgrupos de Sylow. En consecuencia, por el item (1) del Teorema de Sylow

$$(p-2)! \cong 1 \pmod{p},$$

que es lo que dice el famoso Teorema de Wilson.

Ejemplo 3.64. *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 3.34 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* $\mathrm{GL}(n,k)$.

3.2. 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 3.65 (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 $G \approx \mathbb{Z}_{pq}$.*
- *Si G no es abeliano, entonces q divide a $p-1$, el conjunto*

$$R = \{r \in \mathbb{N} : 1 < r < p \text{ y } r^q \cong 1 \pmod{p}\}$$

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 3.13, 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 $G = \langle g\rangle \times \langle k\rangle \approx \mathbb{Z}_{pq}$. Supongamos entonces que $\langle k\rangle$ no es normal. Como $\langle g\rangle$ si lo es, existe $0 \le r_1 < p$ tal que $kgk^{-1} = g^{r_1}$, y un argumento inductivo muestra que $k^i g k^{-i} = g^{r_1^i}$ para todo $i > 1$, por lo que

$$g^{r_1^q} = k^q g k^{-q} = g,$$

lo cual implica que $r_1^q \cong 1 \pmod{p}$. Por otra parte, dado que la igualdad $kgk^{-1} = 1$ es imposible y que G no es conmutativo, debe ser $r_1 > 1$. Por lo tanto, como q es primo, q es el orden de r_1 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_1 es una raíz, existe $\alpha < q$ tal que $r_1^\alpha \cong r_0 \pmod{p}$, donde r_0 es el mínimo de los enteros r tales que

$$1 < r < p \qquad \text{y} \qquad r^q \cong 1 \pmod{p}.$$

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

$$h^q = (k^\alpha)^q = (k^q)^\alpha = 1 \quad \text{y} \quad hgh^{-1} = k^\alpha g k^{-\alpha} = g^{r_1^\alpha} = g^{r_0},$$

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, sabemos que $\mathbb{Z}_p^*$ tiene al menos un elemento r de orden q, y por el Ejemplo 1.135, sabemos también que para cada uno existe un grupo de orden pq, generado por elementos g y h, de órdenes p y q respectivamente, que satisfacen $hgh^{-1} = g^r$. Pero tanta variedad es ilusoria, porque, como lo muestra el teorema anterior, todos estos grupos son isomorfos.

Ejercicio 3.66. *¿Cuántos elementos tiene el grupo $\langle x, y | x^5, y^3, yxy^{-1} = x^2\rangle$?*

En el resto de esta subsección denotaremos con n_p a la cantidad de p-subgrupos de Sylow de un grupo finito G.

Proposición 3.67. *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 3.50, 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. Por el item 1) del Teorema de Sylow, en el segundo $p \cong 1 \pmod{q}$, por lo que $p > q$. Puesto que, nuevamente por el Corolario 3.50 y el item 1) del Teorema de Sylow, $n_p \mid q$ y $n_p \cong 1 \pmod{p}$, esto implica que $n_p = 1$, y así G tiene un único p-subgrupo de Sylow, el cual es normal, por el Corolario 3.51. 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. □

Proposición 3.68. *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 $h_p, h_q \geq 1$ por el Corolario 3.51 y, por lo tanto,

$$\begin{aligned} |(G \setminus S) \cup 1| &= 2pq - \big((h_p p + 1)(p-1) + (h_q q + 1)(q-1)\big) \\ &\leq 2pq - \big((p+1)(p-1) + (q+1)(q-1)\big) \\ &= 2pq - (p^2 - 1 + q^2 - 1) \\ &= -(q-p)^2 + 2 \leq -2, \end{aligned}$$

lo que es absurdo. □

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 3.12 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 3.12, 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 $n_7 \cong 1 \pmod 7$ 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 3.12, 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 $n_5 \cong 1 \pmod 5$ 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 $n_7 \cong 1 \pmod 7$ 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 3.12, 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 2.12 y el Corolario 3.9, 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 (¿porqué?). Por el item 1) del Teorema de Sylow y el Corolario 3.50 sabemos que $n_2 \in \{1, 3, 5, 15\}$ y $n_5 \in \{1, 6\}$. Por el Corolario 3.51, 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 3.49, sabemos que si $n_2 = 3$, entonces G tiene un subgrupo de índice 3. Pero esto es imposible, porque por el Teorema 3.8, 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 3.49, 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 3.8. Así pues, el índice de $\langle P_1, P_2\rangle$ en G es 5 y podemos tomar $H = \langle P_1, P_2\rangle$.

4. p-Grupos finitos

En esta sección establecemos algunas propiedades básicas de los p-grupos finitos.

TEOREMA 3.69. *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 3.70. *Todo subgrupo normal de orden p de un p-grupo G está incluído en el centro de G.*

COROLARIO 3.71. *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 3.69 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 3.72. *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 3.69, los grupos $\mathrm{Z}\,G$ y $G/\mathrm{Z}\,G$ tienen orden p y, por eso mismo son cíclicos, lo que contradice la Proposición 1.153.

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). Por la Observación 1.113 para ello basta notar que si H_1 y H_2 son dos subgrupos distintos de orden p de G, entonces $H_1 \cap H_2 = 1$ y $H_1H_2 = G$. □

Corolario 3.73. *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 3.69 sabemos que $\mathrm{Z}\,G \neq 1$ y, como G no es abeliano, $\mathrm{Z}\,G \neq G$. Además, por la Proposición 1.153, 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 3.70, el único subgrupo normal de orden p de G es $\mathrm{Z}\,G$. □

Teorema 3.74. *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 $p-1$. Tomemos uno 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 3.75. *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 sabemos que $H \triangleleft G$. Además, por el Corolario 1.92, el cociente G/H no tiene subgrupos no triviales y, en consecuencia, debido al Corolario 3.71, su cardinal es p. □

Observación 3.76. *Supongamos que H es un subgrupo propio de un p-grupo finito G. Por el Teorema 3.74, 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 3.71, para cada* $j < i$ *hay una cadena*

$$\mathrm{N}_G^j(H) = G_{\alpha_j} \subsetneq G_{\alpha_j+1} \subsetneq \cdots \subsetneq G_{\alpha_{j+1}-1} \subsetneq G_{\alpha_{j+1}} = \mathrm{N}_G^{j+1}(H),$$

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 3.77. *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 3.48. Supongamos que $n > 0$ y que el teorema vale para subgrupos de G de orden p^{m+1}. Designemos con

$$P_1, \dots, P_u \qquad \text{y} \qquad Q_1, \dots, Q_v$$

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 dado Q_j, 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 dado, 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 $u \cong v \pmod{p}$. Con esto en mente fijemos P_i y supongamos que

$$Q_{j_1}, \dots, Q_{j_{v'}}$$

son los Q_j's contenidos en P_i. Debemos mostrar que $v' \cong 1 \pmod{p}$. Por la Observación 3.76 sabemos que $v' \geq 1$. Si $v' = 1$, entonces es obvio que $v' \cong 1 \pmod{p}$. Analizemos que ocurre cuando $v' > 1$. Por el Corolario 3.75, cada Q_{j_l} es un subgrupo normal de P_i. Por consiguiente $Q_{j_1}Q_{j_2} = P_i$. Por la Proposición 1.43, esto implica que $D_1 = Q_{j_1} \cap Q_{j_2}$ tiene orden p^{m-1}. Además $D_1 \triangleleft P_i$ porque es la intersección de dos subgrupos normales de P_i. Por el Corolario 3.72, el cociente P_i/D_1 es abeliano y tiene $p+1$ subgrupos de orden p. En consecuencia, en el conjunto

$$\{Q_{j_1}, \dots, Q_{j_{v'}}\}$$

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 está 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

$$\{Q_{j_1}, \dots, Q_{j_{v'}}\},$$

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 $\{Q_{j_1},\dots,Q_{j_{v'}}\}$ 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 están incluídos en $Q_{j_{l_4}}$ y escribamos $D_3 = Q_{j_1} \cap Q_{j_{l_4}}$. En $\{Q_{j_1},\dots,Q_{j_{v'}}\}$ 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 $\{Q_{j_1},\dots,Q_{j_{v'}}\}$ que contienen a D_1, D_2 o D_3. Si $v' = 3p+1$ esto termina la demostracón, y si no podemos continuar con este procedimiento hasta que todos los elementos de $\{Q_{j_1},\dots,Q_{j_{v'}}\}$ estén listados. $\square$

Corolario 3.78. *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. $\square$

Observación 3.79. *Supongamos que N es un subgrupo normal de un p-grupo finito G. Fijemos $m < n$ tales que $p^m \le |N|$ y $p^n \le |G|$ y designemos con X al conjunto de los subgrupos de orden p^n de G cuya intersección con N es un subgrupo de orden p^m de G (X puede ser vacío). Como N es normal, G actúa sobre X por conjugación, y los puntos fijos de X bajo esta acción son los subgrupos normales de G que pertenecen a X. Notemos ahora que $|\operatorname{PF} X| \cong |X| \pmod{p}$, porque $X \setminus \operatorname{PF} X$ es una unión disjunta de órbitas no triviales, y, por el Corolario 3.33, el cardinal de cada una de esta órbitas es una potencia positiva de p. Así,*

$$|\{P \in X : P \text{ es un subgrupo normal de } G\}| \cong |X| \pmod{p}.$$

En consecuencia, por el Teorema 3.77, si N un subgrupo normal de un p-grupo finito G y

$$|N| \le p^n \le |G|,$$

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 3.69, si $n > 0$, entonces 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 3.80. *El grupo $G_1 = \langle g, h | g^{p^2}, h^p, hgh^{-1}g^{-p-1}\rangle$ tiene p^3 elementos.*

Demostración. El subgrupo $\langle g\rangle$ de G_1 es normal, $|g| \le p^2$ y $|G_1/\langle g\rangle| \le p$. Por lo tanto, $|G_1| \le p^3$. 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 $(1+p)^p \cong 1 \pmod{p^2}$, la aplicación

$$\begin{aligned} C_{p^2} &\xrightarrow{\psi} C_{p^2} \quad, \\ x^i &\longmapsto x^{i(p+1)} \end{aligned}$$

es un automorfismo de orden p y, por consiguiente, la correspondencia

$$\begin{aligned} C_p &\xrightarrow{\varsigma} \operatorname{Aut} C_{p^2} \ , \\ y^j &\longmapsto \psi^j \end{aligned}$$

es un morfismo. Consideremos el producto semidirecto $C_{p^2} \times_\varsigma C_p$ 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 $\xi\colon G_1 \to C_{p^2} \times_\varsigma C_p$ tal que $\xi(g) = \hat{x}$ y $\xi(h) = \hat{y}$. Como ξ es sobreyectivo y $|C_{p^2} \times_\varsigma C_p| = p^3$, esto termina la demostración. $\square$

LEMA 3.81. *El grupo* $G_2 = \langle g, h, k | g^p, h^p, k^p, ghg^{-1}h^{-1}, gkg^{-1}k^{-1}, hkh^{-1}k^{-1}g^{-1} \rangle$ *tiene* p^3 *elementos.*

DEMOSTRACIÓN. Notemos que el subgrupo $\langle g \rangle$ de G_2 es normal, $|g| \le p$ y $|G_2/\langle g \rangle| = p^2$. Por lo tanto, $|G_2| \le p^3$. 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

$$\begin{aligned} C_p \times C_p &\xrightarrow{\psi} C_p \times C_p \ , \\ (y^i, y^j) &\longmapsto (y^{i-j}, y^j) \end{aligned}$$

donde $C_p = \langle y \rangle$ es un grupo cíclico con p elementos, es un automorfismo de orden p, por lo que la correspondencia

$$\begin{aligned} C_p &\xrightarrow{\varsigma} \operatorname{Aut}(C_p \times C_p) \\ y^k &\longmapsto \psi^k \end{aligned}$$

es un morfismo. Tomemos el producto semidirecto $(C_p \times C_p) \times_\varsigma C_p$ y escribamos $\widehat{y}_1 = (y, 0, 0)$, $\widehat{y}_2 = (0, y, 0)$ y $\widehat{y}_3 = (0, 0, y)$. Puesto que

$$\hat{y}_1^p = \hat{y}_2^p = \hat{y}_3^p = 1, \quad \hat{y}_1\hat{y}_2 = \hat{y}_2\hat{y}_1, \quad \hat{y}_3\hat{y}_1 = \hat{y}_1\hat{y}_3 \quad \text{y} \quad \hat{y}_3\hat{y}_2 = \hat{y}_1^{-1}\hat{y}_2\hat{y}_3,$$

hay un morfismo $\xi\colon G_2 \to (C_p \times C_p) \times_\varsigma C_p$ tal que $\xi(g) = \hat{y}_1$, $\xi(h) = \hat{y}_2$ y $\xi(k) = \hat{y}_3$. Como ξ es sobreyectivo y $|(C_p \times C_p) \times_\varsigma C_p| = p^3$, esto termina la demostración. □

NOTA 3.82. *En las demostraciones de los Lemas 3.80 y 3.81 se probó más que lo establecido en los enunciados. Específicamente, en la del primero que* G_1 *es producto semidirecto interno de los subgrupos* $\langle g \rangle$ *(de orden* p^2*) y* $\langle h \rangle$ *(de orden* p*), y en la del segundo 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 3.83 (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 *introducido en el Lema 3.80 o al grupo* G_2 *introducido en el Lema 3.81.*

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 3.13 el subgrupo de G generado por g es normal. En consecuencia $h^p \in \langle g \rangle$ porque $|G/\langle g \rangle| = p$, 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 $0 \le j < p^2$. Como

$$1 = h^{p^2} = g^{pj},$$

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

$$G \approx \langle g \rangle \times \langle h \rangle \approx \mathbb{Z}_{p^2} \times \mathbb{Z}_p$$

por el Teorema 1.111 y la Proposición 1.124.

r > 1: Un argumento inductivo prueba que $h^i g h^{-i} = g^{r^i}$ para todo $i \geq 1$. En particular $g = h^p g h^{-p} = g^{r^p}$, por lo que $r^p \cong 1 \pmod{p^2}$. Puesto que

$$(1+p)^p \cong 1 \pmod{p^2}$$

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 $1 + p \cong r^{\alpha} \pmod{p^2}$. 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 antes, existe $0 \leq t < p$ 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, $G \approx D_4$, y 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, $G \approx H_2$.

