
ÁLGEBRA

Grupos Anillos y Módulos

JORGE ALBERTO GUCCIONE

Y

JUAN JOSÉ GUCCIONE

Índice general

1 Grupos	1
Capítulo 1. Teoría elemental	3
1 Monoides	3
2 Submonoides	6
2.1 Ejemplos	7
3 Morfismos de monoides	7
4 Grupos	9
5 Subgrupos	10
5.1 Subgrupos de un grupo cíclico	13
5.2 Subgrupos de los grupos diedrales y cuaterniónicos	13
6 Coclasas a izquierda y a derecha	14
7 Coclasas dobles	17
8 Subgrupos normales	18
9 Una caracterización de los grupos cíclicos finitos	20
10 Morfismos de grupos	22
10.1 Estructuras en el conjunto de los morfismos de un grupo en otro	25
11 Núcleo e imagen	25
12 Cociente de grupos	26
13 Grupos libres y presentaciones	32
13.1 Grupos libres	32
13.2 Presentaciones	35
14 Producto directo	39
14.1 Producto directo interno	39
14.2 Producto directo	40
14.3 Producto directo restringido	42
14.4 Morfismos entre productos directos finitos de grupos	45
15 Producto semidirecto	47
15.1 Producto semidirecto interno	47
15.2 Producto semidirecto	48
16 Sucesiones exactas cortas	51

17	Automorfismos interiores y subgrupos característicos	56
17.1	Subgrupo conmutador y abelianizado	59
17.2	El conmutador de dos subgrupos	60
17.3	Subgrupos conjugados	61
17.4	El normalizador y el centralizador	62
Capítulo 2. El grupo simétrico		65
1	Estructura cíclica	65
2	Generadores de \mathbf{S}_n	69
3	El signo de una permutación	70
4	Generadores de \mathbf{A}_n	71
5	El conmutador y el centro de \mathbf{S}_n y \mathbf{A}_n	72
6	Presentaciones de \mathbf{S}_n y \mathbf{A}_n	75
Capítulo 3. Acciones de grupos		79
1	Acciones y \mathbf{G} -espacios	79
2	Núcleo de una acción, teorema de Cayley y aplicaciones	80
3	Subconjuntos estables y morfismos	83
4	Más ejemplos	83
5	Órbitas, puntos fijos y estabilizadores	85
5.1	La ecuación de las clases	89
5.2	\mathbf{k} -transitividad	91
5.3	Contando órbitas	91
6	Teoremas de Sylow	92
6.1	Algunos ejemplos	95
6.2	Algunas aplicaciones	98
	Aplicaciones a grupos de orden pequeño	100
7	\mathbf{p} -Grupos finitos	101
2 Anillos y módulos		109
Capítulo 4. Teoría elemental de anillos		111
1	Anillos	111
2	Subanillos	114
3	Ideales	117
4	Morfismos de anillos	120
5	Núcleo e imagen	122
6	Cociente de anillos por ideales	122
7	Ideales primos en anillos conmutativos	124
8	Producto de anillos	125
8.1	El teorema chino del resto	127
9	El anillo de un monoide	128
10	Los cuaterniones	133
11	El cuerpo de cocientes de un dominio conmutativo	136
Capítulo 5. Dominios de factorización única		139

Índice general

1	Monoides factoriales	139
2	Dominios de factorización única	142
	Capítulo 6. Teoría elemental de módulos	145
1	Módulos.	145
2	Submódulos	147
3	Morfismos de módulos	149
	3.1 Estructuras en el conjunto de los morfismos de un módulo en otro	150
4	Núcleo e imagen	150
5	Cociente de módulos.	151
6	Producto y coproducto directo.	154
	6.1 Suma directa interna	154
	6.2 Producto directo.	155
	6.3 Coproducto directo.	157
	6.4 Morfismos entre sumas directas finitas de A -módulos	159
7	Sucesiones exactas cortas	160
	Capítulo 7. Algunos tipos de módulos	163
1	Módulos libres	163
2	Módulos de torsión y divisibles.	168
	2.1 Torsión	168
	2.2 Divisibilidad	169
3	Módulos proyectivos y módulos inyectivos	171
	Capítulo 8. Condiciones de cadena	177
1	Módulos noetherianos	177
2	Módulos artinianos	180
3	Módulos de longitud finita	182
	Capítulo 9. Módulos sobre dominios principales	185
1	Módulos libres	185
2	Módulos de torsión	187
3	Teoremas de estructura.	189

Parte 1

Grupos

Capítulo 1

Teoría elemental

1. Monoides

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

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

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

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

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

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

Un elemento $e \in S$ es *neutro a izquierda* si $e * s = s$ para todo $s \in S$, es *neutro a derecha* si $s * e = s$ para todo $s \in S$ y es *neutro* si lo es a izquierda y a derecha. Si un magma S tiene neutro a izquierda e y neutro a derecha e' , entonces $e = e'$. En efecto, como e' es neutro a derecha, $e = e * e'$ y como e es neutro a izquierda, $e * e' = e'$. En particular S tiene a lo sumo un neutro. Diremos que un magma es *unitario* si tiene neutro. Evidentemente 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 *invertible a izquierda* si existe $t \in S$ tal que $t * s = e$, y es *invertible 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 *invertible*, si lo es a ambos lados. Es claro que s es invertible a izquierda si y sólo si r_s es sobreyectiva, e invertible a derecha si y sólo si l_s es sobreyectiva. Si s tiene inversa a izquierda y a derecha, entonces estas son únicas y coinciden. En efecto, supongamos que t es una inversa a izquierda de s , y t' una inversa a derecha. Entonces

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

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

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

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

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

similarmente, que los elementos inversibles a derecha son cancelables a derecha. El siguiente resultado completa el panorama general.

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

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

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

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

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

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

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

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

DEMOSTRACIÓN. Como S es finito,

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

Por dualidad,

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

El resultado es una consecuencia inmediata de estos dos hechos. \square

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 1.3. *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 monoïdes abelianos vía el producto. Salvo \mathbb{N} todos los demás también lo son vía la suma.*

EJEMPLO 1.4. *El conjunto $\text{Fun}(X, X)$, de las funciones de un conjunto X en si mismo, es un monoïde vía la composición, que sólo es abeliano cuando el cardinal de X es menor o igual que 1.*

EJEMPLO 1.5. *Para cada número natural n , el conjunto $M_n(k)$ de las matrices de $n \times n$ con coeficientes en un cuerpo k , es un monoïde cuyo neutro es la matriz identidad, vía el producto.*

EJEMPLO 1.6. *El conjunto $\text{End}_k(V)$, de los endomorfismos de un k -espacio vectorial V , es un monoïde cuyo neutro es la función identidad, vía la composición. Si $\dim_k(V) \geq 2$, entonces $\text{End}_k(V)$ no es abeliano.*

2. Submonoides

Un subconjunto T de un monoïde S es un *submonoïde* de S si es cerrado para el producto y $1 \in T$. Es evidente que entonces T es un monoïde. 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 submonoïde de S es *propio* si es distinto de S . Es claro que la intersección de una familia arbitraria de submonoides de S es un submonoïde 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 submonoïde $\langle U \rangle_M$ de S que contiene a U , el cual es llamado el *submonoïde de S generado por U* . Si $S = \langle U \rangle_M$, decimos que U *genera* a S . Siguiendo una práctica usual, escribiremos $\langle u_1, \dots, u_n \rangle_M$ en lugar de $\langle \{u_1, \dots, u_n\} \rangle_M$. Esto se debe simplemente a una cuestión de estética. Un monoïde 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 $S = \langle s \rangle_M$. Dejamos a cargo del lector comprobar que, si adoptamos la convención de que el producto vacío da 1, entonces, para cada familia U de elementos de S ,

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

Para cada par de subconjuntos K y L de un monoide S , denotamos con KL al subconjunto de S formado por todos los productos kl con $k \in K$ y $l \in L$. Por supuesto, escribiremos sK y Ks en lugar de $\{s\}K$ y $K\{s\}$, respectivamente. En general $KL \subseteq \langle K \cup L \rangle_M$, 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 1.7. *Si K y L son submonoides de S , entonces KL es un submonoide de S si y sólo si $LK \subseteq KL$.*

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

$$KLKL \subseteq KKLL = KL.$$

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

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

Notemos que si $S_i S_j = S_j S_i$ 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* $\varphi: S \rightarrow S'$ es una terna (S, φ, S') , formada por dos monoides S y S' y una función φ del conjunto subyacente de S en el de S' , que satisface:

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

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

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

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

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

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

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

Son ejemplos de morfismos de monoides

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

Es evidente que si $\varphi: S \rightarrow S'$ 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 $\varphi: S \rightarrow S'$ es un *isomorfismo* si existe un morfismo $\varphi^{-1}: S' \rightarrow S$, necesariamente único, llamado la *inversa* de φ , tal que $\varphi^{-1} \circ \varphi = \text{id}_S$ y $\varphi \circ \varphi^{-1} = \text{id}_{S'}$. Es fácil ver que esto ocurre si y sólo si φ es biyectiva. Dos monoides S y S' son *isomorfos* si hay un isomorfismo de S en S' . En ese caso escribimos $S \simeq S'$. Un *automorfismo* de S es un endomorfismo de S que es un isomorfismo. Los símbolos $\text{Hom}_M(S, S')$, $\text{Iso}_M(S, S')$, $\text{End}_M(S)$ y $\text{Aut}_M(S)$ denotan respectivamente a los conjuntos de morfismos de S en S' , isomorfismos de S en S' , endomorfismos de S y automorfismos de S . Es obvio que $\text{End}_M(S)$ es un monoide (cuyo elemento neutro es la función identidad) vía la composición. Decimos que un morfismo $\varphi: S \rightarrow S'$ es un *monomorfismo* si $\varphi \circ \psi = \varphi \circ \psi' \Rightarrow \psi = \psi'$ para todo par de morfismos de monoides $\psi, \psi': S'' \rightarrow S$ con codominio S , un *epimorfismo* si $\psi \circ \varphi = \psi' \circ \varphi \Rightarrow \psi = \psi'$ para todo par de morfismos de monoides $\psi, \psi': S' \rightarrow S''$ con dominio S' , una *sección* si existe $\psi: S' \rightarrow S$ tal que $\psi \circ \varphi = \text{id}_S$ y una *retracción* si existe $\zeta: S' \rightarrow S$ tal que $\varphi \circ \zeta = \text{id}_{S'}$. Como el lector podrá comprobar sin dificultad, los monomorfismos, epimorfismos, secciones y retracciones son cerrados bajo la composición, toda retracción es sobreyectiva, toda sección es inyectiva, todo morfismo inyectivo es un monomorfismo y todo morfismo sobreyectivo es un epimorfismo. Además un morfismo $\varphi: S \rightarrow S'$ 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 apenas un poco más difícil de verificar es que todo monomorfismo $\varphi: S \rightarrow S'$ es inyectivo. Para comprobar esto supongamos que $\varphi(r) = \varphi(s)$ y consideremos los morfismos de monoides $\psi, \psi': \mathbb{N}_0 \rightarrow S$, definidos por

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

Como

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

y φ es un monomorfismo, obtenemos que $\psi = \psi'$ y, por lo tanto, $r = \psi(1) = \psi'(1) = s$.