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

$$(g^{-t(1+p)}h)^l = g^{-t(1+p)(1+\cdots+(1+p)^{l-1})} h^l = g^{-t(1+p)\frac{(1+p)^l - 1}{p}} h^l.$$

Como $(1+p)^p \cong 1 + p^2 \pmod{p^3}$ porque $p > 2$, de la fórmula anterior se sigue en particular que

$$(g^{-t(1+p)}h)^p = g^{-t(1+p)\frac{(1+p)^p - 1}{p}} h^p = g^{-t(1+p)p} h^p = g^{-tp} h^p = 1.$$

Dado que

$$(g^{-t(1+p)}h) g (g^{-t(1+p)}h)^{-1} = g^{-t(1+p)} h g h^{-1} g^{t(1+p)} = g^{-t(1+p)} g^{1+p} g^{t(1+p)} = g^{1+p},$$

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, $G \approx G_1$.

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 $G/\langle g \rangle$. Por el Teorema 1.111, como $\langle h \rangle \cap \langle k \rangle = 1$ y $\langle g \rangle \cap \langle h, k \rangle = 1$, el grupo G es producto directo interno de los subgrupos $\langle g \rangle$, $\langle h \rangle$ y $\langle k \rangle$. Entonces, por la Proposición 1.124, es isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$.

G no es conmutativo: Por el Ejercicio 1.18 y los Corolarios 3.72 y 3.73 sabemos que $p > 2$, que $\mathrm{Z}\,G = [G, G]$ es un subgrupo invariante de orden p de G y que $G/\,\mathrm{Z}\,G \approx \mathbb{Z}_p \times \mathbb{Z}_p$. 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

$$g^p = h^p = k^p = ghg^{-1}h^{-1} = gkg^{-1}k^{-1} = hkh^{-1}k^{-1}g^{-1} = 1,$$

y en consecuencia es isomorfo a G_2.

No habiendo más casos para considerar, la prueba está terminada. □

Parte 2

Anillos y módulos

Capítulo 4

Teoría elemental

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 $\dim V > 1$. 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 4.1. *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) Para concluir que $(-a)b = -ab$ basta observar que, por el item anterior,

$$ab + (-a)b = (a + (-a))b = 0b = 0.$$

La otra afirmación puede probarse en forma similar. $\square$

Corolario 4.2. *Si $1 = 0$, entonces $A = 0$.*

Demostración. Por la proposición anterior $a = a1 = a0 = 0$ para cada $a \in A$. $\square$

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 ó 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}.

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 4.3. *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 $b - c \neq 0$. $\square$

Proposición 4.4. *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 4.3 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 que tiene las propiedades equivalentes listadas en la proposición anterior.

Ejemplo 4.5. *Los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son dominios conmutativos. También lo son los anillos de polinomios $k[X_1, \dots, X_n]$, donde k es cualquiera de los anteriores.*

Ejemplo 4.6. *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*

$$(aX^m Y^n)(bX^{m'} Y^{n'}) = q^{m'n} abX^{m+m'} Y^{n+n'}$$

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 1.3 del Capítulo 1, sabemos que todo elemento de A que es inversible a izquierda es cancelable a izquierda. Además, por dicha proposición también sabemos que si A es un anillo finito, entonces cada $a \in A$ que es cancelable a izquierda o a derecha, es inversible.

Ejercicio 4.7. *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 $I = \{b \in A : ba = 1\}$, 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 4.8. *Pruebe que si V es un k-espacio vectorial con base numerable, entonces $\operatorname{End}_k V$ tiene elementos inversibles a izquierda que son divisores de cero a derecha.*

Ejercicio 4.9. *Pruebe que si V es un k-espacio vectorial de dimensión finita, entonces para cada $\varphi \in \operatorname{End}_k V$ 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 numeros 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 4.7, todo dominio finito es un anillo de división.

Un elemento a de un anillo es *nilpotente* si $a^n = 0$ para algún $n \in \mathbb{N}$.

Ejercicio 4.10. *Consideremos dos elementos a, b de un anillo A no nulo. Pruebe que:*

1. *Si a es nilpotente, entonces a es un divisor de cero a izquierda y a derecha.*
2. *Si a es nilpotente, entonces $1 - a$ es inversible.*
3. *Si a y b son nilpotentes y conmutan entre sí, entonces $a + b$ también es nilpotente.*

2. Subanillos

Dados subconjuntos X e Y de un anillo A, denotamos con XY al conjunto

$$XY := \{x_1y_1 + \cdots + x_ny_n : n \geq 0, x_i \in X \text{ e } y_i \in Y\},$$

formado por todas las sumas finitas de elementos de X por elementos de Y. Como el lector seguramente habrá notado, el símbolo XY no significa lo mismo en las teorías de anillos y de monoides.

Un subconjunto B de un anillo A es un *subanillo* de A si es cerrado para la suma y el producto y $1 \in B$. Esto es, si $BB \subseteq B$ 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 $S = \{x_1, \dots, x_s\}$, escribiremos $\mathbb{Z}\{x_1, \dots, x_s\}$ en lugar de $\mathbb{Z}\{\{x_1, \dots, x_s\}\}$. 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 $\mathbb{Z}[x_1, \dots, x_s]$ en lugar de $\mathbb{Z}\{x_1, \dots, x_s\}$.

Ejemplo 4.11. *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 4.12. *Los anillos de matrices $\mathrm{M}_n(\mathbb{Q})$ y $\mathrm{M}_n(\mathbb{R})$ son subanillos de $\mathrm{M}_n(\mathbb{C})$.*

Ejemplo 4.13. *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 k, son subanillos de* $\mathrm{M}_n(A)$*.*

Ejemplo 4.14. *El anillo de los* enteros de Gauss *es el subanillo* $\mathbb{Z}[i]$ *de* $\mathbb{C}$*. Es evidente que* $\mathbb{Z}[i]$ *es el conjunto de los números complejos con parte real e imaginaria enteras.*

Ejemplo 4.15. *El subanillo* $\mathbb{Z}[\sqrt{3}]$ *de* $\mathbb{R}$ *está formado por los elementos de la forma* $a + b\sqrt{3}$*, con* $a, b \in \mathbb{Z}$ *de* $\mathbb{R}$*. Como* $\sqrt{3} \notin \mathbb{Q}$*, si* $a + b\sqrt{3} = a' + b'\sqrt{3}$*, entonces* $a = a'$ *y* $b = b'$*, de modo que esta escritura es única.*

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 4.16. *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 $\mathrm{B}\mathrm{E}_{rs}$ 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, $\mathrm{Z}\,\mathrm{M}_n(A) = \mathrm{Esc}_n(\mathrm{Z}\,A)$. □

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, 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. Dado un subanillo de división B de A y un 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 4.17. *Dos de los subanillos del Ejemplo 4.11 son subcuerpos.*

Ejemplo 4.18. *El subcuerpo* $\mathbb{Z}(\sqrt{3})$ *de* $\mathbb{R}$ *consiste de los elementos de la forma* $a + b\sqrt{3}$*, con* $a, b \in \mathbb{Q}$*. Como en el Ejemplo 4.15, también esta escritura es única. El inverso multiplicativo de un elemento no nulo* $a + b\sqrt{3}$ *es* $\frac{a-b\sqrt{3}}{a^2-3b^2}$*.*

3. Ideales

Un subconjunto no vacío I 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 los 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, dado un 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, dado $x \in A$, 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, escribiremos 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

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} \\ a_{21}b_{11} & a_{21}b_{12} \end{pmatrix}, \tag{33}$$

no es un ideal bilátero, porque $\mathrm{M}_2(\mathbb{Q})$ no tiene ideales biláteros no triviales (vease la Proposición 4.23) y la expresión (33) 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 incluido en ningún otro ideal propio del mismo tipo.

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 $i \in J$.

Dados ideales $I \subseteq J$ a izquierda de un anillo A, decimos que I es un sumando directo de J si existe un ideal a izquierda I' 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 claro que $I \cap (J + K) \supseteq J + I \cap K$, y 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 4.19. *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, dado $a \in I$ 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 4.20. *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.

Un anillo es un *dominio principal* si es un dominio conmutativo y todos sus ideales son principales. En el Ejemplo 4.19 mostramos que los anillos de enteros y de polinomios en una variable sobre un cuepo son dominios principales. Más adelante estudiaremos estos anillos con más detalle.

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 4.21. *Pruebe que si $A[X]$ es un dominio principal, entonces A es un cuerpo.*

Proposición 4.22. *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 4.23. *Si D es un anillo de división, entonces los únicos ideales biláteros de $\mathrm{M}_n(D)$ son los triviales.*

Demostración. Dados $1 \le i, j \le n$, 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. El mismo argumento usado en la teoría de monoide prueba que un morfismo es un isomorfismo si y sólo si es biyectivo.

Proposición 4.24. *Un morfismo de anillos $f\colon A \to A'$ es un isomorfismo si y sólo si es biyectivo.*

Demostración. Copiese la prueba hecha para monoides. □

Mantenemos la notación $A \approx A'$ 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.

Igual que en la teoría de monoides y grupos, dados morfismos $f\colon A \to A'$ y $g\colon A' \to A''$, 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 evidente 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 4.25. *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 $m/n \in \mathbb{Q}$.
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 4.26. *Para cada anillo A hay un único morfismo $\iota\colon \mathbb{Z} \to A$. Es fácil ver que la imagen de ι es el anillo primo $\mathbb{Z}\{1_A\}$ de A. También es fácil ver que*
$$\mathbb{Z}\{1_A\} \approx \begin{cases} \mathbb{Z} & \text{si } n1_A \neq 0 \text{ para todo } n \in \mathbb{N}, \\ \mathbb{Z}/n\mathbb{Z} & \text{si no, donde } n \in \mathbb{N} \text{ es el mínimo natural tal que } n1_A = 0. \end{cases}$$
En el primer caso decimos que la característica *de A es cero y en el segundo que es n. Es obvio 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 4.27. *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 $i^4 = 1$, debe ser $f(i)^4 = 1$. 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 $\{a \in A : a^4 = 1\}$. Cuando $A = \mathbb{Z}[i]$, este conjunto es $\{1, -1, i, -i\}$. Como de los 4 endomorfismos obtenidos, sólo dos, la identidad y la conjugación, son automorfismos,* $\mathrm{Aut}(\mathbb{Z}[i])$ *es un grupo cíclico de orden 2.*

EJEMPLO 4.28. *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 $\mathrm{M}_n(A^{\mathrm{op}}) \approx \mathrm{M}_n(A)^{\mathrm{op}}$.

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 4.29. *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. Cocientes de anillos

Dados 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. En efecto, para que π respete el producto, forzosamente la multiplicación de A/I deberá estár dada por

$$[a][a'] = [aa'].$$

El requisito de que I sea un ideal es una condición necesaria y suficiente para que esta definición no dependa de a y a', sino sólo de sus clases. Las igualdades

$$([a][a'])[a''] = [aa'][a''] = [(aa')a''] = [a(a'a'')] = [a][a'a''] = [a]([a'][a'']),$$

muestran que la multiplicación de A/I es asociativa. 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. Además $\pi\colon A \to A/I$ 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 $\bar{f}\colon A/I \to B$ tal que el triángulo

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"'] & B \\ A/I \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

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 $\bar{f}$ tal que $\bar{f}\circ\pi = f$, y notar que $\bar{f}$ aplica la identidad en la identidad y respeta el producto, si f lo hace.

Por la Observación 1.79 sabemos que $\ker \bar{f} = \pi(\ker f)$ e $\operatorname{Im} \bar{f} = \operatorname{Im} f$. En particular, $A/\ker f$ es isomorfo a $\operatorname{Im} f$. Además, como grupo aditivo, $\pi(\ker f)$ es isomorfo a $\ker f/I$.

OBSERVACIÓN 4.30. *Por la propiedad universal del cociente, dados ideales I y J de un anillo A, con $I \subseteq J$, existe un único morfismo $\bar{\pi}_J\colon A/I \to A/J$ tal que el triángulo*

$$\begin{tikzcd} A \arrow[r, "\pi_J"] \arrow[d, "\pi_I"'] & A/J \\ A/I \arrow[ur, "\bar{\pi}_J"'] & \end{tikzcd},$$

donde π_I y π_J son las proyecciones canónicas, conmuta. Además $\bar{\pi}_J$ es sobreyectivo, el subgrupo J/I de A/I es un ideal bilátero de A/I y $\ker \bar{\pi}_J = \pi_I(J) = J/I$. Por lo tanto $\bar{\pi}_J$ induce un isomorfismo $(A/I)/(J/I) \approx A/J$.

OBSERVACIÓN 4.31. *Supongamos que $f\colon A \to B$ es un morfismo de anillos. Dado un ideal J 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 $\bar{f}\colon A/f^{-1}(J) \to (f(A) + J)/J$. En particular, si A es un subanillo de B, entonces $A/(A \cap J) \approx (A + J)/J$.*

EJERCICIO 4.32. *Pruebe que si $f\colon A \to B$ es un morfismo sobreyectivo de anillos e I es un ideal de A, entonces $A/(I + \ker f) \approx B/f(I)$.*

PROPOSICIÓN 4.33. *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 $\bar{f}\colon A/I \to B/J$ tal que el diagrama*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi_I"'] & B \arrow[d, "\pi_J"] \\ A/I \arrow[r, "\bar{f}"] & B/J, \end{tikzcd}$$

donde $\pi_I\colon A \to A/I$ y $\pi_J\colon B \to B/J$ son las proyecciones canónicas, conmuta. Además, $\operatorname{Im} \bar{f} = (J + \operatorname{Im} f)/J$ *y* $\ker \bar{f} = f^{-1}(J)/I$.

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 $\ker(\pi_J\circ f) = f^{-1}(J)$. $\square$

Observación 4.34. *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*
$$g(f(I)) \subseteq K \quad y \quad \overline{g\circ f} = \bar{g}\circ\bar{f}.$$

Ejercicio 4.35. *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* $\bar{f}\colon A/I \to B/J$, *donde* $I = f^{-1}(J)$, *tal que el diagrama*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi_I"] & B \arrow[d, "\pi_J"] \\ A/I \arrow[r, "\bar{f}"] & B/J, \end{tikzcd}$$

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* $\operatorname{Im}\bar{f} = (f(A)+J)/J$.

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 $\pi_j\colon \prod_{i\in I} A_i \to A_j$ $(j\in I)$ 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:

- Dada una familia $(f_i\colon A\to A_i)_{i\in I}$ de morfismos de anillos, existe un único morfismo $\overrightarrow{(f_i)}_{i\in I}\colon A \to \prod A_i$ tal que, para cada $j\in I$, el diagrama

$$\begin{tikzcd} A \arrow[d, "\overrightarrow{(f_i)}"] \arrow[dr, "f_j"] & \\ \prod A_i \arrow[r, "\pi_j"] & A_j \end{tikzcd}$$

conmuta. Claramente $\overrightarrow{(f_i)}(a) = (f_i(a))_{i\in I}$ y $\ker(f_i) = \bigcap \ker f_i$.