Por último, para cada par $\varphi: S \rightarrow S'$ y $\psi: S' \rightarrow S''$ de morfismos,

1. Si $\psi \circ \varphi$ es una sección o un monomorfismo, entonces también lo es φ .

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

EJEMPLO 1.8. Supongamos que X es un subconjunto de Y . Definamos

$$i_*: \text{Fun}(X, X) \rightarrow \text{Fun}(Y, Y)$$

por

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

Es evidente que i es un morfismo inyectivo de monoïdes.

EJEMPLO 1.9. Supongamos que $i: X \rightarrow Y$ es una biyección. Definamos

$$i_*: \text{Fun}(X, X) \rightarrow \text{Fun}(Y, Y)$$

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

EJEMPLO 1.10. Supongamos que $i: X \rightarrow Y$ es una función inyectiva. Definamos

$$i_*: \text{Fun}(X, X) \rightarrow \text{Fun}(Y, Y)$$

por

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

Es fácil ver que:

- i_* es un morfismo inyectivo de monoïdes cuya imagen es el conjunto de las funciones de Y en si mismo que dejan fijos a los elementos que están fuera de $i(X)$.
- Si X es un subconjunto de Y e i es la inclusión canónica de X en Y recuperamos la definición dada en el Ejemplo 1.8, mientras que si i es una biyección recuperamos la dada en el Ejemplo 1.9.
- Si $j: Y \rightarrow Z$ es otra función inyectiva, entonces $(j \circ i)_* = j_* \circ i_*$.

4. Grupos

Un grupo G es un monoïde 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 monoïde 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. \square

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 $g, g' \in G$. □

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 submonoide S^\times , de los elementos inversibles de un monoide S , es un grupo llamado el grupo de unidades de S . Por ejemplo, si S es un monoide, entonces $\text{Aut}_M(S)$ es el grupo de unidades de $\text{End}_M(S)$.*

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 $\text{GL}(V)$ es el grupo de unidades del anillo de endomorfismos $\text{End}_k(V)$. Este grupo es abeliano si y sólo si $\dim_k(V) = 1$.*

EJEMPLO 1.16. *El grupo $\text{GL}(n, k)$ es el grupo de unidades del anillo $M_n(k)$, 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 $\varphi: X \rightarrow X$. 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 $\text{Fun}(X, X)$. Cuando $|X| \geq 3$ este grupo no es conmutativo. Para comprobarlo es suficiente considerar $x_1, x_2, x_3 \in X$ y exhibir dos permutaciones σ y τ de X que se restringen a la identidad sobre $X \setminus \{x_1, x_2, x_3\}$ y no conmutan. Por ejemplo, podemos tomar*

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

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

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

4. $h^{-1}l \in H$ para todo $h, l \in H$.

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

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

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 $\langle T \rangle_M$ puede estar incluido propiamente en $\langle T \rangle$. Por ejemplo, si $G = \mathbb{Z}$, entonces $\langle \mathbb{N} \rangle_M = \{0\} \cup \mathbb{N}$ y $\langle \mathbb{N} \rangle = \mathbb{Z}$. Sin embargo, si $g \in G$ tiene orden finito y $g \in \langle T \rangle_M$, entonces g^{-1} pertenece a $\langle T \rangle_M$, porque es una potencia de g . En consecuencia, si $T \neq \emptyset$ y todos sus elementos tienen orden finito, $\langle T \rangle_M = \langle T \rangle$. 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. *Un subgrupo G del grupo aditivo \mathbb{R} es discreto si para cada $g \in G$ existe $\varepsilon > 0$ tal que $G \cap (g - \varepsilon, g + \varepsilon) = \{g\}$. Pruebe que todo grupo discreto es cíclico.*

EJERCICIO 1.20. *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 1.21. *Los conjuntos $\mathbb{Q}_{>0}$ y $\mathbb{R}_{>0}$ son subgrupos de \mathbb{Q}^\times y \mathbb{R}^\times , respectivamente*

EJEMPLO 1.22. *El conjunto $\mathbb{Z}[X]$, de polinomios con coeficientes enteros, es un subgrupo de $\mathbb{Q}[X]$.*

EJEMPLO 1.23. *Consideremos un espacio euclideo E . El grupo ortogonal de E es el subgrupo $O(E)$ de $GL(E)$, formado por las transformaciones ortogonales de E . El grupo lineal especial $SO(E)$ es el subgrupo de $O(E)$ formado por las transformaciones ortogonales con determinante 1.*

EJEMPLO 1.24. *El conjunto $SL(n, k)$, de las matrices de $n \times n$ de determinante 1 con coeficientes en un cuerpo k , es un subgrupo de $GL(n, k)$.*

EJEMPLO 1.25. *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 $G_\infty := \bigcup_{n \in \mathbb{N}} G_n$.*

EJEMPLO 1.26. Consideremos el ángulo $\theta := 2\pi/n$, donde $n \in \mathbb{N}$ es mayor que 1. El subgrupo de $\text{GL}(2, \mathbb{R})$ generado por

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

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

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

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

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

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

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

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

EJEMPLO 1.27. Tomemos $w := e^{i\pi/n}$ donde $n \in \mathbb{N}$ es mayor que 1. Es claro que w es una raíz de la unidad $w \in \mathbb{C}$ de orden $2n$. El subgrupo de $\text{GL}(2, \mathbb{C})$ generado por

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

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

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

Notemos que de estas condiciones se sigue que $x^n = yy^2y^{-1} = yx^ny^{-1} = x^{-n}$ 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 $2n/(2n:i)$. En consecuencia, para cada divisor d de $2n$ hay $\phi(d)$ elementos de orden d de la forma x^i .

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

5.1. Subgrupos de un grupo cíclico

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

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

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

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

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

por lo que $r = 0$ y $H = \langle g^{n_0} \rangle$. De paso, notemos que como $g^{|g|} = 1$, la cuenta anterior implica que n_0 divide a $|g|$.

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

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

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

5.2. Subgrupos de los grupos diedrales y cuaterniónicos

A continuación calculamos los subgrupos de D_n y H_n . Usaremos libremente las notaciones introducidas en los Ejemplos 1.26 y 1.27. Consideremos primero un subgrupo H de D_n . Si $H \subseteq \langle x \rangle$, entonces $H = \langle x^i \rangle$, donde i es un divisor de n . Supongamos ahora que $H \not\subseteq \langle x \rangle$ y que j el mínimo entero no negativo tal que $x^j y \in H$. Denotemos con i al único divisor positivo de n tal que $H \cap \langle x \rangle = \langle x^i \rangle$. Claramente

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

lo que muestra en particular que $0 \leq j < i$. Es fácil ver que la unión que aparece a la izquierda de esta inclusión es igual a $\langle x^i, x^j y \rangle$. Afirmamos que este grupo coincide con H . En efecto si $x^{j'} y \in H$, entonces $x^{j'-j} = x^{j'} y (x^j y)^{-1} \in H \cap \langle x \rangle$ y, en consecuencia, $x^{j'-j} = x^{hi}$ para algún $0 \leq h < n/i$, lo que implica que $x^{j'} y = x^{j+hi} y \in \langle x^i, x^j y \rangle$. Notemos finalmente que si m divide a n , entonces $D_m = \langle x^{n/m}, y \rangle$ es un subgrupo de D_n .

Tomemos ahora un subgrupo H de H_n . Si $H \subseteq \langle x \rangle$, entonces $H = \langle x^i \rangle$, donde i es un divisor de $2n$. Supongamos ahora que $H \not\subseteq \langle x \rangle$ y que j el mínimo entero no negativo tal que

$x^j y \in H$. Denotemos con i al único divisor positivo de $2n$ tal que $H \cap \langle x \rangle = \langle x^i \rangle$. Dado que $x^n = y^2 = x^j y x^j y \in H \cap \langle x \rangle$, necesariamente $i \mid n$. Claramente

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

lo que muestra en particular que $0 \leq j < i$. Es fácil ver que la unión que aparece a la izquierda de esta inclusión es igual a $\langle x^i, x^j y \rangle$. Afirmamos que este grupo coincide con H . En efecto si $x^{j'} y \in H$, entonces $x^{j'-j} = x^{j'} y (x^j y)^{-1} \in H \cap \langle x \rangle$ y, en consecuencia, $x^{j'-j} = x^{hi}$ para algún $0 \leq h < n/i$, lo que implica que $x^{j'} y = x^{j+hi} y \in \langle x^i, x^j y \rangle$. Notemos finalmente que si m divide a n , entonces $H_m = \langle x^{n/m}, y \rangle$ es un subgrupo de H_n .

6. Coclasas a izquierda y a derecha

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

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

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

TEOREMA 1.28 (Lagrange). *Para cada $H \leq G$, los ordenes de H y G están relacionados por la igualdad*

$$(2) \quad |G| = |G : H| |H|,$$

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

El mismo razonamiento, aplicado a las coclasas 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 (2). Más aún, como la aplicación $gH \mapsto Hg^{-1}$ (que está bien definida pues de $g_1 H = g_2 H$ se sigue que $Hg_1^{-1} = (g_1 H)^{-1} = (g_2 H)^{-1} = Hg_2^{-1}$) es una función biyectiva del conjunto G/H de las coclasas a izquierda de H en G , en el conjunto $G \setminus H$ de las coclasas a derecha H en G , ambos tienen el mismo cardinal.

EJERCICIO 1.29. *Calcule las coclasas a izquierda y a derecha de $\langle y \rangle$ en D_n y muestre que en general no coinciden.*

EJERCICIO 1.30. *Calcule las coclasas a izquierda y a derecha de $\langle y \rangle$ en H_n y muestre que en general no coinciden.*

OBSERVACIÓN 1.31. *Del teorema de Lagrange se sigue inmediatamente que si H y L son subgrupos finitos de un grupo G , entonces $|H \cap L|$ divide a $(|H| : |L|)$. En particular si $|H|$ y $|L|$ son coprimos, entonces $H \cap L = 1$.*

COROLARIO 1.32. Si G es finito, entonces el exponente de G divide al orden de G .