Ejercicio 4.36. *Muestre que si* $A = \prod A_j$, *entonces* $A^\times = \prod A_j^\times$.

Proposición 4.37. *Dada una 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 $\bigl(f_j(a_j)\bigr)_{j\in J}$ y, usando esto, que $\ker \prod f_j = \prod \ker f_j$ e $\operatorname{Im} \prod f_j = \prod \operatorname{Im} f_j$.

Observación 4.38. *La correspondencia introducida en la Proposición 4.37 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,*
$$\prod g_j \circ \prod f_j = \prod (g_j \circ f_j).$$

Consideremos ahora un producto finito de anillos $A = A_1 \times \cdots \times A_n$. Dado un ideal a izquierda, a derecha o bilátero I de A denotemos con I_j a $\pi_j(I)$. Afirmamos que

$$I = I_1 \times \cdots \times I_n. \tag{34}$$

En efecto, supongamos por ejemplo que I es un ideal a izquierda. Para cada $i \le n$, denotemos con e_i al elemento de A que tiene 1 en la i-ésima coordenada y cero en las demás. Si $(a_1,\dots,a_n) \in I$, entonces

$$(0,\dots,0,a_i,0,\dots,0) = e_i(a_1,\dots,a_n) \in I,$$

por lo que la igualdad (34) se sigue inmediatamente. En consecuencia:

- I es maximal si y sólo existe un índice i tal que I_i es maximal en A_i e $I_j = A_j$ para todo $j \neq i$.
- Si I es bilátero, entonces las proyecciones canónicas $\bar{\pi}_j\colon A \to A_j/I_j$ inducen un isomorfismo de A/I en $A_1/I_1 \times \cdots \times A_n/I_n$.

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 $y \in J$. Es evidente que

$$(I+J)(I\cap J) \subseteq IJ + JI \subseteq I \cap J.$$

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.

EJERCICIO 4.39. *Pruebe que* $\langle m\rangle\langle n\rangle = \langle mn\rangle$ *para cada par* $\langle m\rangle$ *y* $\langle n\rangle$ *de ideales de* $\mathbb{Z}$. *Pruebe que lo mismo vale para el anillo* $k[X]$, *de polinomios con coeficientes en un cuerpo* k.

Dados ideales $I_1, \dots, I_n$ 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 $\ker \pi = I_1 \cap \dots \cap I_n$. En particular, π es inyectivo si y sólo si $I_1 \cap \dots \cap I_n = 0$. El siguiente resultado da condiciones necesarias y suficientes para que sea sobreyectivo.

TEOREMA 4.40 (Teorema chino del resto). *El morfismo* π *es sobreyectivo si y sólo si los ideales* $I_1, \dots, I_n$ *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 la definición de π, 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 $a_{(i)} \in I_1 \cap \dots \cap \widehat{I_i} \cap \dots \cap I_n$ tal que $1 - a_{(i)} \in I_i$, lo cual implica que

$$\pi\left(\sum_{i=1}^{n} a_i a_{(i)}\right) = ([a_1], \dots, [a_n])$$

para cada n-upla $(a_1, \dots, a_n)$ de elementos de A. □

8. El anillo de un monoide

Dados un anillo A y un monoide S, el conjunto $A^{(S)}$, de las funciones $\varphi\colon S \to A$ con 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

$$\begin{aligned}
(\varphi\psi)\vartheta(s) &= \sum_{\substack{u,v \in S \\ uv = s}} \varphi\psi(u)\vartheta(v) \\
&= \sum_{\substack{u,v \in S \\ uv = s}} \left(\sum_{\substack{p,q \in S \\ pq = u}} \varphi(p)\psi(q)\right)\vartheta(v) \\
&= \sum_{\substack{x,y,z \in S \\ xyz = s}} \varphi(x)\psi(y)\vartheta(z)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{u,v\in S\\ uv=s}} \varphi(u)\left(\sum_{\substack{p,q\in S\\ pq=v}} \psi(p)\vartheta(q)\right)\\
&= \sum_{\substack{u,v\in S\\ uv=s}} \varphi(u)\psi\vartheta(v)\\
&= \varphi(\psi\vartheta)(s)
\end{aligned}
$$

muestran que el producto es asociativo; las igualdades

$$\varphi(\psi+\vartheta)(s) = \sum_{\substack{u,v\in S\\ uv=s}} \varphi(u)(\psi(v)+\vartheta(v)) = \sum_{\substack{u,v\in S\\ uv=s}} \varphi(u)\psi(v) + \sum_{\substack{u,v\in S\\ uv=s}} \varphi(u)\vartheta(v) = (\varphi\psi+\varphi\vartheta)(s)$$

que es distributivo a izquierda respecto de la suma; y las igualdades

$$(\varphi+\psi)\vartheta(s) = \sum_{\substack{u,v\in S\\ uv=s}} (\varphi(u)+\psi(u))\vartheta(v) = \sum_{\substack{u,v\in S\\ uv=s}} \varphi(u)\vartheta(v) + \sum_{\substack{u,v\in S\\ uv=s}} \psi(u))\vartheta(v) = (\varphi\vartheta+\psi\vartheta)(s),$$

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 $A[S]$.

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

(35) $$\sum_{s\in S} a_s s,$$

con soporte finito. Una expresión como (35) es lo que se conoce con el nombre de *suma formal de monomios en S con coeficientes en A*. En términos de estas, la suma y el producto en $A[S]$ están dados por la fórmulas

$$\sum_{s\in S} a_s s + \sum_{s\in S} b_s s = \sum_{s\in S} (a_s+b_s)s \qquad \text{y} \qquad \left(\sum_{s\in S} a_s s\right)\left(\sum_{s\in S} b_s s\right) = \sum_{s\in S}\left(\sum_{\substack{u,v\in S\\ uv=s}} a_u b_v\right)s,$$

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 $1_A s$. 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 ${}^f\psi\colon A[S] \to B$, tal que los triángulos

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\iota_A"'] & B \\ A[S] \arrow[ur, "{}^f\psi"'] & \end{tikzcd} \quad \text{y} \quad \begin{tikzcd} S \arrow[r, "\psi"] \arrow[d, "\iota_S"'] & B \\ A[S] \arrow[ur, "{}^f\psi"'] & \end{tikzcd}$$

conmutan.

En efecto, por la conmutatividad de los triángulos de arriba, debe ser

$${}^f\psi\left(\sum_{s\in S} a_s s\right) = \sum_{s\in S} f(a_s)\psi(s).$$

Es evidente que con esta definición, ${}^f\psi$ 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 respeta el producto.

Ejemplo 4.41. *Si G es un grupo, entonces 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*

$$\begin{array}{rcl} A^{\mathrm{op}}[G] & \xrightarrow{f} & A[G]^{\mathrm{op}} \\ \sum_g \lambda_g g & \longmapsto & \sum_g \lambda_g g^{-1} \end{array},$$

que es biyectivo porque la aplicación antipodal de G, introducida en el Ejemplo 1.60 del Capítulo 1, lo es. En particular, si A es conmutativo, entonces $A[G]^{\mathrm{op}}$ es isomorfo a $A[G]$.

Proposición 4.42. *Dados un morfismo de anillos $f\colon A \to B$ y un 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*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\iota_A"'] & B \arrow[d, "\iota_B"] \\ A[S] \arrow[r, "{f[\psi]}"] & B[T] \end{tikzcd} \quad y \quad \begin{tikzcd} S \arrow[r, "\psi"] \arrow[d, "\iota_S"'] & T \arrow[d, "\iota_T"] \\ A[S] \arrow[r, "{f[\psi]}"] & B[T], \end{tikzcd}$$

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 4.43. *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 $\vartheta\colon T \to L$,*

$$g[\vartheta]\circ f[\psi] = (g\circ f)[\vartheta\circ\psi].$$

PROPOSICIÓN 4.44. *Dados un anillo A y 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. □

EJEMPLO 4.45. *Dado un 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 $X_1,\dots,X_r$ e identificando cada r-upla $\mathbf{n} = (n_1,\dots,n_r)$ 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 $A[\mathbb{N}_0^r]$ es el anillo de polinomios $A[X_1,\dots,X_r]$.

PROPOSICIÓN 4.46. *Los anillos $A[X_1,\dots,X_r]$ y $A[X_1,\dots,X_l][X_{l+1},\dots,X_r]$ son isomorfos para cada $l < r$.*

DEMOSTRACIÓN. Es una consecuencia inmediata de la Proposición 4.44. □

OBSERVACIÓN 4.47 (Propiedad universal del anillo de polinomios). *Dados elementos $b_1,\dots,b_n$ 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 dado 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 ${}^f\gamma\colon A[X_1,\dots,X_n] \to B$, tal que ${}^f\gamma(a) = f(a)$ para cada $a \in A$ y ${}^f\gamma(X_i) = b_i$ para cada i. Es fácil ver que ${}^f\gamma$ está dado por*

$${}^f\gamma\Bigl(\sum a_{n_1,\dots,n_r} X_1^{n_1}\cdots X_r^{n_r}\Bigr) = \sum f(a_{n_1,\dots,n_r}) b_1^{n_1}\cdots b_r^{n_r}.$$

PROPOSICIÓN 4.48. *Para cada morfismo de anillos $f\colon A \to B$, son equivalentes:*

1. *f es un monomorfismo.*
2. *f es inyectiva.*
3. $\ker f = 0$.

DEMOSTRACIÓN. Por la Observación 4.29 sabemos que 2) equivale a 3), y es claro que 2) implica 1). Veamos que 1) implica 2). Dados $a, a' \in A$ tales que $f(a) = f(a')$, consideremos los morfismos $i_a, i_{a'}\colon \mathbb{Z}[X] \to A$ definidos por $i_a(X) = a$ e $i_{a'}(X) = a'$. Como $f\circ i_a = f\circ i_{a'}$ y f es un monomorfismo, $i_a = i_{a'}$. Pero entonces $a = a'$. □

9. Los cuaterniones

Consideremos el subconjunto $\mathbb{H}$ de $\mathrm{M}_2(\mathbb{C})$, formado por las matrices

$$q_{y,z} = \begin{pmatrix} y & -z \\ \bar{z} & \bar{y} \end{pmatrix}, \qquad \text{con } y, z \in \mathbb{C}.$$

Es obvio que $\mathbb{H}$ es un subgrupo aditivo de $\mathrm{M}_2(\mathbb{C})$ y que la matriz identidad pertenece a $\mathbb{H}$. La igualdad

$$q_{w,x}q_{y,z} = q_{wy-x\bar{z},wz+x\bar{y}},$$

cuya comprobación es directa y muy simple, muestra que de hecho es un subanillo de $\mathrm{M}_2(\mathbb{C})$. A $\mathbb{H}$ se lo llama el *anillo de cuaterniones* con coeficientes reales. Dado que

$$\det(q_{y,z}) = y\bar{y} + z\bar{z} = |y|^2 + |z|^2$$

es distinto de cero si $(y,z) \neq (0,0)$, todas la matrices no nulas de $\mathbb{H}$ son inversibles. Como además

$$q_{y,z}^{-1} = d^{-1}q_{\bar{y},-z} = q_{d^{-1}\bar{y},-d^{-1}z} \quad \text{con } d = \det(q_{y,z})$$

(lo que puede comprobarse directamente, o recordando que la inversa de una matriz inversible es la transpuesta de la matriz de los cofactores dividida por el determinante), $\mathbb{H}$ es un anillo de división. No es un cuerpo, porque $q_{i,0}q_{0,1} = q_{0,i} = -q_{0,1}q_{i,0}$.

Los cuaterniones tienen en su interior una copia de los números complejos. Más precisamente, la aplicación

$$\begin{aligned} \mathbb{C} &\xrightarrow{\varrho} \mathbb{H} \\ y &\longmapsto q_{y,0} \end{aligned}$$

es un morfismo inyectivo de anillos. Dejamos como tarea para el lector probar que $\mathrm{Z}\,\mathbb{H} = \varrho(\mathbb{R})$. En consecuencia, $\mathbb{H}$ es un $\mathbb{C}$-espacio vectorial vía

$$\lambda \cdot q_{y,z} := q_{\lambda,0}q_{y,z} = q_{\lambda y,\lambda z},$$

pero no es un $\mathbb{C}$-subespacio vectorial de $\mathrm{M}_2(\mathbb{C})$.

La conjugación y el módulo de números complejos se extienden a los cuaterniones. Definimos el *conjugado* $\overline{q_{y,z}}$ y el *módulo* $|q_{y,z}|$ de un cuaternión $q_{y,z} \in \mathbb{H}$, por

$$\overline{q_{y,z}} := q_{\bar{y},-z} \qquad \text{y} \qquad |q_{y,z}| := (q_{y,z}\overline{q_{y,z}})^{1/2}.$$

La definición de módulo es correcta, porque $q_{y,z}\overline{q_{y,z}} = \det q_{y,z} \in \mathbb{R}_{\geq 0}$.

Proposición 4.49. *Para cada par q, r de cuaterniones,*

$$\overline{q+r} = \bar{q} + \bar{r}, \qquad \overline{qr} = \bar{r}\bar{q} \qquad y \qquad |qr| = |q||r|.$$

Además, si $q \neq 0$, entonces $q^{-1} = \bar{q}/|q|^2$.

Demostración. Es claro que la primera y la última afirmación son verdaderas. La tercera lo es porque

$$|qr|^2 = \det(qr) = \det q \det r = |q|^2|r|^2.$$

La segunda es trivial si $q = 0$ o $r = 0$, y las igualdades

$$\overline{qr} = |qr|^2(qr)^{-1} = |r|r^{-1}|q|q^{-1} = \bar{r}\bar{q},$$

muestran que vale siempre. □

Consideremos el $\mathbb{C}$-espacio vectorial $\mathbb{C}\times\mathbb{C}$. La función

$$\begin{aligned} \mathbb{C}\times\mathbb{C} &\xrightarrow{\varrho_e} \mathbb{H}\\ (y,z) &\longmapsto q_{y,z}\end{aligned}$$

es un isomorfismo de $\mathbb{C}$-espacios vectoriales. Definiendo la multiplicación en $\mathbb{C}\times\mathbb{C}$ por transporte de estructura a través de ϱ_e, obtenemos la presentación usual del anillo de cuaterniones. Designaremos con $\check{\mathbb{H}}$ a este anillo, para distinguirlo de $\mathbb{H}$. Es evidente que el diagrama

$$\begin{tikzcd} \mathbb{C} \arrow[r, "\varrho"] \arrow[d, "\iota_1"'] & \mathbb{H} \\ \check{\mathbb{H}} \arrow[ur, "\varrho_e"'] & \end{tikzcd},$$

en el cual la flecha vertical es la inclusión canónica en la primera coordenada, conmuta. Como $\varrho(\mathbb{C})$ no está incluído en el centro de $\mathbb{H}$, para determinar la multiplicación de $\check{\mathbb{H}}$ no es suficiente calcular los productos de los elementos de una base de $\check{\mathbb{H}}$ como $\mathbb{C}$-espacio vectorial. Debemos hacer esto, pero con los elementos de una base de $\check{\mathbb{H}}$ como $\mathbb{R}$-espacio vectorial. A partir de ahora identificamos $\check{\mathbb{H}}$ con $\mathbb{R}^4$ y llamamos $1,i,j,k$ a los elementos $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$ y $(0,0,0,1)$, de la base canónica de $\check{\mathbb{H}}$ como $\mathbb{R}$-espacio vectorial. Esta notación es razonable, porque $\varrho_e(1)=q_{1,0}$ es el neutro multiplicativo de $\mathbb{H}$. Un cálculo directo muestra que:

$$i^2=j^2=k^2=-1,\quad ij=k=-ji,\quad jk=i=-kj \quad \text{y} \quad ki=j=-ik.$$

Entonces, la multiplicación en $\check{\mathbb{H}}$ está dada por:

$$\begin{aligned}(a_1+a_ii+a_jj+a_kk)(b_1+b_ii+b_jj+b_kk) &= a_1b_1-a_ib_i-a_jb_j-a_kb_k\\ &+(a_1b_i+a_ib_1+a_jb_k-a_kb_j)i\\ &+(a_1b_j+a_jb_1-a_ib_k+a_kb_i)j\\ &+(a_1b_k+a_kb_1+a_ib_j-a_jb_i)k.\end{aligned}$$

Para determinar como se traslada a $\check{\mathbb{H}}$ el operador de conjugación en $\mathbb{H}$, también basta verlo sobre los elementos de la base canónica. Las cuentas son mucho más fáciles que para el producto, y prueban que el operador de $\check{\mathbb{H}}$ obtenido por traslación de estructura a partir de la conjugación en $\mathbb{H}$, satisface

$$\overline{a_1+a_ii+a_jj+a_kk}=a_1-a_ii-a_jj-a_kk.$$

Por último, es evidente que el módulo en $\check{\mathbb{H}}$, definido como la composición del módulo en $\mathbb{H}$ con ϱ_e, satisface

$$|z|=(z\bar{z})^{1/2}=\sqrt{a_1^2+a_i^2+a_j^2+a_k^2},$$

para cada $z=a_1+a_ii+a_jj+a_kk\in\check{\mathbb{H}}$.

Consideremos el subanillo $\check{\mathbb{H}}_{\mathbb{Z}}$ de $\check{\mathbb{H}}$ formado por todos los cuaterniones

$$z=a_1+a_ii+a_jj+a_kk,$$

cuyos coeficientes a_1, a_i, a_j y a_k son enteros. Es fácil ver que el grupo de unidades $\check{\mathbb{H}}_{\mathbb{Z}}^{\times}$ de $\check{\mathbb{H}}_{\mathbb{Z}}$ es $\{\pm1,\pm i,\pm j,\pm k\}$. Usando que el mismo tiene ocho elementos, que

$$i^2j^{-2}=jij^{-1}i=1,$$

y razonando como en el Ejemplo 1.105, se comprueba sin dificultad que $\check{\mathbb{H}}_{\mathbb{Z}}^{\times}$ es isomorfo a $\mathbb{H}_2$. Esta es la razón por la que se llama grupos cuaterniónicos generalizados a los grupos $\mathbb{H}_n$.

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, y que $(p,q)\sim(r,s)$ si y sólo si existen $a,b\in A\setminus\{0\}$ tales que $(pa,qa)=(rb,sb)$. 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 4.50. *El cuerpo de cocientes de A es, efectivamente, un cuerpo. Además, la aplicación*

$$\begin{aligned} A &\xrightarrow{\ \iota\ } \mathbb{Q}_A\\ a &\longmapsto \tfrac{a}{1}\end{aligned}$$

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\iota"'] & k \\ \mathbb{Q}_A \arrow[ur, "\tilde{f}"'] \end{tikzcd}$$

conmuta.

DEMOSTRACIÓN. Las igualdades

$$\begin{aligned}
&\Bigl(\frac{p}{q}+\frac{r}{s}\Bigr)+\frac{t}{u}=\frac{ps+qr}{qs}+\frac{t}{u}=\frac{psu+qru+qst}{qsu}=\frac{p}{q}+\frac{ru+st}{su}=\frac{p}{q}+\Bigl(\frac{r}{s}+\frac{t}{u}\Bigr),\\
&\frac{p}{q}+\frac{r}{s}=\frac{ps+qr}{qs}=\frac{rq+sp}{sq}=\frac{r}{s}+\frac{p}{q},\\
&\frac{p}{q}+\frac{0}{1}=\frac{p1+q0}{q1}=\frac{p}{q},\\
&\frac{p}{q}+\frac{-p}{q}=\frac{pq-qp}{q^2}=\frac{0}{q^2}=\frac{0}{1},\\
&\Bigl(\frac{p}{q}\frac{r}{s}\Bigr)\frac{t}{u}=\frac{pr}{qs}\frac{t}{u}=\frac{prt}{qsu}=\frac{p}{q}\frac{rt}{su}=\frac{p}{q}\Bigl(\frac{r}{s}\frac{t}{u}\Bigr),\\
&\frac{p}{q}\frac{r}{s}=\frac{pr}{qs}=\frac{rp}{sq}=\frac{r}{s}\frac{p}{q},
\end{aligned}$$

$$\frac{p}{q}\frac{1}{1} = \frac{p1}{q1} = \frac{p}{q}$$

y

$$\frac{p}{q}\left(\frac{r}{s}+\frac{t}{u}\right) = \frac{p}{q}\frac{ru+st}{su} = \frac{pru+pst}{qsu} = \frac{prqu+qspt}{qsqu} = \frac{pr}{qs}+\frac{pt}{qu} = \frac{p}{q}\frac{r}{s}+\frac{p}{q}\frac{t}{u},$$

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 $p \neq 0$ y $q \neq 0$, 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

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

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 $\tilde{f}\left(\frac{p}{q}\right) = f(p)f(q)^{-1}$ define un morfismo de anillos. □

NOTA 4.51. *Es usual identificar $a \in A$ con $\iota(a) = \frac{a}{1}$.*

11. 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 4.52. *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. Dada una acción de un anillo A sobre M, la función

$$\begin{aligned} M &\xrightarrow{\rho(a)} M \\ m &\longmapsto a \cdot m \end{aligned}$$

es un endomorfismo de M para cada $a \in A$, y la aplicación

$$\begin{aligned} A &\xrightarrow{\rho} \operatorname{End} M \\ a &\longmapsto \rho(a) \end{aligned}$$

es un morfismo de anillos. Recíprocamente, si $\rho\colon A \to \operatorname{End} M$ 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 $\operatorname{End} M$.

Ejemplo 4.53. *El A-*módulo nulo *es el grupo* 0 *provisto de la única acción a izquierda de A sobre él.*

Ejemplo 4.54. *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 4.55. *Un módulo sobre un cuerpo k es un k-espacio vectorial.*

Ejemplo 4.56. *Por el Ejemplo 4.26, para cada grupo abeliano M, hay un único morfismo de anillos $\iota\colon \mathbb{Z} \to \operatorname{End} M$. 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 4.57. *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 y la función*

$$\begin{aligned} M &\xrightarrow{f} M \\ m &\longmapsto X \cdot m \end{aligned}$$

es un endomorfismo de k-espacios vectoriales porque

$$X \cdot (m+n) = X \cdot m + X \cdot n \qquad y \qquad X \cdot (\lambda \cdot m) = (X\lambda) \cdot m = (\lambda X) \cdot m = \lambda \cdot (X \cdot m),$$

para todo $m, n \in M$ y $\lambda \in k$. Recíprocamente, dados un k-espacio vectorial M y una aplicación k-lineal $f\colon M \to M$, 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 $m \in M$. 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 $\operatorname{End} M$, y utilizar la Propiedad universal del anillo de polinomios (Observación 4.47).

Ejemplo 4.58. *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 $f^4 = \mathrm{id}$.*

Ejemplo 4.59. *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*

  $$\begin{aligned} M &\xrightarrow{\rho(s)} M \\ m &\longmapsto s \cdot m \end{aligned}$$

  es un morfismo de k-espacios vectoriales,
- *La función*

  $$\begin{aligned} S &\xrightarrow{\rho} \operatorname{End}_k M \\ s &\longmapsto \rho(s) \end{aligned}$$

  es un morfismo de monoides.

Recíprocamente, dados un k-módulo M y un morfismo de monoides $\rho\colon S \to \operatorname{End}_k M$, 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 4.60. *Una* representación *de un grupo G sobre un k-espacio vectorial M es un morfismo de grupos $\rho\colon G \to \operatorname{Aut}_k M$. 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 $\rho\colon A \to \operatorname{End} M$ 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 $\rho\colon Z \to \operatorname{End}(\mathbb{Z}_6 \times \mathbb{Z}_9)$ asociado es $18\mathbb{Z}$. La acción inducida de $\mathbb{Z}_{18}$ sobre $\mathbb{Z}_6 \times \mathbb{Z}_9$ es fiel.

12. 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 $S = \{s_1, \dots, s_n\}$ escribimos $\langle s_1, \dots, s_n\rangle$ en lugar de $\langle\{s_1, \dots, s_n\}\rangle$. 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 4.61. *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 $M = A\{x_1, \dots, x_n\}$ y que $(M_i)_{i\in I}$ es una familia de submódulos de M cuya suma es M. Para cada $1 \le j \le n$ 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 $I' = I_1 \cup \dots \cup I_n$.

2) $\Rightarrow$ 3) Esto es claro.

3) $\Rightarrow$ 1) Aplíquese el item 3) a la familia formada por los submódulos finitamente generados de M. $\square$

Un conjunto de generadores S de M es *minimal* si ningún subconjunto propio de S genera M. Si M es finitamente generado, entonces todo conjunto de generadores contiene uno minimal, como puede comprobarse fácilmente. Existen módulos que no tienen conjuntos de generadores minimales. Un ejemplo es el grupo aditivo $\mathbb{Q}$.

PROPOSICIÓN 4.62. *Si un módulo M es finitamente generado, entonces todos los conjuntos minimales de generadores de M son finitos. Si no lo es, entonces todos (suponiendo que haya alguno) tienen el mismo cardinal.*

DEMOSTRACIÓN. Tomemos conjuntos de generadores S y T de M, con S minimal. Para cada $t \in T$ existe un subconjunto finito S_t de S, tal que $t \in AS_t$. Como T genera M y S es minimal, $S = \bigcup_{t\in T} S_t$. En consecuencia, S es es unión de una familia indexada por T

de conjuntos finitos no vacíos. La primera afirmación se sigue inmediatamente de este hecho tomando T finito. Para la segunda basta observar que si T es infinito, entonces la igualdad $S = \bigcup_{t\in T} S_t$ implica que $|S| \leq |T|$. En consecuencia, si T también es mininal, entonces por simetría $|S| = |T|$. $\square$

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 los subespacios vectoriales cerrados bajo la acción de S; y los de ${}_AA$, los ideales a izquierda.

13. 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 $M \approx M'$ 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 inyectiva, todo morfismo inyectivo un monomorfismo, y todo morfismo sobreyectivo 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 muestran que cuando $A = \mathbb{Z}$ hay epimorfismos que no son secciones y monomorfismos 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 $\operatorname{Hom}_A(M, M')$, $\operatorname{Iso}_A(M, M')$, $\operatorname{End}_A M$ y $\operatorname{Aut}_A M$ 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 evidente que $\operatorname{End}_A M$ es un monoide (cuyo elemento neutro es la función identidad) vía la composición y que $\operatorname{Aut}_A M$ es su grupo de unidades.

Como veremos enseguida, los morfismos de A-modulos tienen una estructura mucho más rica que los de monoides, grupos y anillos. En particular, $\operatorname{End}_A M$ tiene una estructura natural de anillo.

13.1. 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 $\operatorname{Hom}_A(M, N)$ 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. En otras palabras, para cada par de morfismos de A-módulos $v\colon N \to N'$ y $u\colon M' \to M$, las aplicaciones

$$v_*\colon \operatorname{Hom}_A(M, N) \to \operatorname{Hom}_A(M, N') \quad \text{y} \quad u^*\colon \operatorname{Hom}_A(M, N) \to \operatorname{Hom}_A(M', N),$$

definidas por $v_*(f) = v \circ f$ y $u^*(f) = f \circ u$ 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 $u, u'\colon M' \to M$.

En particular $\operatorname{End}_A(M)$ es un anillo.

Observación 4.63. *Para cada A-módulo M, la función*

$$\begin{aligned} M &\longrightarrow \operatorname{Hom}_A(A, M)\ , \\ m &\longmapsto f_m \end{aligned} \tag{36}$$

donde f_m es la aplicación A-lineal definida por $f_m(a) = a \cdot m$, es un isomorfismo de grupos abelianos. Su inversa es la función que asigna a cada morfismo $f\colon A \to M$ su valor en 1. Cuando $M = A$ tiene sentido preguntarse si (36) *es un isomorfismo de anillos. Un cálculo sencillo muestra que $f_{ab} = f_b \circ f_a$, de modo que si lo es, pero de A^{op} en* $\operatorname{End}_A(A)$.

14. 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 $\operatorname{Im} f$ un submódulo de M'. Más aún, no es dificil 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*:

- $f\circ\iota = 0_{\ker f, M}$,
- Dado un 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

$$\begin{tikzcd} N \arrow[r, "g"] \arrow[d, "g'"'] & M \arrow[r, "f"] & M' \\ \ker f \arrow[ur, "\iota"'] & & \end{tikzcd}$$

  conmuta.