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

COROLARIO 1.33. Si un grupo G tiene orden primo, entonces es cíclico.

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

OBSERVACIÓN 1.34. Debido al teorema de Lagrange si un grupo finito G tiene elementos de orden 2, entonces $|G|$ es par. En realidad también vale la recíproca. Para comprobarlo supongamos que $|G|$ es par y consideremos la partición

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

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

El resultado que sigue generaliza la igualdad (2).

TEOREMA 1.35. Si K y H son subgrupos de un grupo G y $K \subseteq H$, entonces

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

DEMOSTRACIÓN. Escribamos G y H como uniones disjuntas

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

de coclasas 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 $j = j'$. \square

OBSERVACIÓN 1.36. Del teorema anterior se sigue que si H , L y K son subgrupos de un grupo G , tales que $K \subseteq H \cap L$ y $|H : K|$ y $|L : K|$ son finitos, entonces $|H \cap L : K|$ divide a $(|H : K| : |L : K|)$. En particular si $|H : K|$ y $|L : K|$ son coprimos, entonces $H \cap L = K$.

OBSERVACIÓN 1.37. Si la intersección de una familia $(g_i H_i)_{i \in I}$ de coclasas a izquierda de un grupo G no es vacía, entonces es una coclase a izquierda de la intersección de los H_i 's. En efecto, si $g \in \bigcap_{i \in I} g_i H_i$, entonces $g H_i = g_i H_i$ para todo $i \in I$ y, por lo tanto,

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

OBSERVACIÓN 1.38. Consideremos dos subgrupos H y L de un grupo G . Como $hL = h'L \Leftrightarrow h^{-1}h' \in L \Leftrightarrow h^{-1}h' \in H \cap L \Leftrightarrow h(H \cap L) = h'(H \cap L)$ para todo $h, h' \in H$, la aplicación

$$\begin{array}{ccc} H/(H \cap L) & \xrightarrow{s} & G/L, \\ h(H \cap L) & \longmapsto & hL \end{array}$$

es inyectiva. Dado que además $\text{Im } \varsigma = \{hL : h \in H\}$ y $|G : H \cap L| = |G : H||H : H \cap L|$, se sigue de esto que

$$(3) \quad |H : H \cap L| = |HL : L| \quad y \quad |G : H \cap L| = |G : H||HL : L|,$$

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

$$(4) \quad |H : H \cap L| \leq |G : L| \quad y \quad |G : H \cap L| \leq |G : H||G : L|.$$

Además, si HL es un subgrupo de G , entonces

$$|H : H \cap L||G : HL| = |G : L| \quad y \quad |G : H \cap L||G : HL| = |G : H||G : L|$$

y, por lo tanto, si $HL = G$ las desigualdades (4) se convierten en igualdades.

De la presente exposición se sigue que:

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

Por último, si $|G : H|$ y $|G : L|$ son finitos, entonces

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

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

PROPOSICIÓN 1.39. 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 $g = kl \in KL$. \square

EJERCICIO 1.40. Pruebe que cada elemento de un cuerpo finito es suma de dos cuadrados.

Las últimas tres proposiciones de esta subsección están dedicadas al estudio del producto de subgrupos. En la primera establecemos dos propiedades generales conocidas como ley modular y ley de Dedekind, respectivamente, 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 1.41. Si $K \leq H$ y L son subgrupos de un grupo G , entonces

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

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

2) Por el ítem 1) y las hipótesis,

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

como queríamos. \square

PROPOSICIÓN 1.42. *Si H y L son subgrupos de un grupo G , entonces*

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

DEMOSTRACIÓN. Como la función $\varsigma: H \times L \rightarrow HL$, 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 $y \in H \cap L$. \square

PROPOSICIÓN 1.43. *Para cada par de subgrupos H y L de un grupo G son equivalentes:*

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

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

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

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

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

como queremos. \square

7. Coclasas dobles

Consideremos dos subgrupos (no necesariamente distintos) H y L de un grupo G . Una (H, L) -coclasa 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 coclasas dobles. Afirmamos que si L es finito, entonces

$$(5) \quad |G : L| = \sum_{i \in I} |H : H \cap g_iLg_i^{-1}|.$$

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

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

Pero $|Hg_iL| = |Hg_iLg_i^{-1}|$ y, dado que H y $g_iLg_i^{-1}$ son subgrupos de G , de la Proposición 1.42 se sigue que

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

como necesitamos. Cuando $L = 1$, la fórmula (5) se reduce a la establecida en el teorema de Lagrange.

EJEMPLO 1.44. *Escribamos $S_3 = \{\text{id}, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$, donde*

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

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

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

8. Subgrupos normales

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

PROPOSICIÓN 1.45. *Para cada $N \leq G$ son equivalentes:*

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

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

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

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

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

Los items 1) y 2) son equivalentes porque

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

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

EJEMPLO 1.46. *Recordemos que el grupo diedral D_n es el subgrupo de $GL(2, \mathbb{R})$ generado por las matrices*

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

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

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

Lo primero es obvio y lo segundo se sigue de que

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

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

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

y, por lo tanto,

$$N = \bigcup_{0 \leq j < n/2} \{x^{2j}, x^{2j} y\}, \quad N = \bigcup_{0 \leq j < n/2} \{x^{2j}, x^{2j+1} y\} \quad o \quad N = D_n$$

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

EJEMPLO 1.47. Recordemos que el grupo cuaterniónico generalizado H_n es el subgrupo de $GL(2, \mathbb{C})$ generado por las matrices

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

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

$$N = \bigcup_{0 \leq j < n} \{x^{2j}, x^{2j} y\}, \quad N = \bigcup_{0 \leq j < n} \{x^{2j}, x^{2j+1} y\} \quad o \quad N = H_n$$

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

EJERCICIO 1.48. Pruebe que un subgrupo N de G es invariante si y sólo si $hg \in N$ siempre que $gh \in N$.

OBSERVACIÓN 1.49. Si $N \subseteq L$ son subgrupos de un grupo G y $N \triangleleft G$, entonces $N \triangleleft L$.

OBSERVACIÓN 1.50. Si $N \triangleleft G$, entonces $NL = LN$ para todo subconjunto L de G . Si además $L \leq G$, entonces $NL \leq G$. Por último, si $L \triangleleft G$, entonces $NL \triangleleft G$.

El siguiente resultado será mejorado más adelante.

PROPOSICIÓN 1.51. Todo subgrupo N de índice 2 de un grupo G es normal.

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

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

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

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

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

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

PROPOSICIÓN 1.52. 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 1.50, sabemos que $G_i G_j = G_j G_i$ para todo $i, j \in I$. \square

9. Una caracterización de los grupos cíclicos finitos

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

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

Por ejemplo, si p es un número primo, entonces $\phi(p^n) = p^{n-1}(p-1)$ para todo $n \in \mathbb{N}$, porque $\{0, \dots, p^n - 1\}$ 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.

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

LEMA 1.53. Cada grupo G es la unión disjunta

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

de los generadores de los subgrupos cíclicos C de G .

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

PROPOSICIÓN 1.54. La igualdad $n = \sum_{d|n} \phi(d)$ vale para cada $n \in \mathbb{N}$.

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

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

como queríamos. \square

TEOREMA 1.55. *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 1.53 y la Proposición 1.54,

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

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

TEOREMA 1.56. *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. \square

PROPOSICIÓN 1.57. *Si p es un primo impar, entonces el grupo de unidades del anillo de congruencias \mathbb{Z}_{p^r} es cíclico de orden $(p-1)p^{r-1}$, para todo $r \in \mathbb{N}$. En cambio, $\mathbb{Z}_{2^r}^\times$ es cíclico de orden 2^{r-1} si $r \leq 2$, e isomorfo a $\mathbb{Z}_{2^{r-2}} \oplus \mathbb{Z}_2$ si $r \geq 3$. Además, en este caso*

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

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

DEMOSTRACIÓN. 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

$$(6) \quad y \equiv 1 + p^i \pmod{p^{i+1}} \Rightarrow y^p \equiv 1 + p^{i+1} \pmod{p^{i+2}},$$

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

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

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 (6) se sigue que

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

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

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

y, en consecuencia, es distinto de -1 en $\mathbb{Z}_{2^r}\mathbb{Z}$. Por el Teorema 1.55, 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 $\mathbb{Z}_{2^r}^\times$. Por último, es fácil ver que $\{\pm 5^i : 0 \leq i < 2^{r-2}\}$ es isomorfo a $\mathbb{Z}_{2^{r-2}} \oplus \mathbb{Z}_2$. \square

10. Morfismos de grupos

Un *morfismo* $\varphi: G \rightarrow G'$, de un grupo G en otro G' , es por definición un morfismo de monoides de G en G' . Es fácil ver que $\varphi: G \rightarrow G'$ 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 $\text{id}_G: G \rightarrow G$, y más generalmente, la inclusión canónica $i: H \rightarrow G$ de un subgrupo H de G en G , es un morfismo de grupos. También lo es la composición $\psi \circ \varphi: G \rightarrow G''$ de dos morfismos de grupos $\varphi: G \rightarrow G'$ y $\psi: G' \rightarrow G''$.

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

EJEMPLO 1.58. *Hay monomorfismos que no son secciones y epimorfismos que no son retracciones. En efecto:*

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

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

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

Al tratar con grupos utilizaremos los símbolos $\text{Hom}(G, G')$, $\text{Iso}(G, G')$, $\text{End}(G)$ y $\text{Aut}(G)$ 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 $\text{End}(G)$ es un monoide (cuyo elemento neutro es la función identidad) vía la composición y $\text{Aut}(G)$ es su grupo de unidades.

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

EJERCICIO 1.59. Consideremos un morfismo $\varphi: G \rightarrow G'$ 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 1.60. Para cada par de grupos G y G' , el morfismo nulo $1_{GG'}: G \rightarrow G'$ 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 1.61. Para cada grupo G , la aplicación antipodal

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

es un isomorfismo de grupos.

EJEMPLO 1.62. El determinante $\det: \text{GL}(n, k) \rightarrow k^\times$ es un morfismo sobreyectivo de grupos.

EJEMPLO 1.63. 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 1.64. 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 1.65. La aplicación $\varsigma: \mathbb{C}^\times \rightarrow \mathbb{R}_{>0}$, definida por $\varsigma(x) := |x|$, es un morfismo sobreyectivo.