Proposición 4.64. *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. Es una consecuencia inmediata de la Proposición 1.73. □

Corolario 4.65. *Un morfismo de A-módulos $f\colon M \to M'$ es inyectivo si y sólo si $\ker f = 0$.*

15. Cocientes de módulos

Consideremos un A-módulo M y un subgrupo N de M. Es fácil ver que el grupo cociente M/N tiene una estructura de A-módulo tal que la proyección canónica $\pi\colon M \to M/N$ es A-lineal, si y sólo si N es un submódulo de M. Dado $m \in M$, denotemos con $[m]$ a la clase de m en M/N. Como π es sobreyectiva, la acción de A sobre M/N es única y está dada por

$$a \cdot [m] = [am].$$

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 $\bar{f}\colon M/N \to M'$ tal que el triángulo

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi"'] & M' \\ M/N \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

  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 $\bar{f}\colon M/N \to M'$ tal que el diagrama anterior conmuta, y que $\bar{f}$ es A-lineal si y sólo si f lo es. Es fácil ver que $\ker \bar{f} = \ker f/N$ e $\operatorname{Im} \bar{f} = \operatorname{Im} f$ (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 4.66 (Primer teorema de isomorfismo). *Toda función A-lineal $f\colon M \to M'$ induce un isomorfismo $\bar{f}\colon M/\ker f \to \operatorname{Im} f$.*

Demostración. Es claro. □

Teorema 4.67 (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 $M/N \approx (M/L)/(N/L)$.*

Demostración. Imítese la prueba del Teorema 1.81. □

Teorema 4.68 (Tercer teorema de isomorfismo). *Si L y N son dos submódulos de un A-módulo M, entonces $L/L\cap N \approx (N+L)/N$.*

Demostración. Imítese la prueba del Teorema 1.82. □

El conjunto $\operatorname{Sub}_N M$, 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 $\operatorname{Sub} M$ en lugar de $\operatorname{Sub}_0 M$. 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 4.69 (Teorema de la correspondencia). *Si $f\colon M \to M'$ es un morfismo sobreyectivo de A-módulos, entonces las funciones*

$$\begin{aligned} \operatorname{Sub}_{\ker f} M &\longrightarrow \operatorname{Sub} M' \\ N &\longmapsto f(N) \end{aligned} \qquad y \qquad \begin{aligned} \operatorname{Sub} M' &\longrightarrow \operatorname{Sub}_{\ker f} M \\ N' &\longmapsto f^{-1}(N') \end{aligned}$$

son isomorfismos de reticulados, inversos uno del otro. Además $L/N \approx f(L)/f(N)$ para cada $L, N \in \operatorname{Sub}_{\ker f} M$ con $N \subseteq L$.

Demostración. Es una consecuencia fácil del Teorema 1.89. Alternativamente, se lo puede probar copiando la demostración de una parte de ese resultado. □

Definición 4.70. *Un A-módulo M es simple si $M \neq 0$ y sus únidos submódulos son los triviales.*

Observación 4.71. *Un A-módulo no nulo M es simple si y sólo si $M = Am$ para todo $m \in M$. En particular todo A-módulo simple es cíclico.*

Definición 4.72. *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 4.73. *Un submódulo N de un A-módulo M es maximal si y sólo si M/N es simple.*

Proposición 4.74. *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 $\{n_1,\dots,n_r\}$ genera N y $m_1,\dots,m_s$ son elementos de $M\setminus N$, cuyas clases generan M/N, entonces $\{n_1,\dots,n_r,m_1,\dots,m_s\}$ genera M. Tomemos $m\in M$ arbitrario y escribamos

$$[m]=a_1\cdot[m_1]+\cdots+a_s\cdot[m_s]\quad\text{con } a_1,\dots,a_s\in A.$$

Como $m-a_1\cdot m_1-\cdots-a_s\cdot m_s\in N$, existen $b_1,\dots,b_r\in A$ 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 4.75. *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. Usando que M/N es finitamente generado es fácil ver que la unión de cada cadena de submódulos propios de M que incluyen a N, es un submódulo propio de M. Entonces, por el Lema de Zorn, M tiene un submódulo maximal que contiene a N, como afirmamos. □

Corolario 4.76. *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 4.22, es un cuerpo. Es evidente que podemos tomar como el morfismo en cuestión, la proyección canónica de A en A/I. □

Ejercicio 4.77. *Pruebe que el $\mathbb{Z}$-módulo $\mathbb{Q}$ no tiene submódulos maximales.*

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 $\bar f\colon M/N\to M'/N'$ tal que el cuadrado

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi"] & M' \arrow[d, "\pi'"] \\ M/N \arrow[r, "\bar f"] & M'/N' \end{tikzcd},$$

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

$$\operatorname{Im}\bar f=\pi'(\operatorname{Im} f)\qquad\text{y}\qquad \ker\bar f=f^{-1}(H')/H.$$

Proposición 4.78. *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 $g\circ f(N)\subseteq N''$ 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

$$\begin{tikzcd} M \arrow[r, "\mathrm{id}"] \arrow[d, "\pi"] & M \arrow[d, "\pi"] \\ M/N \arrow[r, "\mathrm{id}"] & M/N \end{tikzcd}$$

y el rectángulo exterior del diagrama

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi"] & M' \arrow[r, "g"] \arrow[d, "\pi'"] & M'' \arrow[d, "\pi''"] \\ M/N \arrow[r, "\bar{f}"] & M'/N' \arrow[r, "\bar{g}"] & M''/N'' \end{tikzcd}$$

conmutan. $\square$

16. 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.

16.1. 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

$$m = \sum_{j\in J} m_j, \tag{37}$$

de elementos $m_j \in M_j$, no es única. En particular, 0 puede tener escrituras no triviales (i.e. con algún m_j no nulo). Decimos que una familia $(M_j)_{j\in J}$ de submódulos de M *está en suma directa*, o que la suma de los M_j es *directa*, si la escritura (37), de cada elemento $m \in \sum_{j\in J} M_j$, es única. En este caso escribimos $\bigoplus_{j\in J} M_j$ en lugar de $\sum_{j\in J} M_j$. Decimos que un A-módulo M es *suma directa interna* de una familia $(M_j)_{j\in J}$ de submódulos si la suma de los M_j es directa y $\bigoplus_{j\in J} M_j = M$. Si este es el caso, entonces las aplicaciones

$$\begin{aligned} M_i &\xrightarrow{\iota_i} M \\ m &\longmapsto m \end{aligned} \qquad \text{y} \qquad \begin{aligned} M &\xrightarrow{\pi_i} M_i \\ \textstyle\sum_{j\in J} m_j &\longmapsto m_i \end{aligned}$$

son morfismos bien definidos de A-módulos para cada $i \in J$, que satisfacen

$$\pi_i\circ\iota_j = \delta_{ij} \qquad \text{y} \qquad \sum_{j\in J} \iota_j\circ\pi_j = \mathrm{id}\,.$$

TEOREMA 4.79. *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. □

OBSERVACIÓN 4.80. *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 4.74, cada uno de los sumandos es finitamente generado.*

16.2. 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*

$$a \cdot (m_j)_{j\in J} = (a \cdot m_j)_{j\in J}.$$

Las proyecciones canónicas $\pi_j \colon \prod_{i\in I} M_i \to M_j$ $(j \in I)$ son morfismos de A-módulos, y las operaciones están definidas adrede para que esto ocurra. 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, siguiendo una costumbre bien establecida 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:

- Dada una familia $(f_i\colon M\to M_i)_{i\in I}$ de morfismos de A-módulos, existe un único morfismo $\overrightarrow{(f_i)}_{i\in I}\colon M\to\prod M_i$ tal que para cada $j\in I$ el diagrama

$$\begin{tikzcd} M \arrow[d, "\overrightarrow{(f_i)}"] \arrow[dr, "f_j"] & \\ \prod M_i \arrow[r, "\pi_j"] & M_j \end{tikzcd}$$

conmuta.

Claramente $\overrightarrow{(f_i)}(m)=(f_i(m))_{i\in I}$ y $\ker(f_i)=\bigcap\ker f_i$. Una manera equivalente de establecer la propiedad universal de $\prod M_i$ es diciendo que, para cada A-módulo M, la correspondencia

$$\begin{tikzcd}[row sep=small] \operatorname{Hom}(M,\prod M_i) \arrow[r, "\Psi"] & \prod \operatorname{Hom}(M,M_i) \\ f \arrow[r, mapsto] & (\pi_i\circ f)_i\in I \end{tikzcd}$$

es biyectiva. Es fácil ver que Ψ es un isomorfismo de grupos abelianos.

Observación 4.81. *Consideremos submódulos $M_1,\dots,M_n$ de un A-módulo M. Como en el Teorema 4.79, escribamos $M_{\hat\imath}=M_1+\cdots+\widehat{M_i}+\cdots+M_n$. Por la propiedad universal del producto, las proyecciones canónicas $\pi_{\hat\imath}\colon M\to M/M_{\hat\imath}$ inducen un morfismo*

$$G\xrightarrow{\overrightarrow{(\pi_{\hat 1},\dots,\pi_{\hat n})}} M/M_{\hat 1}\times\cdots\times M/M_{\hat n}\ ,$$

cuyo núcleo es $\bigcap_{i=1}^n M_{\hat\imath}$. Por la Observación 1.113, sabemos que $\overrightarrow{(\pi_{\hat 1},\dots,\pi_{\hat n})}$ es sobreyectivo si y sólo si $M=M_1+\cdots+M_n$.

Corolario 4.82. *El morfismo $\overrightarrow{(\pi_{\hat 1},\dots,\pi_{\hat n})}$ es bijectivo si y sólo si M es suma directa interna de $M_1,\dots,M_n$.*

Demostración. Es consecuencia inmediata del Teorema 4.79 y la Observación 4.81. □

Proposición 4.83. *Dada una 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

$$\begin{tikzcd} \prod M_i \arrow[r, "\prod f_i"] \arrow[d, "\pi_i"] & \prod N_i \arrow[d, "\pi_j"] \\ M_j \arrow[r, "f_j"] & N_j \end{tikzcd}$$

conmutan.

Demostración. Se sigue de la propiedad universal de $\prod N_i$. □

Es fácil ver que $\prod f_i((m_i)_{i\in I}) = (f_i(m_i))_{i\in I}$, $\ker \prod f_i = \prod \ker f_i$ e $\operatorname{Im} \prod f_i = \prod \operatorname{Im} f_i$.

OBSERVACIÓN 4.84. *La correspondencia introducida en la Proposición 4.83 tiene las siguientes propiedades:*

1. $\prod \mathrm{id}_{M_i} = \mathrm{id}_{\prod M_i}$.
2. *Dadas familias de morfismos de grupos* $(f_i\colon L_i \to M_i)_{i\in I}$ *y* $(g_i\colon M_i \to N_i)_{i\in I}$,

$$\left(\prod g_i\right)\circ\left(\prod f_i\right) = \prod g_i\circ f_i.$$

OBSERVACIÓN 4.85. *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,*

$$\frac{\prod M_i}{\prod N_i} \approx \prod \frac{M_i}{N_i}.$$

16.3. Coproducto directo

El *coproducto directo* o *suma directa* de una familia de A-módulos $(M_i)_{i\in I}$, es el submódulo $\bigoplus_{i\in I} M_i$ de $\prod M_i$, formado por todos los elementos con soporte finito. Esto es:

$$\bigoplus M_i := \left\{(m_i)_{i\in I} \in \prod M_i : m_i = 0 \text{ salvo para finitos índices } i \in I\right\}.$$

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 $\bigoplus_{i\in I} M_i$ es el producto directo restringido de los grupos aditivos subyacentes a los M_i's. Es fácil comprobar que las inclusiones canónicas $\iota_j\colon M_j \to \bigoplus_{i\in I} M_i$ 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, dada una familia morfismos de grupos abelianos $(f_i\colon M_i \to M)_{i\in I}$, existe un único morfismo de grupos abelianos $\overleftarrow{(f_i)}_{i\in I}\colon \bigoplus M_i \to M$ tal que para cada $j \in I$ el diagrama

$$\begin{tikzcd} & M \\ M_j \arrow[ur, "f_j"] \arrow[r, "\iota_j"'] & \bigoplus M_i \arrow[u, "\overleftarrow{(f_i)}"'] \end{tikzcd}$$

conmuta. Recordemos que $\overleftarrow{(f_i)}(m) = \sum f_j(\pi_j(m))$, donde $\pi_j\colon \bigoplus_{i\in I} M_i \to M_j$ es la proyección canónica. Un cálculo directo muestra que si M es un A-módulo y los f_i's son A-lineales, entonces $\overleftarrow{(f_i)}$ 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

$$\Psi\colon \operatorname{Hom}_A\Bigl(\bigoplus M_i, M\Bigr) \to \prod \operatorname{Hom}_A(M_i, M),$$

definida por $\Psi(\varphi) = (\varphi\circ\iota_i)_{i\in I}$, es biyectiva. En realidad vale algo más fuerte, Ψ es un isomorfismo de grupos abelianos.

PROPOSICIÓN 4.86. *Dada una 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

$$\begin{tikzcd} M_j \arrow[r, "f_j"] \arrow[d, "\iota_j"] & N_j \arrow[d, "\iota_j"] \\ \bigoplus M_i \arrow[r, "\bigoplus f_i"] & \bigoplus N_i \end{tikzcd}$$

conmutan.

DEMOSTRACIÓN. Se sigue de la propiedad universal de $\bigoplus M_i$. □

Es fácil ver que $(\bigoplus f_i)((m_i)_{i\in I}) = (f_i(m_i))_{i\in I}$, $\ker(\bigoplus f_i) = \bigoplus \ker f_i$ e $\operatorname{Im}(\bigoplus f_i) = \bigoplus \operatorname{Im} f_i$.

OBSERVACIÓN 4.87. *La correspondencia introducida en la Proposición 1.119 tiene las siguientes propiedades:*

1. $\bigoplus \mathrm{id}_{M_i} = \mathrm{id}_{\bigoplus M_i}$.
2. *Dadas familias de morfismos de A-módulos $(f_i\colon L_i \to M_i)_{i\in I}$ y $(g_i\colon M_i \to N_i)_{i\in I}$,*

$$\Bigl(\bigoplus g_i\Bigr)\circ\Bigl(\bigoplus f_i\Bigr) = \bigoplus g_i\circ f_i.$$

OBSERVACIÓN 4.88. *Para cada familia $(M_i)_{i\in I}$ de submódulos de un A-módulo M, la función*

$$\begin{tikzcd} \bigoplus M_i \arrow[r, "\varsigma"] & M \\ (m_i)_{i\in I} \arrow[r, mapsto] & \sum_{i\in I} m_i \end{tikzcd}$$

es un morfismo de A-módulos. Es obvio que

$$\ker\varsigma = \Bigl\{(m_i)_{i\in I} \in \bigoplus M_i : \sum_{i\in I} m_i = 0\Bigr\} \quad e \quad \operatorname{Im}\varsigma = \sum M_i.$$

PROPOSICIÓN 4.89. *Consideremos una familia $(M_i)_{i\in I}$ de submódulos de 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 $\varsigma\bigl((m_i)_{i\in I}\bigr) = \sum_{i\in I} m_i$, es inyectiva.*

DEMOSTRACIÓN. Se lo comprueba inmediatamente. □

Observación 4.90. *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*

$$\coprod M_i \xrightarrow{\coprod \pi_i} \coprod \tfrac{M_i}{N_i},$$

cuyo núcleo es $\coprod N_i$. Por consiguiente,

$$\frac{\coprod M_i}{\coprod N_i} \approx \coprod \frac{M_i}{N_i}.$$

16.4. Morfismos entre sumas directas finitas de A-módulos

Los resultados que daremos ahora son similares a los establecidos para grupos en la subsección (16.4) 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 $\mathbf{M} = (M_1, \dots, M_r)$ y $\mathbf{M}' = (M_1', \dots, M_s')$ 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

$$(f_{ij}) = \begin{pmatrix} f_{11} & \dots & f_{1r} \\ \vdots & \ddots & \vdots \\ f_{s1} & \dots & f_{sr} \end{pmatrix}$$

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 4.91. *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

$$\theta(f_{ij})(m_1, \dots, m_r) = \Big(\sum_j f_{1j}(m_j), \dots, \sum_j f_{sj}(m_j)\Big),$$

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

$$\theta(f_{ij})(m_1, \dots, m_r) = \begin{pmatrix} f_{11} & \dots & f_{1r} \\ \vdots & \ddots & \vdots \\ f_{s1} & \dots & f_{sr} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}.$$

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

$$\theta\colon \mathrm{M}_r\big(\operatorname{End}_A \mathbf{M}\big) \to \operatorname{End}_A(M_1 \oplus \cdots \oplus M_r)$$

es un isomorfismo de anillos.

Observación 4.92. *Dada* $\mathrm{B} = (b_{ij}) \in \mathrm{M}_{s\times r}(A^{\mathrm{op}})$, *consideremos el morfismo* $l_{\mathrm{B}}\colon A^r \to A^s$ *que a cada* r*-upla de elementos de* A *le asigna el resultado obtenido luego 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 4.63, se comprueba fácilmente que la correspondencia*

$$\begin{aligned} \mathrm{M}_{s\times r}(A^{\mathrm{op}}) &\longrightarrow \operatorname{Hom}_A(A^r, A^s) \\ \mathrm{B} &\longmapsto l_{\mathrm{B}} \end{aligned}$$

es un isomorfismo de grupos abelianos. Más aún, evidentemente $l_{\mathrm{I}_r} = \mathrm{id}_{A^r}$ *(aquí* I_r *denota a la matriz identidad de* $r \times r$*) 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* $\mathrm{C} \in M_{t\times s}(A^{\mathrm{op}})$.

17. 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 4.93. *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 $\bar{f}\colon M \to N$, tal que el triángulo

$$\begin{tikzcd} S \arrow[r, "f"] \arrow[d, "\iota"'] & N \\ M \arrow[ur, "\bar{f}"'] \end{tikzcd},$$

  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

$$m = \sum_{s\in S} a_s \cdot s, \tag{38}$$

necesariamente $\overline{f}(m) = \sum_{s\in S} a_s \cdot f(s)$. Como la escritura (38) es única, esta definición no es ambigua. Finalmente, es fácil comprobar que la función $\overline{f}$ que acabamos de determinar, es A-lineal.

Proposición 4.94. *Si M es un 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 $s \in S$. Por la unicidad en la propiedad universal de (M, S), como los triángulos

$$\begin{tikzcd} S \arrow[r, "\iota"] \arrow[d, "\iota"'] & M \\ M \arrow[ur, "f\circ g"'] \end{tikzcd} \qquad \text{y} \qquad \begin{tikzcd} S \arrow[r, "\iota"] \arrow[d, "\iota"'] & M \\ M \arrow[ur, "\mathrm{id}"'] \end{tikzcd}$$

conmutan, $f\circ g = \mathrm{id}_M$. Similarmente, $g\circ f = \mathrm{id}_{A^{(S)}}$. □

Nota 4.95. *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 4.96. *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) $\Rightarrow$ 2) Es suficiente verificar que hay un A-módulo simple. Para ello basta notar que por la Proposición 4.75, el anillo A tiene un ideal a izquierda maximal I, y que por la proposición 4.73, el módulo cociente A/I es simple.

2) $\Rightarrow$ 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

$$\begin{array}{c} A \xrightarrow{\rho(a)} M \\ a \longmapsto a \cdot m \end{array}$$

es un isomorfismo. Así, A es un A-módulo simple y entonces, por la Proposición 4.22, un anillo de división.

3) $\Rightarrow$ 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 B. Si $m \in M \setminus B$, entonces $B \cup \{m\}$ es linealmente dependiente y, por lo tanto, hay una combinación lineal no trivial

$$\lambda_m \cdot m + \sum_{b \in B} \lambda_b \cdot b = 0.$$

Por la independencia lineal de B, necesariamente $\lambda_m \neq 0$. Despejando obtenemos que

$$m = -\sum_{b \in B} \lambda_m^{-1} \lambda_b \cdot b,$$

lo cual prueba que $\langle B \rangle \supseteq (M \setminus B) \cup B = M$ y muestra que B es una base de M. $\square$

Observación 4.97. *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 aplicación $\pi\colon A^{(S)} \to M$, definida por $\pi(e_s) = s$, para todo $s \in S$, es un epimorfismo. Por lo tanto $M \approx A^{(S)}/\ker \pi$.*

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 $\bar{f}\colon M \to N$, tal que el triángulo

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "j"'] & N \\ M \arrow[ur, "\bar{f}"'] & \end{tikzcd},$$

  conmuta.

Observación 4.98. *Si (M, j) es un A-módulo libre sobre X, $l\colon Y \to X$ es una función biyectiva y $f\colon M \to N$ es un isomorfismo de A-módulos, entonces $(N, f \circ j \circ l)$ es un A-módulo libre sobre Y.*

Proposición 4.99. *Un par (M, j), formado por un A-módulo M y una función $j : X \to M$, 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. Dejamos como ejercicio para el lector probar que si φ es un isomorfismo, entonces (M, j) tiene la propiedad universal requerida. Recíprocamente, si (M, j) tiene esta propiedad, entonces hay un único morfismo $\psi\colon M \to A^{(X)}$ tal que el triángulo

$$\begin{tikzcd} X \arrow[r, "j"] \arrow[d, "\iota"'] & M \arrow[dl, "\psi"] \\ A^{(X)} & \end{tikzcd},$$

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 $(A^{(X)}, \{e_x : x \in X\})$ y (M, j), debe ser $\psi\circ\varphi = \mathrm{id}_{A^{(X)}}$ y $\varphi\circ\psi = \mathrm{id}_M$. □

Proposición 4.100. *Si un módulo libre M es finitamente generado, entonces todas sus bases son finitas; 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 4.62. □

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 $A^n \approx A^m \Leftrightarrow n = m$. Finalmente, puesto que tener un isomorfismo $A^n \approx A^m$ 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 claro que A tiene la ICB si y sólo si la existencia de tales matrices es imposible cuando $m \neq n$.

Ejemplo 4.101. *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 $\psi = (\psi_1, \psi_2)\colon B \to B \oplus B$, 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 4.102. *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 obtienem 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 4.103. *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

$$\begin{array}{ccc} A^n & \xrightarrow{\quad g \quad} & A^n \\ (x_1, \dots, x_n) & \longmapsto & f(x_1, \dots, x_m) \end{array},$$

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 4.104. *Todos los anillos conmutativos satisfacen la ICB.*

DEMOSTRACIÓN. Por el Corolario 4.76, hay un morfismo de A en un cuerpo. Entonces, por el item 3) de la Proposición 4.102, bastará probar los cuerpos tienen la ICB. Para comprobar esto es suficiente verificar que si $\{v_1, \dots, v_m\}$ y $\{w_1, \dots, w_n\}$ son bases de un k-espacio vectorial finitamente generado V y $m \leq n$, entonces es posible reordenar los w_j's, de forma tal que

$$(a_i) \qquad\qquad \{v_1, \dots, v_i, w_{i+1}, \dots, w_n\}$$

sea una base de M para todo $i \leq m$. Procedemos por inducción en i. La existencia de la base (a_0) es evidente. Supongamos que hay una reordenación de los w_j's tal que (a_0),…,(a_i) son bases y que $i < m$. Como $\{v_1, \dots, v_n\}$ es una base, obligatoriamente debe ser $n > i$. Escribamos

$$v_{i+1} = \lambda_1 v_1 + \cdots + \lambda_i v_i + \lambda_{i+1} w_{i+1} + \cdots + \lambda_m w_m,$$

como combinación lineal de los elementos de (a_i). Puesto que $v_1, \dots, v_{i+1}$ son linealmente independientes, $\lambda_j \neq 0$ para algún $j > i$. Podemos suponer sin pérdida de generalidad que $j = i + 1$. Usando que λ_{i+1} es inversible, se comprueba ahora fácilmente que (a_{i+1}) es una base de M. □

Ahora estamos en posición de probar el Teorema 1.99. Para ello será conveniente establecer primero un resultado auxiliar, que es importante en si mismo.

LEMA 4.105. *Si (G, j) es un grupo libre, entonces $(G/[G,G], \pi\circ j)$, 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 $\overline{\varphi}\colon G/[G,G]$ tales que el diagrama

$$\begin{tikzcd}
 & & H \\
X \arrow[r, "j"] \arrow[urr, "\varphi"] \arrow[dr, "\pi\circ j"'] & G \arrow[ur, "\tilde{\varphi}"] \arrow[d, "\pi"] & \\
 & \frac{G}{[G,G]} \arrow[uur, "\overline{\varphi}"'] &
\end{tikzcd},$$

donde π es la proyección canónica, conmuta. En particular, $\overline{\varphi}\circ\pi\circ j = \varphi$. Además $\overline{\varphi}$ es el único morfismo con esta propiedad, porque si $\psi\colon G/[G,G] \to H$ también satisface $\psi\circ\pi\circ j = \varphi$, entonces, por la propiedad universal de (G, j), forzosamente $\psi\circ\pi = \overline{\varphi}\circ\pi$ y, por lo tanto, dado que π es sobreyectivo, $\psi = \overline{\varphi}$. $\square$

Demostración del Teorema 1.99. Supongamos que (G, j) y (H, l) son grupos libres sobre X e Y respectivamente. Por los comentarios hechos al comienzo de la subsección 18.1 del Capítulo 1, sabemos que si G y H son isomorfos, entonces $G/[G,G]$ y $H/[H,H]$ también lo son. Debido al Lema 4.105 y al Teorema 4.104, 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

$$\begin{tikzcd}
X \arrow[r, "\varphi"] \arrow[d, "j"] & Y \arrow[d, "l"] \\
G \arrow[r, "\overline{\varphi}"] & H
\end{tikzcd}
\quad \text{y} \quad
\begin{tikzcd}
Y \arrow[r, "\varphi^{-1}"] \arrow[d, "l"] & X \arrow[d, "j"] \\
H \arrow[r, "\overline{\varphi^{-1}}"] & G
\end{tikzcd}$$

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 $\overline{\varphi}\circ\overline{\varphi^{-1}} = \mathrm{id}_H$. $\square$

18. 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

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0. \tag{39}$$

Como vimos en la Sección 17, esto ocurre si y sólo si f es inyectiva, g es sobreyectiva y $\ker g = \operatorname{Im} f$.

Decimos que la sucesión exacta corta (39) es equivalente a la sucesión exacta corta

$$0 \longrightarrow N' \xrightarrow{i} N \xrightarrow{p} N'' \longrightarrow 0\ ,$$

si existe un morfismo de A-módulos $h\colon M \to N$ tal que el diagrama

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "\mathrm{id}_{M'}"] & M \arrow[r, "g"] \arrow[d, "h"] & M'' \arrow[r] \arrow[d, "\mathrm{id}_{M''}"] & 0 \\
1 \arrow[r] & N' \arrow[r, "i"] & N \arrow[r, "p"] & N' \arrow[r] & 0
\end{tikzcd}$$

conmuta. Como vimos en la Sección 17, 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 4.106. *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, dados s y r como en el item 3), 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 sobreyectiva, de la igualdad

$$g{\circ}s{\circ}g = g{\circ}(f{\circ}r + s{\circ}g) = g$$

se sigue que s es una sección de g. Una cuenta similar muestra que r es una retracción de f. Pero entonces

$$r{\circ}s = r{\circ}(f{\circ}r + s{\circ}g){\circ}s = r{\circ}f{\circ}r{\circ}s + r{\circ}s{\circ}g{\circ}s = r{\circ}s + r{\circ}s,$$

por lo que $\operatorname{Im} s \subseteq \ker r$. En realidad $\operatorname{Im} s = \ker r$ porque

$$m = (f{\circ}r + s{\circ}g)(m) = s{\circ}g(m) \quad \text{para cada } m \in \ker r.$$

Ahora estamos listos para probar la equivalencia de los items 1), 2) y 3) y las últimas afirmaciones del enunciado. Notemos primero que en los comentarios anteriores ya fue probado que 1) y 2) son consecuencia de 3).

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) Un argumento similar al usado para probar que 1) $\Rightarrow$ 3) muestra que dada una retracción r de f, existe un único morfismo $s\colon M'' \to M$ tal que $f{\circ}r + s{\circ}g = \mathrm{id}_M$. □

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

$$(40)\qquad 0 \longrightarrow M' \xrightarrow{\iota_{M'}} M' \oplus M'' \xrightarrow{\pi_{M''}} M'' \longrightarrow 0\ ,$$

donde $\iota_{M'}$ y $\pi_{M''}$ son la inclusión y proyección canónicas, es escindida. El siguiente resultado muestra que este ejemplo es arquetípico.

Proposición 4.107. *Una sucesión exacta corta de A-módulos*

$$(41)\qquad 0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

es escindida si y sólo si es equivalente a la sucesión exacta corta (40).

Demostración. Basta observar que un morfismo $(r,h)\colon M \to M' \oplus M''$ realiza una equivalencia entre las sucesiones exactas cortas (40) y (41) si y sólo si $h = g$ y r es una retracción de f. □

19. Condiciones de cadena

Nuestro objetivo en esta seción es introducir las nociones de anillos noetherianos y artinianos y estudiar sus propiedades básicas. En esta exposición M designa a un A-módulo arbitrario.