EJEMPLO 1.66. La aplicación $\varsigma: \mathbb{Z}[X] \rightarrow \mathbb{Q}_{>0}$, definida por

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

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

EJEMPLO 1.67. Fijemos una raíz $w \in \mathbb{C}$ de orden n de la unidad (por ejemplo, podemos tomar $w := \cos(2\pi/n) + i \sin(2\pi/n)$). La aplicación $\varphi: \mathbb{Z}_n \rightarrow G_n$, definida por $\varphi(n) = w^n$, es un isomorfismo de grupos.

EJEMPLO 1.68. Para cada $n > 1$, consideremos el subgrupo \tilde{D}_n de $GL(2, \mathbb{C})$ generado por las matrices

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

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

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

Por lo tanto a y b satisfacen las relaciones

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

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

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

donde x e y son como en el Ejemplo 1.26, es un isomorfismo.

EJEMPLO 1.69. Supongamos que X es un subconjunto de Y . Definamos

$$i_*: S_X \rightarrow S_Y$$

por

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

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

EJEMPLO 1.70. Supongamos que $i: X \rightarrow Y$ es una biyección. Definamos

$$i_*: S_X \rightarrow S_Y$$

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

EJEMPLO 1.71. Supongamos que $i: X \rightarrow Y$ es una función inyectiva. Definamos

$$i_*: S_X \rightarrow S_Y$$

por

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

Es fácil ver que:

- i_* es un morfismo inyectivo de grupos cuya imagen es el conjunto de las permutaciones de Y que dejan fijos a los elementos que están fuera de $i(X)$.
- Si X es un subconjunto de Y e i es la inclusión canónica de X en Y recuperamos la definición dada en el Ejemplo 1.69, mientras que si i es una biyección recuperamos la dada en el Ejemplo 1.70.

- Si $g: Y \rightarrow Z$ es otra función, entonces $(j \circ i)_* = j_* \circ i_*$.

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

En general $\text{Hom}(G, G')$ 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 1.72. *Si G' es abeliano, entonces $\text{Hom}(G, G')$ es un grupo abeliano vía la operación $(\varphi + \psi)(g) := \varphi(g) + \psi(g)$. El neutro de este grupo es el morfismo nulo $0_{GG'}$ y la inversa de un morfismo φ es la función $-\varphi$ definida por $(-\varphi)(g) := -\varphi(g)$.*

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

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

Ahora es evidente que

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

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

OBSERVACIÓN 1.73. *De la misma manera puede probarse que si M y M' son monoïdes y M' es abeliano, entonces $\text{Hom}(M, M')$ es un monoïde abeliano.*

OBSERVACIÓN 1.74. *Si $\varphi: H \rightarrow G$ es un morfismo de grupos y $\psi: G' \rightarrow H'$ es un morfismo de grupos abelianos, entonces las aplicaciones*

$$\varphi^*: \text{Hom}(G, G') \rightarrow \text{Hom}(H, G') \quad \text{y} \quad \psi_*: \text{Hom}(G, G') \rightarrow \text{Hom}(G, H'),$$

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

11. Núcleo e imagen

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

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

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

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

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

conmuta.

OBSERVACIÓN 1.75. Una manera equivalente de formular la propiedad universal del núcleo es decir que para todo grupo H la correspondencia

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

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

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

PROPOSICIÓN 1.76. Si $\varphi: G \rightarrow G'$ es un morfismo de grupos, entonces dos elementos g y h de G tienen la misma imagen bajo φ si y sólo si $g \ker \varphi = h \ker \varphi$.

DEMOSTRACIÓN. En efecto,

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

como afirmamos. □

COROLARIO 1.77. Un morfismo de grupos $\varphi: G \rightarrow G'$ es inyectivo si y sólo si $\ker \varphi = 1$.

EJEMPLO 1.78. El núcleo de $\det: \text{GL}(n, k) \rightarrow k^\times$ es el grupo lineal especial $\text{SL}(n, k)$.

EJEMPLO 1.79. El núcleo de la función exponencial

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

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

EJEMPLO 1.80. El núcleo del morfismo $\varsigma: \mathbb{C}^\times \rightarrow \mathbb{R}_{>0}$, definido por $\varsigma(x) = |x|$, es el círculo unidad.

12. Cociente de grupos

Consideremos una relación de equivalencia \simeq definida en el conjunto subyacente de un monoide S . Para cada $s \in S$ denotemos con $[s]$ a la clase de equivalencia de s en el conjunto cociente S/\simeq . Es fácil ver que S/\simeq tiene una estructura de monoide tal que la aplicación canónica $\pi: S \rightarrow S/\simeq$ es un morfismo si y sólo si \simeq satisface la siguiente condición:

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

Llamaremos *compatibles* a tales relaciones de equivalencia. La definición del producto en S/\simeq ,

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

esta forzada por el requerimiento de que π sea un morfismo y, por lo tanto, es única. 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 1 y que S/\simeq es conmutativo si S lo es. Por último, si 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 $\pi: S \rightarrow S/\simeq$ es un morfismo de grupos.

Se pueden decir muchas cosas más acerca de los cocientes de monoides por relaciones de equivalencia compatibles, pero casi todas son de carácter 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 $N \triangleleft G$, y es trivial que

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

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

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

Recíprocamente, si N es un subgrupo normal de G , entonces por la Proposición 1.45 las relaciones de equivalencia

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

coinciden y son compatibles con la operación de G , porque

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

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

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

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow \pi & \nearrow \bar{\varphi} & \\ G/N & & \end{array}$$

conmuta.

Para comprobarlo, notemos que

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

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

$$\begin{array}{ccc} \text{Hom}(G/N, G') & \longrightarrow & \text{Hom}(G, G') \\ \bar{\varphi} & \longmapsto & \bar{\varphi} \circ \pi \end{array}$$

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

OBSERVACIÓN 1.82. *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 1.83 (Primer teorema de isomorfismo). *Todo morfismo de grupos $\varphi: G \rightarrow G'$ induce un isomorfismo $\bar{\varphi}: G/\ker \varphi \rightarrow \text{Im } \varphi$.*

DEMOSTRACIÓN. Es claro. □

TEOREMA 1.84 (Segundo teorema de isomorfismo). *Si $L \subseteq N$ son subgrupos normales de un grupo G , entonces $N/L \triangleleft G/L$ y $G/N \simeq (G/L)/(N/L)$.*

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

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

donde $\pi_L: G \rightarrow G/L$ y $\pi_N: G \rightarrow G/N$ son los morfismos canónicos, conmuta. Es fácil ver que $\tilde{\pi}$ es sobreyectivo y que $\ker \tilde{\pi} = N/L$. En consecuencia, por el teorema anterior, $\tilde{\pi}$ induce un isomorfismo $\bar{\pi}: (G/L)/(N/L) \rightarrow G/N$. □

TEOREMA 1.85 (Tercer teorema de isomorfismo). *Si L y N son dos subgrupos de un grupo G y N es normal en G , entonces $L \cap N \triangleleft L$ y $L/L \cap N \simeq NL/N$.*

DEMOSTRACIÓN. Consideremos el morfismo $\tilde{\iota}: L \rightarrow G/N$ obtenido componiendo la inclusión canónica $\iota: L \rightarrow G$ con la sobreyección canónica $\pi_N: G \rightarrow G/N$. Por la propiedad

universal del cociente sabemos que hay un único monomorfismo $\bar{\iota}: L/\ker \tilde{\iota} \rightarrow G/N$ tal que el triángulo

$$\begin{array}{ccc} L & \xrightarrow{\tilde{\iota}} & G/N \\ \downarrow \pi_L & \nearrow \bar{\iota} & \\ L/\ker \tilde{\iota} & & \end{array}$$

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

TEOREMA 1.86. Si $\varphi: G \rightarrow G'$ es un morfismo de grupos, entonces

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

DEMOSTRACIÓN. Por el teorema de Lagrange, $|G| = |G : \ker \varphi| |\ker \varphi|$, y por el primer teorema de isomorfismo, $|G : \ker \varphi| = |\text{Im } \varphi|$. \square

OBSERVACIÓN 1.87. Consideremos un morfismo de grupos $\varphi: G \rightarrow G'$. Por el teorema de Lagrange, sabemos que $|\text{Im } \varphi|$ divide a $|G'|$, y por el Teorema 1.86, que divide a $|G|$. Por lo tanto, si G y G' son finitos $|\text{Im } \varphi|$ divide a $(|G| : |G'|)$. En particular, si $|G|$ y $|G'|$ son coprimos, entonces φ es el morfismo nulo.

EJEMPLO 1.88. Supongamos que k es un cuerpo finito. Si G es un subgrupo de $\text{GL}(n, k)$, cuyo orden es coprimo con $|k| - 1$, entonces $G \leq \text{SL}(n, k)$, porque la aplicación $\det: G \rightarrow k^\times$ es el morfismo nulo. En particular, todos los subgrupos de orden impar de $\text{GL}(n, \mathbb{Z}_3)$ están incluidos en $\text{SL}(n, \mathbb{Z}_3)$.

Recordemos que un *orden parcial* en un conjunto X es una relación binaria \leq en X , que es reflexiva antisimétrica y transitiva. Un *conjunto parcialmente ordenado* es un conjunto X provisto de un orden parcial. El *supremo* de 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 $x \leq z$.

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 elementos de X tiene supremo e ínfimo. Por ejemplo, el conjunto $\text{Sub}_H(G)$, 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 $\text{Sub}(G)$ en lugar de $\text{Sub}_1(G)$.

PROPOSICIÓN 1.89. 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 $1) \Rightarrow 2)$ y $1) \Rightarrow 3)$. Veamos que $2) \Rightarrow 1)$. 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 $3) \Rightarrow 1)$. \square

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

- $x_1 \leq x_2 \Rightarrow f(x_1) \leq f(x_2)$ para todo $x_1, x_2 \in X$,
- $f(\bigvee_{i \in I} x_i) = \bigvee_{i \in I} f(x_i)$ 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, no es difícil probar que cualquiera de las dos últimas implica la primera. Un morfismo de reticulados completos $f: X \rightarrow X'$ es un *isomorfismo* si hay un morfismo $f^{-1}: X' \rightarrow X$, llamado la *inversa* de f , tal que $f^{-1} \circ f = \text{id}_X$ y $f \circ f^{-1} = \text{id}_{X'}$. Es fácil ver que esto sucede si y sólo si f es biyectiva y tanto f como f^{-1} preservan el orden.