19.1. Módulos noetherianos

Un A-módulo es *noetheriano* si todos sus submódulos son finitamente generados. En el siguiente resultado establecemos otras caracterizaciones muy útiles de esto módulos. Una sucesión $M_1, M_2, M_3, M_4, \dots$ 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 4.108. *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) ⇒ 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) ⇒ 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 $i_1, i_2, i_3, \dots$ 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 $i_1, \dots, i_n$ 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 4.109. *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

$$M' \cap N \qquad \text{y} \qquad \frac{M'}{M' \cap N} \approx \frac{M' + N}{N}$$

son finitamente generados. Pero entonces, por el item 2) de la Proposición 4.74, también lo es M'. □

COROLARIO 4.110. *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 4.111. *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,

$$\ker f^i \subsetneq \ker f^{i+1} \Rightarrow \ker f^{i+1} = f^{-1}(\ker f^i) \subsetneq f^{-1}(\ker f^{i+1}) = \ker f^{i+2}.$$

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 4.112. *Todo cociente de un anillo noetheriano a izquierda es un anillo noetheriano a izquierda.*

TEOREMA 4.113 (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 $P_1, P_2, \dots$ en I como sigue: Tomamos como P_1 a un polinomio no nulo de grado mínimo de I. Habiendo elegido $P_1, \dots, P_i$, 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 $J := \sum_{j\ge 1} Aa_j$ de A, es finitamente generado. Así, existe $m \in \mathbb{N}$ tal que $J = \sum_{j=1}^{m} Aa_j$. Escribamos $a_{m+1} = u_1a_1 + \cdots + u_m a_m$. Como el grado de P_{m+1} no es menor que el de ninguno de los polinomios $P_1, \dots, P_m$,

$$P := u_1 X^{\mathrm{gr}(P_{m+1})-\mathrm{gr}(P_1)} P_1 + \cdots + u_m X^{\mathrm{gr}(P_{m+1})-\mathrm{gr}(P_m)} P_m \in \sum_{j=1}^{m} A[X]P_j.$$

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}. $\square$

Corolario 4.114. *Si A es noetheriano a izquierda, entonces $A[X_1, \dots, X_n]/I$ es noetheriano para cada ideal I de $A[X_1, \dots, X_n]$.*

Demostración. Es consecuencia inmediata del Teorema de la base de Hilbert y de la Observación 4.112. $\square$

Proposición 4.115. *Si A es noetheriano a izquierda y M es un A-módulo finitamente generado, entonces M es noetheriano.*

Demostración. Por el corolario 4.110, todo módulo libre finitamente generado es noetheriano a izquierda. El resultado se sigue ahora del Teorema 4.109, ya que al ser finitamente generado, M es un cociente de un módulo libre, que también lo es. $\square$

Corolario 4.116. *Todo anillo noetheriano a izquierda o a derecha satisface la ICB.*

Demostración. Por el item 1) de la Proposición 4.102 basta probarlo para anillos noetherianos a izquierda, y para estos vale por la Proposiciones 4.103, 4.111 y 4.115 $\square$

Corolario 4.117. *Los anillos de división satisfacen la ICB.*

Proposición 4.118. *Consideremos submódulos $M_1, \dots, M_n$ 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 4.110, la suma directa $M_1 \oplus \cdots \oplus M_n$ es noetheriana. En consecuencia, por el Teorema 4.109, 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. $\square$

Corolario 4.119. *Consideremos submódulos $M_1, \cdots, M_n$ 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 4.110, 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 4.109 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 $\frac{M}{M_1 \cap \cdots \cap M_n}$. $\square$

19.2. Módulos artinianos

En esta subsección introducimos los módulos artinianos y estudiamos algunas de sus propiedades básicas.

PROPOSICIÓN 4.120. *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 $i_1, i_2, i_3 \dots$ 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 $i_1, \dots, i_n$ 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 4.121. *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 1.42 del Capítulo 1. □

COROLARIO 4.122. *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 4.123. *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 4.124. *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 4.125. *Todo anillo finito es artiniano.*

EJEMPLO 4.126. *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 semigrupo finito, entonces $A[S]$ es artiniano).*

PROPOSICIÓN 4.127. *Si A es artinianos a izquierda y M es un A-módulo finitamente generado, entonces M es artiniano.*

DEMOSTRACIÓN. Por el corolario 4.122, todo módulo libre finitamente generado es artiniano a izquierda. El resultado se sigue ahora del Teorema 4.121, ya que al ser finitamente generado, M es un cociente de un módulo libre con base finita. □

COROLARIO 4.128. *Consideremos submódulos $M_1, \dots, M_n$ 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 4.122, la suma directa $M_1 \oplus \cdots \oplus M_n$ es artiniana. Así, por el Teorema 4.121, 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 4.129. *Consideremos submódulos $M_1, \cdots, M_n$ 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 4.122, 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 4.121 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 $\frac{M}{M_1\cap\cdots\cap M_n}$. □

Hay grupos abelianos que son noetherianos y no artinianos. Por ejemplo, $\mathbb{Z}$. También hay grupos abelianos que son artinianos y no noetherianos. Un ejemplo es

$$\mathbb{Z}_{p^\infty} := \frac{\{a/p^n : a \in \mathbb{Z} \text{ y } n \in \mathbb{N}\}}{\mathbb{Z}}.$$

Para ver esto será suficiente probar que los subgrupos no triviales de $\mathbb{Z}_{p^\infty}$, son los subgrupos cíclicos $\langle [1/p^n] \rangle$. Supongamos que I es un subgrupo no trivial de $\mathbb{Z}_{p^\infty}$ y tomemos $[a/p^n] \in I$ con a coprimo con p. Entonces existen enteros r y s tales que $1 = ra + sp^n$. Así,

$$[1/p^n] = [(ra + sp^n)/p^n] = r[a/p^n] \in I.$$

Como $I \subsetneq \mathbb{Z}_{p^\infty}$ hay máximo n tal que $[1/p^n] \in I$ y, claramente, $I = \langle [1/p^n] \rangle$.

19.3. Módulos de longitud finita

Ahora vamos a estudiar los módulos que son simultaneamente noetherianos y artinianos. Decimos que dos cadenas crecientes finitas

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_m \qquad \text{y} \qquad M_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq N_n,$$

de submódulos de un A-módulo M, son *equivalentes* si $m = n$ y existe una permutación $\sigma \in \mathrm{S}_m$ tal que $\frac{M_i}{M_{i-1}} \approx \frac{N_{\sigma(i)}}{N_{\sigma(i)-1}}$, para todo i entre 1 y m; y decimos que la primera *refina* a la segunda si existen índices $1 \le i_1 < \cdots < i_n \le m$, tales que $M_{i_j} = N_j$ para todo j.

Lema 4.130 (Lema de la Mariposa). *Dados submódulos $N_1 \subseteq N_2$ y $M_1 \subseteq M_2$ de M, existen isomorfismos canónicos*

$$\frac{N_1 + (N_2 \cap M_2)}{N_1 + (N_2 \cap M_1)} \approx \frac{N_2 \cap M_2}{(N_1 \cap M_2) + (N_2 \cap M_1)} \approx \frac{M_1 + (N_2 \cap M_2)}{M_1 + (N_1 \cap M_2)}.$$

Demostración. El primer isomorfismo se obtiene aplicando el isomorfismo $\frac{L}{L\cap K} \approx \frac{L+K}{K}$ 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 4.131 (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

$$M_{ij} = M_{j-1} + (N_i \cap M_j) \qquad \text{y} \qquad N_{ij} = N_{i-1} + (N_i \cap M_j),$$

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 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

$$\frac{M_{ij}}{M_{i-1,j}} \approx \frac{N_{ij}}{N_{i,j-1}} \quad \text{para } 1 \le i \le n \text{ y } 1 \le j \le m.$$

El resultado es consecuencia inmediata de esto. □

Una cadena $0 = M_0 \subsetneq \cdots \subsetneq M_n = M$ 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 4.132 (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.

Es evidente que si M tiene longitud finita, digamos m, y N es un submódulo no trivial de M, entonces refinando la cadena $0 \subseteq N \subseteq M$ a una serie de composición

$$0 = N_0 \subsetneq \cdots \subsetneq N_i = N \subsetneq \cdots \subsetneq N_m = M, \tag{42}$$

obtenemos series de composición

$$0 = N_0 \subsetneq \cdots \subsetneq N_i = N \qquad \text{y} \qquad 0 = \frac{N_i}{N} \subsetneq \cdots \subsetneq \frac{N_m}{N} = \frac{M}{N}, \tag{43}$$

de N y M/N, respectivamente. 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 (43), combinándolas se obtiene una serie de composición como (42).

PROPOSICIÓN 4.133. *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 claro 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. □

TEOREMA 4.134 (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 los resultados mencionados en el comentario que precede a la Proposición 4.133 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 $\frac{M_1}{M_1 \cap M_2} \approx \frac{M_1+M_2}{M_2}$. □

En relación al teorema anterior, notemos que el hecho de que $M_1 \cap M_2$ tiene longitud finita es una consecuencia de que $M_1 + M_2$ la tiene.

20. Torsión y divisibilidad

En esta sección asumimos que A es un dominio conmutativo y estudiamos las nociones de torsión y divisibilidad de un A-módulo M.

20.1. Torsión

Un elemento m de 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. La *torsión* de M es el conjunto

$$\mathrm{T}(M) = \{m \in M : m \text{ es de torsión}\}.$$

Un módulo M es *de torsión* si $\mathrm{T}(M) = M$ y es *sin torsión* si $\mathrm{T}(M) = 0$.

EJEMPLO 4.135. *Cada A-módulo libre es sin torsión.*

EJEMPLO 4.136. $\mathbb{Q}$ *es un $\mathbb{Z}$-módulo sin torsión, que no es libre.*

PROPOSICIÓN 4.137. $\mathrm{T}(M)$ *es un submodulo 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

$$aa' \cdot (m + m') = aa' \cdot m + aa' \cdot m' = a'a \cdot m + aa' \cdot m' = 0 \quad \text{y} \quad a \cdot (b \cdot m) = ba \cdot m = 0$$

porque A es conmutativo, y que $aa' \neq 0$ porque A es un dominio. □

PROPOSICIÓN 4.138. *Para cada A-módulo M, el submódulo $\mathrm{T}(M)$ es de torsion y el módulo cociente $M/\mathrm{T}(M)$ es sin torsion.*

Demostración. Es evidente que la primera sfirmación es verdadera. Veamos que también lo es la segunda. Tomemos $m \in M$. Si $[m] \in T(M/\mathrm{T}(M))$, entonces $a \cdot m \in \mathrm{T}(M)$ para algún $a \in A \setminus \{0\}$ y, por lo tanto, existe $b \in A \setminus \{0\}$ tal que $ba \cdot m = 0$. Como $ba \neq 0$, esto implica que $m \in \mathrm{T}(M)$. □

Observación 4.139. *Cada morfismo de A-módulos $f\colon M \to N$ aplica $\mathrm{T}(M)$ en $\mathrm{T}(N)$. En consecuencia induce por restricción un morfismo $f_{\mathrm{T}}\colon \mathrm{T}(M) \to \mathrm{T}(N)$ y, por paso al cociente, un morfismo $\overline{f}_{\mathrm{T}}\colon M/\mathrm{T}(M) \to N/\mathrm{T}(N)$. Se comprueba de inmediato que $\mathrm{id}_{M_{\mathrm{T}}} = \mathrm{id}_{\mathrm{T}(M)}$ y $\overline{\mathrm{id}}_{M_{\mathrm{T}}} = \mathrm{id}_{M/\mathrm{T}(M)}$ para cada A-módulo M, y que*

$$(f{\circ}g)_{\mathrm{T}} = f_{\mathrm{T}}{\circ}g_{\mathrm{T}} \quad y \quad \overline{f{\circ}g}_{\mathrm{T}} = \overline{f}_{\mathrm{T}}{\circ}\overline{g}_{\mathrm{T}}$$

para cada par de morfismos de A-módulos $g\colon M \to N$ y $f\colon N \to L$. En consecuencia, f_{T} y $\overline{f}_{\mathrm{T}}$ son isomorfismos si f lo es.

Teorema 4.140. *Si N es un A-módulo finitamente generado y sin torsión, entonces existe un A-módulo libre finitamente generado M y un monomorfismo $\iota\colon N \to M$.*

Demostración. Fijemos un conjunto finito $S = \{n_1, \dots, n_s\}$ de generadores de N, tomemos un subconjunto linealmente independiente maximal $B = \{n_{i_1}, \dots, n_{i_d}\}$ de S y denotemos con M a $\langle B \rangle$. Por la definición de B, para cada $j \in S \setminus B$ 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

$$\begin{aligned} N &\xrightarrow{\ \iota\ } M \\ n &\longmapsto \lambda \cdot n \end{aligned} .$$

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. □

20.2. Divisibilidad

Decimos que M es *divisible* si para cada $m \in M$ y $a \in A \setminus \{0\}$, existe $m' \in M$ tal que $a \cdot m' = m$.

Ejemplo 4.141. *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 4.142. *Si M es divisible, entonces también lo es cada cociente M/N.*

Demostración. Porque $a \cdot m' = m \Rightarrow a \cdot [m'] = [m]$. □

Lema 4.143. *Si M es divisible y sin torsión, entonces para cada $m \in M$ y $a \in A \setminus \{0\}$ 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 4.144. *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

$$q \cdot \left(\frac{p}{q} \cdot m\right) = \frac{q}{1}\frac{p}{q} \cdot m = p \cdot m$$

para cada $\frac{p}{q} \in \mathbb{Q}_A$ y $m \in M$. 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 fuerza a definir

$$\frac{p}{q} \cdot m = m'. \tag{44}$$

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 $m' = m''$, porque M es un A-módulo sin torsión,

$$qs \cdot m'' = qr \cdot m = sp \cdot m = qs \cdot m'$$

y $qs \neq 0$. 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 (44). 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 4.145. *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. Como todo A-módulo es isomorfo a un cociente de un A-módulo libre, podemos suponer sin pérdida de generalidad que $N = A^{(I)}/S$ para un conjunto I y un submódulo S de $A^{(I)}$. Pero por la Proposición 4.142 sabemos que $M = \mathbb{Q}_A^{(I)}/S$ es divisible, y es evidente que hay un monomorfismo $\iota\colon N \to M$. Si $\mathrm{T}(N) = 0$, entonces la composición

$$N \xrightarrow{\iota} M \xrightarrow{\pi} M/T(M)\ ,$$

donde π es la proyección canónica, es inyectiva porque $\iota(N) \cap \mathrm{T}(M) = 0$. Por lo tanto 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.