TEOREMA 1.90 (Teorema de la correspondencia). *Si $\varphi: G \rightarrow G'$ es un morfismo sobreyectivo de grupos, entonces las funciones*

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

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

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

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

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

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

para todo subconjunto H' de G' . Además,

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

para cada $H \leq G$, porque

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

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

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

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

Además, los resultados obtenidos al comienzo de la Sección 11 muestran en particular que $H \triangleleft L$ si y sólo si $\varphi(H) \triangleleft \varphi(L)$. Resta ver que

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

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

OBSERVACIÓN 1.91. *Por el teorema anterior si $\varphi: G \rightarrow G'$ es un morfismo sobreyectivo de grupos y H es un subgrupo de G , entonces $|G' : \varphi(H)| = |G : H \ker \varphi|$ y, por lo tanto, divide a $|G : H|$.*

DEFINICIÓN 1.92. *Un grupo G es simple si $G \neq 1$ y $H \triangleleft G \Rightarrow H = 1$ o $H = G$.*

DEFINICIÓN 1.93. *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 1.94. *$H \triangleleft G$ es maximal si y sólo si G/H es simple.*

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

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

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

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

PROPOSICIÓN 1.95. *La construcción anterior tiene las siguientes propiedades:*

1. *Para todo $H \triangleleft G$, el morfismo $\overline{\text{id}}: G/H \rightarrow G/H$ es la identidad de G/H .*
2. *Consideremos morfismos de grupos $\varphi: G \rightarrow G'$ y $\psi: G' \rightarrow G''$ 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 $\overline{\psi \circ \varphi} = \overline{\psi} \circ \bar{\varphi}$.*

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

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

y el rectángulo exterior del diagrama

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

conmutan. □

EJERCICIO 1.96. Pruebe que si $\varphi: G \rightarrow G'$ es un morfismo de grupos y $H' \triangleleft G'$, entonces $\varphi^{-1}(H') \triangleleft G$ y existe un único morfismo inyectivo $\bar{\varphi}: G/\varphi^{-1}(H') \rightarrow G'/H'$ de grupos, tal que el diagrama

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

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

13. Grupos libres y presentaciones

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

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

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

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

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

13.1. Grupos libres

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

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

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

$$(7) \quad x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n} x_{\beta_1}^{\delta_1} \cdots x_{\beta_m}^{\delta_m}.$$

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 (7) sucesivamente pares de símbolos asociados, hasta obtener una que lo sea.

TEOREMA 1.97. *El conjunto $L(X)$, de las 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 de w_1 y el primero de w_3 sean el elemento de $X^{\pm 1}$ asociado a x^ϵ . Es fácil ver que en todos vale que $w_1(w_2w_3) = (w_1w_2)w_3$. Supongamos ahora que la asociatividad vale cuando $l(w_2) \leq n$ y que $l(w_2) = n + 1$. Escribamos $w_2 = w'_2x^\epsilon$. Entonces, por hipótesis inductiva

$$\begin{aligned} w_1(w_2w_3) &= w_1((w'_2x^\epsilon)w_3) \\ &= w_1(w'_2(x^\epsilon w_3)) \\ &= (w_1w'_2)(x^\epsilon w_3) \\ &= ((w_1w'_2)x^\epsilon)w_3 \\ &= (w_1(w'_2x^\epsilon))w_3 \\ &= (w_1w_2)w_3. \end{aligned}$$

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 $x_{\alpha_n}^{-\epsilon_n} \cdots x_{\alpha_1}^{-\epsilon_1}$. \square

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

TEOREMA 1.98. Para cada función $j: X \rightarrow G$, de X en un grupo G , hay un único morfismo $\varphi: L(X) \rightarrow G$ que extiende a j . Vale decir, con la propiedad de que el triángulo

$$\begin{array}{ccc} X & \xrightarrow{j} & G \\ \downarrow \iota & \nearrow \varphi & \\ L(X) & & \end{array}$$

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. \square

Ampliando un poco la definición dada arriba del Teorema 1.98, diremos que un *grupo libre sobre X* es cualquier par (G, j) , formado por un grupo G y una función $j: X \rightarrow G$, que tiene la misma propiedad universal que $(L(X), \iota)$. Por extensión, en este caso decimos también que G es libre.

OBSERVACIÓN 1.99. Si $l: Y \rightarrow X$ es una función biyectiva, (G, j) es un grupo libre sobre X y $\psi: G \rightarrow H$ es un isomorfismo de grupos, entonces $(H, \psi \circ j \circ l)$ es un grupo libre sobre Y .

PROPOSICIÓN 1.100. Un par (G, j) , formado por un grupo G y una función $j: X \rightarrow G$, es un grupo libre si y sólo si el morfismo $\varphi: L(X) \rightarrow G$ cuya existencia y unicidad fue probada en el Teorema 1.98 es un isomorfismo. En consecuencia, j es inyectivo.

DEMOSTRACIÓN. Por la Observación 1.99, si φ es un isomorfismo, entonces (G, j) tiene la propiedad universal de $(L(X), \iota)$. Supongamos ahora que (G, j) tiene esta propiedad. Entonces hay un único morfismo $\psi: G \rightarrow L(X)$ tal que el triángulo

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

conmuta y, como

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

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

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

lo que prueba que φ es un isomorfismo. \square

Una *base* de un grupo G es cualquier subconjunto X de G tal que el par (G, ι_X) , donde $\iota_X: X \rightarrow G$ es la inclusión canónica, es un grupo libre. Obviamente esto ocurre si y sólo si el morfismo de $L(X)$ en G , inducido por ι_X , es biyectivo. Es claro que un grupo tiene una base si y sólo si es libre. Por la Observación 1.99, si (G, j) es libre, entonces $\text{Im } j$ es una base de G . El siguiente teorema será probado más adelante.

TEOREMA 1.101. Dos grupos libres $L(X)$ y $L(Y)$ son isomorfos si y sólo si $|X| = |Y|$. Equivalentemente, todas las bases de un grupo libre G tienen el mismo cardinal.

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

PROPOSICIÓN 1.102. *Todo grupo es isomorfo a un cociente de un grupo libre.*

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

$$\varphi: L(X) \rightarrow G$$

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

13.2. Presentaciones

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

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

de $L(X)$, que se convierten en 1 al pasar al cociente. Decimos que un subconjunto R de N es un *conjunto de relaciones para G* y que (X, R) es una *presentación* de G , si N es el subgrupo normal de G generado por R . Además, en este caso escribimos $G = \langle X|R \rangle$. Por la Proposición 1.102, 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 para cada grupo cociente G/N un de un grupo G y cada elemento $g \in G$, el símbolo $[g]$ denota a la clase de g en G/N .

EJEMPLO 1.103. $\langle x | \emptyset \rangle \simeq \mathbb{Z}$.

EJEMPLO 1.104. *Por las propiedades universales del grupo libre y del cociente, hay un único morfismo*

$$p: \langle x | x^n \rangle \rightarrow \mathbb{Z}_n,$$

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

EJEMPLO 1.105. *Por la propiedades universales del grupo libre y del cociente, hay un único morfismo*

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

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

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

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

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

En consecuencia,

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

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

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

EJEMPLO 1.106. Recordemos que el grupo diedral D_n es el subgrupo de $\text{GL}(2, \mathbb{R})$ generado por las matrices

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

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

$$p: \langle x_1, x_2 | x_1^n, x_2^2, x_2 x_1 x_2^{-1} x_1 \rangle \rightarrow D_n,$$

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

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

y, en consecuencia,

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

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

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

EJEMPLO 1.107. Recordemos que el grupo cuaterniónico generalizado H_n es el subgrupo de $\text{GL}(2, \mathbb{C})$ generado por las matrices

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

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

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

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

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

En consecuencia,

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

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

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

OBSERVACIÓN 1.108. En los últimos dos ejemplos solamente se usaron las relaciones que satisfacían x e y , nunca que eran matrices. De hecho, los argumentos dados prueban que todo grupo de orden $2n$ generado por un conjunto $\{x, y\}$ de dos elementos que satisfacen $x^n = 1$, $y^2 = 1$ e $yxy^{-1} = x^{-1}$ es isomorfo a $\langle x_1, x_2 | x_1^n, x_2^2, x_2 x_1 x_2^{-1} x_1 \rangle$, y todo grupo de orden $4n$ generado por un conjunto de dos $\{x, y\}$ elementos que satisfacen $x^n = y^2 = 1$ e $yxy^{-1} = x^{-1}$ es isomorfo a $\langle x_1, x_2 | x_1^n x_2^{-2}, x_2 x_1 x_2^{-1} x_1 \rangle$.

EJEMPLO 1.109. Es trivial que para todo divisor $r > 1$ de n , el cociente $D_n/\langle x^r \rangle$ está generado por los elementos $[x]$ e $[y]$ sujetos a las relaciones $[x]^r = [y]^2 = [y][x][y]^{-1}[x] = 1$, y que su orden es $2r$. Por lo tanto $D_n/\langle x^r \rangle$ es isomorfo a D_r .

EJEMPLO 1.110. Razonando como en el ejemplo anterior se comprueba fácilmente que, para todo divisor $r > 1$ de n , el cociente $H_n/\langle x^r \rangle$ es isomorfo a H_r .