Capítulo 5

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

TEOREMA 5.1. *Si A es un dominio principal, entonces todo submódulo de un A-módulo libre es libre.*

DEMOSTRACIÓN. Supongamos que L es un A-módulo libre y 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

$$L_i := \bigoplus_{j<i} \langle v_j \rangle, \quad \overline{L}_i := \bigoplus_{j\le i} \langle v_j \rangle, \quad M_i = M \cap L_i \quad \text{y} \quad \overline{M}_i = M \cap N_i$$

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 unica

$$m = m_i + \lambda_m \cdot v_i, \quad \text{con } m_i \in M_i \text{ y } \lambda_m \in A.$$

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 X_i de $\overline{M}_i$, tal que $\overline{M}_i = M_i \oplus M'_i$ y $X_i \approx \operatorname{Im} g_i$. 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

$$0 = m_{i_1} + \cdots + m_{i_r}, \quad \text{con } r \ge 1,\ m_{i_h} \in X_{i_h} \text{ e } i_1 < i_2 < \cdots < i_r,$$

y procedemos por inducción en r. Es claro que si $r = 1$, entonces $m_{i_1} = 0$. Supongamos entonces 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 ahora que

$$M = \bigoplus_{i \in I} M'_i.$$

Por definición, $\bigoplus_{i\in I} M'_i \subseteq M$. Supongamos que la inclusión recíproca no vale, y, para cada $m \in M \setminus \bigoplus_{i\in I} M'_i$, denotemos con $i(m)$ al menor de los $i \in I$ tal que $m \in \overline{L}_i$. Tomemos $m \in M \setminus \bigoplus_{i\in I} M'_i$ con $i(m)$ mínimo. Como

$$m \in \overline{M}_{i(m)} = M_{i(m)} \oplus M'_{i(m)},$$

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. Así, M es la suma directa de los M'_i, como queremos. □

Corolario 5.2. *Si A es un dominio principal, entonces todo A-módulo finitamente generado sin torsión es libre.*

Demostración. Es consecuencia inmediata de los Teoremas 4.140 y 5.1. □

Corolario 5.3. *Si A es un dominio principal, entonces $M \approx \mathrm{T}(M) \oplus M/\mathrm{T}(M)$ para todo A-módulo finitamente generado M.*

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, $M/\mathrm{T}(M)$ es libre. □

Observación 5.4. *Debido a los corolarios anteriores, todo A-módulo finitamente generado M tiene un submódulo libre L tal que $M = L \oplus \mathrm{T}(M)$. Si bien L no es único su dimensión sólo depende de M, porque L es isomorfo a $M/\mathrm{T}(M)$.*

2. Módulos de torsión

Consideremos un dominio principal A y un elemento irreducible $p \in A$. Un A-módulo M es *p-primario* si para todo $m \in M$ existe $n \in \mathbb{N}$ tal que $p^n \cdot m = 0$. Dado un 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*.

TEOREMA 5.5. *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 $c_1 b_1 + \cdots + c_r b_r = 1$. Por lo tanto

$$m = 1 \cdot m = c_1 b_1 \cdot m + \cdots + c_r b_r \cdot m.$$

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

$$m_1 + \cdots + m_s = 0, \quad \text{con } m_j \in M_{p_j}.$$

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 $h_1, \dots, h_s \in \mathbb{N}$ tales que $p_j^{h_j} \cdot m_j = 0$. Entonces

$$0 = p_1^{h_1} \cdots p_{s-1}^{h_{s-1}} \cdot (m_1 + \cdots + m_s) = p_1^{h_1} \cdots p_{s-1}^{h_{s-1}} \cdot m_s.$$

Pero como $p_1^{h_1} \cdots p_{s-1}^{h_{s-1}}$ y $p_s^{h_s}$ son coprimos, existen $a, b \in A$ tales que

$$ap_1^{h_1} \cdots p_{s-1}^{h_{s-1}} + bp_s^{h_s} = 1,$$

y, por lo tanto,

$$m_s = (1 - bp^{h_s}) \cdot m_s = ap_1^{h_1} \cdots p_{s-1}^{h_{s-1}} \cdot m_s = 0.$$

Ahora $m_1 = \cdots = m_{s-1} = 0$, por hipótesis inductiva. □

OBSERVACIÓN 5.6. *Dado un A-módulo M, el conjunto* $\operatorname{Ann}(M)$ *de todos los $a \in A$ tales que $a \cdot m = 0$ para todo $m \in M$ es un ideal de A. Supongamos que* $\operatorname{Ann}(M) = \langle a \rangle$, *con $a \neq 0$ y escribamos $a = up_1^{r_1} \cdots p_n^{r_n}$, con $u \in A^\times$, $p_1, \dots, p_n \in \mathcal{P}$ y $r_1, \dots, r_n \in \mathbb{N}$. Argumentando como en la demostración del Teorema 5.5 se comprueba fácilmente que*

$$M = M_{p_1} \oplus \cdots \oplus M_{p_n},$$

y que $\operatorname{Ann}(M_{p_i}) = \langle p_i^{r_i} \rangle$ *para todo i. En particular $M_q = 0$ para todo $q \in \mathcal{P} \setminus \{p_1, \dots, p_n\}$.*

OBSERVACIÓN 5.7. *Todo morfismo de A-módulos de torsión $f\colon M \to N$ aplica cada componente p-primaria M_p de M en la correspondiente componente N_p de N. En consecuencia, induce por restricción un morfismo $f_p\colon M_p \to N_p$. Es ovbio que f es un isomorfismo si y sólo si lo son todos los f_p.*

Teorema 5.8. *Si A es un dominio principal y M es un A-módulo anulable por p^n, donde p es un primo no nulo de A y $n \in \mathbb{N}$, entonces existen familias $(x_j^{(i)})_{j\in J_i}$ con $1 \le i \le n$ tales que*

$$M = \bigoplus_{i=1}^{n} \bigoplus_{j\in J_i} \langle x_j^{(i)} \rangle \quad y \quad \operatorname{Ann}(x_j^{(i)}) = \langle p^i \rangle,$$

dónde $\operatorname{Ann}(m) = \{a \in A : am = 0\}$*. Además el cardinal de los J_i's no depende de la descomposición.*

Demostración. Primero probamos la existencia. Consideremos la filtración

$$M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M,$$

donde $M_i = \{m \in M : p^i m = 0\}$. Consideremos también el A/pA-espacio vectorial M/pM y la filtración inducida

$$\frac{M_0 + pM}{pM} \subseteq \frac{M_1 + pM}{pM} \subseteq \cdots \subseteq \frac{M_n + pM}{pM} = \frac{M}{pM}.$$

Para cada i entre 1 y n tomemos familias $(x_j^{(i)})_{j\in J_i}$ en $M_i \setminus M_{i-1}$ tales que $\big([x_j^{(l)}]\big)_{l\le i,\, j\in J_l}$ es una base de $\frac{M_i+pM}{pM}$. Afirmamos que

$$M = \bigoplus_{i=1}^{n} \bigoplus_{j\in J_i} \langle x_j^{(i)} \rangle.$$

Veamos primero que la suma es directa. Para ello será suficiente probar que si existen $a_j^{(i)}$'s en A tales que

$$\sum_{i=1}^{n} \sum_{j\in J_i} a_j^{(i)} \cdot x_j^{(i)} = 0,$$

entonces

$$a_j^{(i)} \cdot x_j^{(i)} \in p^k A x_j^{(i)} \quad \text{para todo } i \in \mathbb{I}_n,\ j \in J_i \text{ y } k \ge 0. \tag{45}$$

Supongamos que (45) vale para un cierto k. Entonces existen $b_j^{(i)}$'s en A tales que

$$a_j^{(i)} \cdot x_j^{(i)} = p^k b_j^{(i)} \cdot x_j^{(i)}.$$

En particular

$$0 = \sum_{i=1}^{n} \sum_{j\in J_i} a_j^{(i)} \cdot x_j^{(i)} = \sum_{i=k+1}^{n} \sum_{j\in J_i} p^k b_j^{(i)} \cdot x_j^{(i)}$$

y, por lo tanto, $\displaystyle\sum_{i=k+1}^{n} \sum_{j\in J_i} b_j^{(i)} \cdot x_j^{(i)} \in M_k$. En consecuencia

$$\sum_{i=k+1}^{n} \sum_{j\in J_i} b_j^{(i)} \cdot [x_j^{(i)}] \in \frac{M_k + pM}{pM} = \bigoplus_{i\le k} \bigoplus_{j\in J_i} \langle [x_j^{(i)}] \rangle,$$

lo cual implica que la clase de $b_j^{(i)}$ en A/pA es cero. Así los $b_j^{(i)}$ son múltiplos de p y, por lo tanto,

$$a_j^{(i)} \cdot x_j^{(i)} = p^k b_j^{(i)} \cdot x_j^{(i)} \in p^{k+1} A x_j^{(i)},$$

como queríamos. Veamos ahora que la suma de los $\langle x_j^{(i)}\rangle$ con $i \le n$ y $j \in J_i$, da M. Designemos con N a esta suma. Como

$$\frac{N+pM}{pM} = \frac{M}{pM},$$

forzosamente $M = N + pM$. Afirmamos que

$$M = N + p^k M \quad \text{para todo } k \ge 0. \tag{46}$$

En efecto, si esto es cierto para un k, entonces

$$M = N + pM = N + pN + p^{k+1}M = N + p^{k+1}M.$$

Dado que $p^n M = 0$, de (46) se sigue que $N = M$.

Resta probar que el cardinal de los J_i sólo depende de M. Procedemos por inducción en n. Si $n = 1$, entonces M es un A/pA-espacio vectorial y en este caso el resultado se sigue de que dos bases de un espacio vectorial tienen en mismo cardinal. Supongamos ahora que $n > 1$ y que el resultado es cierto para módulos anulables por p^{n-1}. Como

$$pM = \bigoplus_{i=2}^{n} \bigoplus_{j\in J_i} \langle p x_j^{(i)}\rangle,$$

por la hiótesis inductiva aplicada a pM, el cardinal de los J_i con $i \ge 2$ depende sólo de M. Para ver que el cardinal de J_1 tampoco depende de la descomposición es suficiente notar que, como

$$p^2M = \bigoplus_{i=3}^{n} \bigoplus_{j\in J_i} \langle p^2 x_j^{(i)}\rangle \quad \text{y} \quad \{m \in M : pm \in p^2M\} = \bigoplus_{j\in J_1} \langle x_j^{(1)}\rangle \oplus \bigoplus_{i=2}^{n} \bigoplus_{j\in J_i} \langle p x_j^{(i)}\rangle,$$

las clases de los $x_j^{(1)}$'s en el A/pA-espacio vectorial

$$\frac{\{m \in M : pm \in p^2M\}}{pM}$$

forman una base de este. □

Observación 5.9. *Si un A-módulo M es anulado por un elemento no nulo de A, entonces el teorema anterior se puede aplicar a cada una de las componentes primarias de M, para obtener una descomposición de M como suma directa de módulos cíclicos primarios. Además, para cada $p \in \mathcal{P}$ e $i \in \mathbb{N}$, la cantidad de los módulos cíclicos cuyo anulador es $\langle p^i\rangle$, que aparecen en esta descomposición sólo depende de M, y es cero para todo $i \in \mathbb{N}$ si p no divide a un generador de* $\operatorname{Ann}(M)$.

Corolario 5.10. *Todo A-módulo finitamente generado y de torsión M se descompone como una suma directa $M = \langle x_1\rangle \oplus \cdots \oplus \langle x_n\rangle$, de submódulos cíclicos no nulos, tal que*

$$d_n \mid d_{n-1} \mid \cdots \mid d_1,$$

donde d_i es un generador de $\operatorname{Ann}(x_i)$. *Además n no depende de la descomposición y los d_i's son únicos módulo asociados.*

Demostración. Por la observación anterior existen $p_1, \dots, p_r \in \mathcal{P}$ tal que

$$M = M_{p_1} \oplus \cdots \oplus M_{p_r}$$

y cada M_{p_i} es suma directa de módulos cíclicos

$$M_{p_i} = \langle x_1^{(i)} \rangle \oplus \cdots \oplus \langle x_{j_i}^{(i)} \rangle.$$

Supongamos que hemos ordenado los sumandos de cada una de estas descomposiciones, de manera tal que si $p_i^{n_{ij}} = \operatorname{Ann}(x_j^{(i)})$, entonces $n_{i1} \geq \cdots \geq n_{ij_i}$. Escribamos

$$M = N \oplus \langle x_1^{(1)} \rangle \oplus \cdots \oplus \langle x_1^{(r)} \rangle,$$

donde

$$N = \bigoplus_{i=1}^{r} \left(\langle x_2^{(i)} \rangle \oplus \cdots \oplus \langle x_{j_i}^{(i)} \rangle \right).$$

Como, por el Teorema chino de los restos,

$$\langle x_1^{(1)} \rangle \oplus \cdots \oplus \langle x_1^{(r)} \rangle \approx \frac{A}{\langle p_1^{n_{11}} \rangle} \oplus \cdots \oplus \frac{A}{\langle p_r^{n_{r1}} \rangle} \approx \frac{A}{\langle p_1^{n_{11}} \cdots p_r^{n_{r1}} \rangle}$$

el submódulo $\langle x_1^{(1)} \rangle \oplus \cdots \oplus \langle x_1^{(r)} \rangle$ es cíclico y $d_1 := p_1^{n_{11}} \cdots p_r^{n_{r1}}$ genera a su anulador. La demostración de la existencia de la descomposición se termina ahora fácilmente por inducción en la cantidad de sumandos de la descomposición de M como suma directa de módulos primarios no nulos. En cuanto a la unicidad, esta se sigue de que si $d_i = p_1^{n_{1i}} \cdots p_r^{n_{ri}}$, entonces, por el Teorema chino de los restos,

$$\langle x_i \rangle \approx \frac{A}{\langle d_i \rangle} \approx \frac{A}{\langle p_1^{n_{1i}} \rangle} \oplus \cdots \oplus \frac{A}{\langle p_1^{n_{ri}} \rangle},$$

y de la unicidad de los anuladores de los módulos que aparecen en cualquier descomposición de M como suma directa de módulos cíclicos primarios no nulos. □

Los elementos $d_1, \dots, d_n$ de A obtenidos en la demostración anterior (o cualesquiera asociados a ellos) son llamados factores invariantes de M.

OBSERVACIÓN 5.11. *Dos A-módulos finitamente generados M y N son isomorfos si y sólo si $M/\operatorname{T}(M)$ y $N/\operatorname{T}(N)$ tienen la misma dimensión y sus submódulos de torsión $\operatorname{T}(M)$ y $\operatorname{T}(N)$ tienen los mismos factores invariantes.*

OBSERVACIÓN 5.12. *Si M es un A-módulo finitamente generado, entonces por la Observación 5.4, sabemos que hay un submódulo libre L de M, cuya dimensión sólo depende de M, tal que $M = L \oplus \operatorname{T}(M)$. Como $\operatorname{T}(M)$ es finitamente generado, su anulador $\operatorname{Ann}(\operatorname{T}(M))$ no es nulo y, en consecuencia, se puede aplicar la Observación 5.9, para obtener una descomposición de $\operatorname{T}(M)$ como suma directa de módulos cíclicos primarios, y el corolario anterior, para obtener una como suma directa de submódulos cíclicos cuyos anuladores están generados por elementos de A, cada uno de los cuales divide al anterior.*