OBSERVACIÓN 1.111 (Descripción de conjuntos de homomorfismos). Por la propiedad universal de los grupos libres, para cada grupo G y cada conjunto X , la aplicación

$$\theta: \text{Hom}(L(X), G) \rightarrow G^X,$$

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

$$\theta: \text{Hom}(\langle x \rangle, G) \rightarrow G$$

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

$$\bar{\theta}: \text{Hom}(L(X)/\langle R \rangle, G) \rightarrow G^X,$$

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

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

Similarmente,

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

y

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

EJEMPLO 1.112. Consideremos $n, m \in \mathbb{N}$ mayores que 1 tales que n es un múltiplo impar de m y escribamos $H_n = \langle x, y \rangle$ y $H_m = \langle \bar{x}, \bar{y} \rangle$ donde x, y, \bar{x} y \bar{y} satisfacen

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

Como n/m es impar,

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

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

EJEMPLO 1.113. Consideremos un grupo cíclico $C_n := \langle x \rangle$ de orden n . Por la Observación 1.111, para cada $i \geq 0$ hay un morfismo

$$v_i: C_n \rightarrow C_n$$

tal que $v_i(x) := x^i$. Como $v_i(x^j) = x^{ji} = 1$ si y sólo si ji es múltiplo de n , el núcleo de v_i es $\langle x^{n/(n:i)} \rangle$, donde, como en el Ejemplo 1.26, el símbolo $(n : i)$ denota al máximo divisor común de n e i . En particular v_i es un automorfismo si y sólo si i es coprimo con n . Por lo tanto la aplicación

$$\phi: \text{Aut}(C_n) \rightarrow U(\mathbb{Z}_n)$$

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

EJEMPLO 1.114. Recordemos que el grupo diedral D_n está generado por dos elementos x e y sujetos a las relaciones $x^n = 1$, $y^2 = 1$ e $xyx^{-1} = y$, y que

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

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

$$\phi: \text{Aut}(D_n) \rightarrow \mathbb{Z}_n \times U(\mathbb{Z}_n),$$

tal que $\phi(f) := (j, i)$ si $f(y) = x^j y$ y $f(x) = x^i$. Se sigue fácilmente de la Observación 1.111 que ϕ también es sobreyectiva. Supongamos ahora que g es otro automorfismo del grupo D_n y que $g(x) = x^{i'}$ y $g(y) = x^{j'} y$. Como

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

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

EJEMPLO 1.115. Recordemos ahora que H_n es un grupo generado por dos elementos x, y sujetos a las relaciones $x^n y^{-2} = 1$ e $xyx^{-1} = 1$ y que

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

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

$$\phi: \text{Aut}(H_n) \rightarrow \mathbb{Z}_{2n} \times U(\mathbb{Z}_{2n}),$$

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

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

TEOREMA 1.116. Si G es un grupo finito, $x, y \in G$ tienen orden 2 e $y \notin \{x, x^{-1}\}$, entonces $\langle x, y \rangle \simeq D_n$, donde n es el orden de yx .

DEMOSTRACIÓN. Escribamos $s = yx$. Como

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

se sigue de la Observación 1.108, que para probar el teorema es suficiente ver que $|\langle x, y \rangle| = 2n$. Ahora bien, debido a las relaciones que aparecen arriba

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

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

14. 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 recuperarse a partir de varios de sus subgrupos. Luego introducimos las nociones de producto directo y producto directo restringido, y estudiamos algunas de sus propiedades y como se relacionan estas construcciones con el producto directo interno.

14.1. Producto directo interno

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

$$g = g_1 \cdots g_n$$

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

$$(8) \quad (g_1 \cdots g_n)(g'_1 \cdots g'_n) = g_1 g'_1 \cdots g_n g'_n$$

para todo $g_1, g'_1 \in G_1, \dots, g_n, g'_n \in G_n$. Es claro que si $G_1 \cdots G_n$ es producto directo interno de G_1, \dots, G_n entonces $G_1 \cdots G_n$ es un subgrupo de G y que $g_i g_j = g_j g_i$ para cada $g_i \in G_i$ y $g_j \in G_j$, con $i \neq j$. En consecuencia $G_1 \cdots G_n$ es producto directo interno de $G_{\sigma_1}, \dots, G_{\sigma_n}$ para todo $\sigma \in S_n$ y $G_i \triangleleft G_1 \cdots G_n$ para todo i . Notemos también que las inclusiones canónicas $\iota_i: G_i \rightarrow G_1 \cdots G_n$ y las aplicaciones $\pi_i: G_1 \cdots G_n \rightarrow G_i$, 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 1.117. *Consideremos subgrupos normales G_1, \dots, G_n de un grupo G . Por brevedad, denotemos con $G_{\widehat{i}}$ a $G_1 \cdots \widehat{G_i} \cdots G_n$. Son equivalentes:*

1. $G_1 \cdots G_n$ es producto directo interno de G_1, \dots, G_n .
2. $\bigcap_{i=1}^n G_{\widehat{i}} = 1$.
3. $G_i \cap G_{\widehat{i}} = 1$ para todo i .
4. $G_i \cap (G_1 \cdots G_{i-1}) = 1$ 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) Es trivial.

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

3) \Rightarrow 4) Es trivial.

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

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

Pero entonces

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

para todo $g_1, h_1 \in G_1, \dots, g_n, h_n \in G_n$, y además la multiplicación de G está dado por la fórmula (8). □

EJEMPLO 1.118. Consideremos $n \in \mathbb{N}$ impar y mayor que 1 y $D_{2n} = \langle x, y \rangle$ donde x e y satisfacen $x^{2n} = y^2 = 1$ e $xyx^{-1} = x^{-1}$. Como $\langle x^2, y \rangle \cap \langle x^n \rangle = 1$ y $\langle x^2, y \rangle$ y $\langle x^n \rangle$ son subgrupos normales de D_{2n} , se sigue del teorema anterior que D_{2n} es el producto directo interno de $\langle x^2, y \rangle$ y $\langle x^n \rangle$. Notemos que $\langle x^2, y \rangle \simeq D_n$ y $\langle x^n \rangle \simeq \mathbb{Z}_2$.

14.2. Producto directo

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

El producto directo tiene la siguiente propiedad universal:

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

$$\begin{array}{ccc} G & & \\ \downarrow \mathbf{f} & \searrow f_j & \\ \prod G_i & \xrightarrow{\pi_j} & G_j \end{array}$$

conmuta.

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

$$\begin{array}{ccc} \text{Hom}(G, \prod G_i) & \xrightarrow{\Psi} & \prod \text{Hom}(G, G_i) \\ f \longmapsto & & (\pi_i \circ f)_{i \in I} \end{array}$$

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

OBSERVACIÓN 1.119. Consideremos subgrupos normales G_1, \dots, G_n de un grupo G . Como en el Teorema 1.117, escribamos $G_{\widehat{i}} := G_1 \cdots \widehat{G_i} \cdots G_n$. Por la propiedad universal del producto, las proyecciones canónicas $\pi_{\widehat{i}}: G \rightarrow G/G_{\widehat{i}}$ inducen un morfismo

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

cuyo núcleo es $\bigcap_{i=1}^n G_{\widehat{i}}$. Afirmamos que π es sobreyectivo si y sólo si $G_1 \cdots G_n = G$. En efecto, si se satisface esta condición, entonces para cada $([g_1], \dots, [g_n]) \in G/G_{\widehat{1}} \times \cdots \times G/G_{\widehat{n}}$,

existen $g_{ij} \in G_i$ para $1 \leq i, j \leq n$, tales que $g_j = g_{1j} \cdots g_{nj}$ para todo j . En consecuencia

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

Recíprocamente, si π es sobreyectivo, entonces para cada $g \in G$ hay un $x \in G$ tal que

$$\pi(x) = ([g], 1, \dots, 1).$$

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

$$g_2 \in G_2, \dots, g_n \in G_n \quad \text{y} \quad g'_1 \in G_1, g'_3 \in G_3, \dots, g'_n \in G_n$$

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 1.50.

COROLARIO 1.120. El morfismo π es biyectivo si y sólo si G es producto directo interno de G_1, \dots, G_n .

DEMOSTRACIÓN. Por el Teorema 1.117 y de la Observación 1.119. □

PROPOSICIÓN 1.121. Para cada familia $(f_i: H_i \rightarrow G_i)_{i \in I}$ de morfismos de grupos, existe un único morfismo

$$\prod f_i: \prod H_i \rightarrow \prod G_i$$

tal que los diagramas

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

conmutan.

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

Es fácil ver que

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

OBSERVACIÓN 1.122. La correspondencia introducida en la Proposición 1.121 tiene las siguientes propiedades:

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

$$\left(\prod g_i\right) \circ \left(\prod f_i\right) = \prod (g_i \circ f_i).$$

OBSERVACIÓN 1.123. Si $H_i \triangleleft G_i$ para todo $i \in I$, entonces la familia de los epimorfismos canónicos $\pi_i: G_i \rightarrow G_i/H_i$, induce un morfismo sobreyectivo

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

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

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

14.3. 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:

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

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* $\iota_j: G_j \rightarrow \bigsqcup G_i$, definidas por

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

Es evidente que

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

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

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

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

existe un único morfismo de grupos $\varphi: \bigsqcup G_i \rightarrow G$ tal que para cada $j \in I$ el diagrama

$$\begin{array}{ccc} & & G \\ & \nearrow \varphi_j & \uparrow \varphi \\ G_j & \xrightarrow{\iota_j} & \bigsqcup G_i \end{array}$$

conmuta.

En efecto, si φ existe, entonces forzosamente

$$\varphi(g) = \varphi\left(\prod \iota_j(\pi_j(g))\right) = \prod \varphi_j(\pi_j(g)),$$

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

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

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

$$\varphi \circ \iota_j(g) = \prod \varphi_i(\pi_i(\iota_j(g))) = \varphi_j(g)$$

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

$$\Psi: \text{Hom}\left(\bigsqcup G_i, G\right) \rightarrow \prod \text{Hom}(G_i, G),$$

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

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

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

PROPOSICIÓN 1.124. *Para cada familia $(\varphi_i: H_i \rightarrow G_i)_{i \in I}$ de morfismos de grupos existe un único morfismo*

$$\bigsqcup \varphi_i: \bigsqcup H_i \rightarrow \bigsqcup G_i$$

tal que los diagramas

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

conmutan.

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

Es obvio que

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

OBSERVACIÓN 1.125. *La correspondencia introducida en la Proposición 1.124 tiene las siguientes propiedades:*

1. $\bigsqcup \text{id}_{H_i} = \text{id}_{\bigsqcup H_i}$.
2. *Para cada par de familias de morfismos de grupos $(\varphi_i: H_i \rightarrow L_i)_{i \in I}$ y $(\psi_i: L_i \rightarrow G_i)_{i \in I}$,*

$$\left(\bigsqcup \psi_i\right) \circ \left(\bigsqcup \varphi_i\right) = \bigsqcup (\psi_i \circ \varphi_i).$$

OBSERVACIÓN 1.126. Si $H_i \triangleleft G_i$ para todo $i \in I$, entonces la familia de los epimorfismos canónicos $\pi_i: G_i \rightarrow G_i/H_i$, induce un morfismo sobreyectivo

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

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

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

EJERCICIO 1.127. 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 1.128. Supongamos que G_1, \dots, G_n son subgrupos de un grupo G . Es fácil ver que la función

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

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

- $\ker \varsigma = \{(g_1, \dots, g_n) \in G_1 \times \cdots \times G_n : g_1 \cdots g_n = 1\}$,
- $\text{Im } \varsigma = G_1 \cdots G_n$,
- si ς es biyectivo, entonces la composición $\pi \circ \varsigma$, del isomorfismo π introducido en la Observación 1.119, con ς , identifica al subgrupo $\iota_i(G_i)$ de $G_1 \times \cdots \times G_n$ con el subgrupo $\iota_i(G/G_{\widehat{i}})$ de $(G/G_{\widehat{1}}) \times \cdots \times (G/G_{\widehat{n}})$.

PROPOSICIÓN 1.129. Si G_1, \dots, G_n son subgrupos de G , entonces son equivalentes:

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

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

COROLARIO 1.130. Supongamos que G_1, \dots, G_n son subgrupos normales finitos de un grupo G y que los elementos de G_i conmutan con los de G_j para todo $i \neq j$. Si $|G_i|$ es coprimo con $|G_j|$ siempre que $i \neq j$, entonces la aplicación

$$\varsigma: G_1 \times \cdots \times G_n \rightarrow G,$$

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 1.42 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 el Teorema 1.117 y la Proposición 1.129, esto implica que ς es un morfismo inyectivo de grupos. Ahora es obvio que es sobreyectivo si y sólo si $|G| = |G_1| \cdots |G_n|$. \square

Recordemos que la función $\phi: \mathbb{N} \rightarrow \mathbb{N}$ de Euler introducida al comienzo de la Sección 9 asigna a cada número natural el cardinal del conjunto de los enteros no negativos menores que el y coprimos con el.

COROLARIO 1.131. 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 1.130, 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. \square

EJERCICIO 1.132. Supongamos que H y L son dos subgrupos normales distintos de un grupo G . Pruebe que si H es simple y tiene índice 2 en G y L no es trivial, entonces $|L| = 2$ y $G \simeq H \times L$.

NOTA 1.133. Si $(G_i)_{i \in I}$ es una familia de subgrupos de un grupo G y los elementos de G_i conmutan con los de G_j para todo $i \neq j$, entonces por la propiedad universal del producto restringido hay un único morfismo

$$\theta: \bigsqcup_{i \in I} G_i \rightarrow G$$

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

14.4. 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 $M_{s \times r}(\text{Hom}(\mathbf{H}, \mathbf{K}))$ 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 $\varsigma_{ij} \in \text{Hom}(H_j, K_i)$, tales que

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

Si $\mathbf{H} = \mathbf{K}$ escribiremos $M_r(\text{End}(\mathbf{H}))$ en lugar de $M_{s \times r}(\text{Hom}(\mathbf{H}, \mathbf{K}))$.

PROPOSICIÓN 1.134. *La aplicación*

$$\theta: M_{s \times r}(\text{Hom}(\mathbf{H}, \mathbf{K})) \rightarrow \text{Hom}(H_1 \times \cdots \times H_r, K_1 \times \cdots \times K_s),$$

definida por

$$\theta(\varsigma_{ij})(h_1, \dots, h_r) = \left(\prod_j \varsigma_{1j}(h_j), \dots, \prod_j \varsigma_{sj}(h_j) \right),$$

es biyectiva.

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

$$\iota_j: H_j \rightarrow H_1 \times \cdots \times H_r \quad \text{y} \quad \pi_i: K_1 \times \cdots \times K_s \rightarrow K_i$$

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

$$(9) \quad \begin{pmatrix} \varsigma_{11} & \cdots & \varsigma_{1r} \\ \vdots & \ddots & \vdots \\ \varsigma_{s1} & \cdots & \varsigma_{sr} \end{pmatrix} \begin{pmatrix} h_1 \\ \vdots \\ h_r \end{pmatrix} := \begin{pmatrix} \varsigma_{11}(h_1) \cdots \varsigma_{1r}(h_r) \\ \vdots \\ \varsigma_{s1}(h_1) \cdots \varsigma_{sr}(h_r) \end{pmatrix}.$$

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

Cuando los K_i son grupos abelianos, entonces cada uno de los Hom que aparecen en la proposición anterior también lo son, via la suma de morfismos introducida en la Proposición 1.72 y, en este caso, θ es un isomorfismo de grupos abelianos si consideramos a $M_{s \times r}(\text{Hom}(\mathbf{H}, \mathbf{K}))$ como un grupo via la suma usual de matrices.

Consideremos ahora otra matriz

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

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

$$\psi_{ij}: H_j \rightarrow L_i \quad \text{para } 1 \leq i \leq t \text{ y } 1 \leq j \leq r,$$

por

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

Afirmamos que

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

y que

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

En efecto lo primero se sigue facilmente de que

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

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

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

mientras que lo segundo sale por cálculo directo.

Es natural ahora escribir

$$(10) \quad \begin{pmatrix} \psi_{11} & \cdots & \psi_{1r} \\ \vdots & \ddots & \vdots \\ \psi_{t1} & \cdots & \psi_{tr} \end{pmatrix} := \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1s} \\ \vdots & \ddots & \vdots \\ \varphi_{t1} & \cdots & \varphi_{ts} \end{pmatrix} \begin{pmatrix} \varsigma_{11} & \cdots & \varsigma_{1r} \\ \vdots & \ddots & \vdots \\ \varsigma_{s1} & \cdots & \varsigma_{sr} \end{pmatrix}.$$

Si los L_j son grupos abelianos y denotamos aditivamente tanto la operación de cada uno de ellos como la de los grupos $\text{Hom}(K_k, L_j)$ y $\text{Hom}(H_i, L_j)$, entonces el producto de matrices (10) toma el aspecto habitual.

15. Producto semidirecto

Por el Teorema 1.117 de la Sección 14 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 construcción, y motivados por el entendimiento de su estructura, introduciremos la noción de producto semidirecto, y estudiaremos algunas de sus propiedades y las relaciones con la versión interna.

15.1. Producto semidirecto interno

Consideremos dos subgrupos N y H de un grupo G . Decimos que G es *producto semidirecto interno* de N con H si $N \triangleleft G$ 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, $hn'h^{-1} \in N$ para cada $n' \in N$ y $h \in H$, por lo que la fórmula

$$(11) \quad (nh)(n'h') = nhn'h^{-1}hh'$$

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

TEOREMA 1.135. *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. 1) \Rightarrow 2) Es trivial.

2) \Rightarrow 3) Si $1 = nh$ con $n \in N$ y $h \in H$, entonces $h^{-1} = n \in N \cap H$ y, por lo tanto, $n = h = 1$.

3) \Rightarrow 1) Si $nh = n'h'$, entonces $n^{-1}n'h'h^{-1} = 1$ y, por consiguiente, $n^{-1}n' = h'h^{-1} = 1$. \square

EJERCICIO 1.136. Supongamos que N y L son subgrupos de un grupo G con L no contenido en N . Pruebe que si N tiene índice 2 en G y L es simple, entonces $|L| = 2$ y G es el producto semidirecto interno de N y L .

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

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

es un automorfismo. Además la función $\zeta: H \rightarrow \text{Aut}(N)$, obtenida de este modo, es un morfismo y, con estas notaciones, la fórmula (11) se escribe

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

Esto justifica la construcción que sigue.

15.2. Producto semidirecto

Consideremos un morfismo de grupos

$$\zeta: H \rightarrow \text{Aut}(N)$$

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

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

y que lo sea ζ se traduce en que

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

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

PROPOSICIÓN 1.137. El producto cartesiano $N \times H$, dotado de la multiplicación

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

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

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

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

y

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

coinciden. Pero esto es cierto, porque

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

Por la Proposición 1.12, para terminar la demostración es suficiente ver que $(1, 1)$ es neutro a izquierda de $N \times_{\zeta} H$ 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. \square

Fijados grupos N , H y un morfismo $\zeta: H \rightarrow \text{Aut}(N)$, llamamos *producto semidirecto de N y H asociado a ζ* , y designamos con $N \times_{\zeta} H$, al grupo construido en la proposición anterior.

PROPOSICIÓN 1.138. *El producto semidirecto tiene las siguientes propiedades:*

1. *Las funciones*

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

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

2. *$N \times 1$ es un subgrupo normal de $N \times_{\zeta} H$ y la función*

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

es un isomorfismo.

3. *$1 \times H$ es un subgrupo de $N \times_{\zeta} H$*

4. *$(1, h)(n, 1) = (h \cdot n, 1)(1, h)$ para todo $h \in H$ y $n \in N$.*

5. *$(n, 1)(1, h) = (n, h)$ para todo $h \in H$ y $n \in N$.*

6. *$(N \times 1) \cap (1 \times H) = 1$ y $(N \times 1)(1 \times H) = N \times_{\zeta} H$.*

DEMOSTRACIÓN. Es indiscutible que π y s son morfismos, $\pi \circ s = \text{id}_H$, $\ker \pi = N \times 1$ y $(N \times 1) \cap (1 \times H) = 1$. En consecuencia $N \times 1 \triangleleft N \times_{\zeta} H$ y $1 \times H \leq N \times_{\zeta} H$. Como

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

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

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

lo que muestra en particular que $(N \times 1)(1 \times H) = N \times_{\zeta} H$. \square

COROLARIO 1.139. *$N \times_{\zeta} H$ es producto semidirecto interno de $N \times 1$ con $1 \times H$.*

DEMOSTRACIÓN. Por los items 2), 3) y 6) del teorema anterior y por el Teorema 1.135. \square

PROPOSICIÓN 1.140. *Si un grupo G es producto semidirecto interno de un subgrupo normal N con un subgrupo H , entonces la función*

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

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

DEMOSTRACIÓN. Como evidentemente θ es biyectiva, sólo hay que observar que, debido a que

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

también es un morfismo. \square

OBSERVACIÓN 1.141. Si $s: H \rightarrow N \times_{\zeta} H$ es una sección conjuntista del epimorfismo canónico $\pi: N \times_{\zeta} H \rightarrow H$, entonces existe una aplicación $\varpi: H \rightarrow N$ tal que

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

Dado que

$$(\varpi(h), h)(\varpi(h'), h') = (\varpi(h)(h \cdot_{\zeta} \varpi(h')), hh') \quad \text{para todo } h, h' \in H,$$

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

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

EJEMPLO 1.142. Fijado un grupo abeliano G consideremos el morfismo

$$\zeta: C_2 \rightarrow \text{Aut}(G),$$

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

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

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

EJEMPLO 1.143. Consideremos dos grupos cíclicos $C_n := \langle x \rangle$ y $C_m := \langle y \rangle$ de orden n y m , respectivamente. Como vimos en el Ejemplo 1.113 para cada $0 \leq i < n$ hay un morfismo

$$v_i: C_n \rightarrow C_n$$

que es un automorfismo si y sólo si i es coprimo con n y que aplica x en x^i . Notemos que $v_i^m(x) = x^{i^m}$, de manera que $v_i^m = \text{id}$ si y sólo si $i^m \equiv 1 \pmod{n}$, y que además esto implica que i y n son coprimos. En consecuencia, nuevamente por la Observación 1.111, existe un morfismo

$$\zeta: C_m \rightarrow \text{Aut}(C_n)$$

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

EJEMPLO 1.144. Fijemos $m \in \mathbb{N}$ y consideremos el grupo cuaterniónico generalizado H_{2^m} de orden 2^{m+2} . Afirmamos que H_{2^m} no es producto semidirecto de dos subgrupos propios. En efecto, por el teorema de Lagrange todos los subgrupos no nulos de H_{2^m} tienen orden par. En consecuencia, por la Observación 1.34 todos tienen elementos de orden 2. Pero como vimos en el Ejemplo 1.27, 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 1.145. Consideremos productos semidirectos $N_1 \times_{\varsigma_1} H_1$ y $N_2 \times_{\varsigma_2} H_2$ y morfismos $\gamma: H_1 \rightarrow H_2$ y $\xi: N_1 \rightarrow N_2$. Son equivalentes:

1. La función

$$\chi: N_1 \times_{\varsigma_1} H_1 \rightarrow N_2 \times_{\varsigma_2} H_2,$$

definida por $\chi(n, h) := (\xi(n), \gamma(h))$, es un morfismo de grupos.

2. $\xi(h \cdot_{\varsigma_1} n) = \gamma(h) \cdot_{\varsigma_2} \xi(n)$ para todo $h \in H_1$ y $n' \in N_1$.

3. El diagrama

$$\begin{array}{ccc} H_1 & \xrightarrow{\varsigma_1} & \text{Aut}(N_1) \\ \downarrow \gamma & & \searrow \xi_* \\ & & \text{Hom}(N_1, N_2) \\ & & \nearrow \xi_* \\ H_2 & \xrightarrow{\varsigma_2} & \text{Aut}(N_2) \end{array} ,$$

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

Además, en este caso χ es biyectivo si y sólo si ξ y γ lo son.

DEMOSTRACIÓN. La equivalencia entre los items (1) y (2) se sigue de que

$$\chi((n, h)(n', h')) = \chi(n(h \cdot_{\varsigma_1} n'), hh') = (\xi(n(h \cdot_{\varsigma_1} n')), \gamma(hh'))$$

y

$$\chi(n, h)\chi(n', h') = (\xi(n), \gamma(h))(\xi(n'), \gamma(h')) = (\xi(n)(\gamma(h) \cdot_{\varsigma_2} \xi(n')), \gamma(h)\gamma(h'))$$

mientras que la equivalencia entre los item (2) y (3) es consecuencia de que

$$\xi(h \cdot_{\varsigma_1} n') = \xi(\varsigma_1(h)(n')) = \xi_*(\varsigma_1(h))(n')$$

y

$$\gamma(h) \cdot_{\varsigma_2} \xi(n') = \varsigma_2(\gamma(h))(\xi(n')) = \xi^*(\varsigma_2(\gamma(h)))(n').$$

Para terminar, es claro que la afirmación adicional es verdadera. \square

16. Sucesiones exactas cortas

Una sucesión de grupos y morfismos

$$\dots \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \xrightarrow{\varsigma} D \longrightarrow \dots$$

es una *sucesión exacta* si la imagen de cada morfismo es el núcleo del siguiente. Por ejemplo, todas las sucesiones

$$G \xrightarrow{\varphi} G' ,$$

consistentes de un sólo morfismo, son exactas. Las de la forma

$$1 \longrightarrow G \xrightarrow{\varphi} G'$$

lo son si y sólo si φ es un monomorfismo, y las de la forma

$$G \xrightarrow{\varphi} G' \longrightarrow 1,$$

si y sólo si φ es un epimorfismo. Una *sucesión exacta corta* es una sucesión exacta de la forma

$$(12) \quad 1 \longrightarrow G' \xrightarrow{\varphi} G \xrightarrow{\psi} G'' \longrightarrow 1 .$$

Es fácil ver que este es el caso si y sólo si φ es inyectiva, ψ es sobreyectiva e $\text{Im } \varphi = \ker \psi$. La sucesión exacta corta (12) es escindida a derecha si ψ es una retracción y a izquierda si φ es una sección.

Si hay un sucesión exacta corta de grupos como (12), decimos que G es una *extensión de G' por G''* .

EJEMPLO 1.146. Si $N \times_{\zeta} H$ es un producto semidirecto, entonces

$$(13) \quad 1 \longrightarrow N \xrightarrow{\iota_N} N \times_{\zeta} H \xrightarrow{\pi_H} H \longrightarrow 1 ,$$

donde ι_N y π_H son los morfismos canónicos, es una sucesión exacta corta escindida a derecha. Si $\zeta: H \rightarrow \text{Aut}(N)$ es el morfismo trivial (esto es, si $N \times_{\zeta} H$ es el producto directo de N con H), entonces esta sucesión también es escindida a izquierda.

EJEMPLO 1.147. 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 que no es escindida ni a izquierda ni a derecha.

Diremos que la sucesión exacta corta (12) es *equivalente* a la sucesión exacta corta

$$(14) \quad 1 \longrightarrow G' \xrightarrow{\iota} L \xrightarrow{\pi} G'' \longrightarrow 1 ,$$

si existe un morfismo $\alpha: G \rightarrow L$ tal que el diagrama

$$\begin{array}{ccccccc} 1 & \longrightarrow & G' & \xrightarrow{\varphi} & G & \xrightarrow{\psi} & G'' \longrightarrow 1 \\ & & \downarrow \text{id}_{G'} & & \downarrow \alpha & & \downarrow \text{id}_{G''} \\ 1 & \longrightarrow & G' & \xrightarrow{\iota} & L & \xrightarrow{\pi} & G'' \longrightarrow 1 \end{array}$$

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

$$\begin{aligned} \alpha(g) = 1 &\Rightarrow \exists g' \in G' \text{ tal que } \varphi(g') = g && \text{porque } \psi(g) = \pi \circ \alpha(g) = 1 \text{ y (12) es exacta} \\ &\Rightarrow g' = 1 && \text{porque } \iota(g') = \alpha(g) = 1 \text{ y (14) es exacta} \\ &\Rightarrow g = \varphi(g') = 1, \end{aligned}$$

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

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

En consecuencia, debido a la exactitud de (14), hay un $g' \in G'$ tal que $\iota(g') = \alpha(g^{-1})l$ y, así,

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

como queremos.

EJERCICIO 1.148. Consideremos un diagrama conmutativo de morfismos de grupos

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G' & \xrightarrow{\varphi} & G & \xrightarrow{\psi} & G'' & \longrightarrow & 1 \\ & & \downarrow \alpha' & & \downarrow \alpha & & \downarrow \alpha'' & & \\ 1 & \longrightarrow & L' & \xrightarrow{\iota} & L & \xrightarrow{\pi} & L'' & \longrightarrow & 1 \end{array}$$

cuyas filas son exactas. Pruebe lo siguiente:

1. Si α' y α'' son inyectivas, entonces α también lo es.
2. Si α' y α'' son sobreyectivas, entonces α también lo es.

De la definición resulta evidente que la relación de equivalencia de sucesiones exactas cortas es reflexiva y transitiva. Ahora es claro que también es simétrica. Notemos que si dos sucesiones como las (12) y (14) son equivalentes, entonces una de ellas es escindida a un lado si y sólo si la otra lo es. En el Ejemplo 1.146 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 1.149. Si una sucesión exacta corta

$$(15) \quad 1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow 1$$

es escindida a derecha, entonces existe un producto semidirecto $N \times_{\zeta} H$ tal que las sucesiones exactas cortas (13) y (15), 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

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

es un morfismo de grupos, y de hecho un automorfismo, con inversa $g \mapsto s(h)^{-1}gs(h)$. Además, $\Phi_{s(h)}$ induce por restricción un automorfismo de $\iota(N)$, porque

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

para cada $g \in \iota(N)$. Por lo tanto, hay una única aplicación $\zeta: H \rightarrow \text{Aut}(N)$, tal que

$$\iota(\zeta(h)(n)) = s(h)\iota(n)s(h)^{-1} \quad \text{para todo } h \in H \text{ y todo } n \in N.$$

Además ζ es un morfismo de grupos, porque

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

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

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\iota_N} & N \times_{\zeta} H & \xrightarrow{\pi_H} & H & \longrightarrow & 1 \\ & & \downarrow \text{id}_N & & \downarrow \alpha & & \downarrow \text{id}_H & & \\ 1 & \longrightarrow & N & \xrightarrow{\iota} & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \end{array}$$

conmuta. Pero las igualdades

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

muestran que lo último es cierto, y las igualdades

$$\begin{aligned} \alpha((n, h)(n', h')) &= \alpha(n(h \cdot n'), hh') \\ &= \iota(n(h \cdot n'))s(hh') \\ &= \iota(n)\iota(h \cdot n')s(h)s(h') \\ &= \iota(n)s(h)\iota(n')s(h)^{-1}s(h)s(h') \\ &= \iota(n)s(h)\iota(n')s(h') \\ &= \alpha(n, h)\alpha(n', h'), \end{aligned}$$

que lo primero también lo es. □

OBSERVACIÓN 1.150. *En la demostración del Teorema 1.149 no sólo probamos que la sucesión exacta corta (15) 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 1.151. *Si G es producto semidirecto interno $G = NH$ de un subgrupo normal N con un subgrupo H , entonces la sucesión de morfismos*

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

donde ι es la inclusión canónica y π está dado por $\pi(nh) := h$ es una sucesión exacta corta. Por el Teorema 1.149, como la inclusión canónica de H en G es una sección de π , el diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\iota_N} & N \times_{\zeta} H & \xrightarrow{\pi_H} & H & \longrightarrow & 1 \\ & & \downarrow \text{id}_N & & \downarrow \alpha & & \downarrow \text{id}_H & & \\ 1 & \longrightarrow & N & \xrightarrow{\iota} & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \end{array},$$

donde $\zeta(h)(n) := hnh^{-1}$ 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 1.140.

PROPOSICIÓN 1.152. *Las sucesiones exactas cortas asociadas a dos productos semidirectos $N \times_{\zeta_1} H$ y $N \times_{\zeta_2} H$ son equivalentes si y sólo si existe una función $\varpi: H \rightarrow N$ que satisfice:*

$$(16) \quad \varpi(hh') = \varpi(h)(h \cdot_{\zeta_2} \varpi(h')) \quad \text{y} \quad (h \cdot_{\zeta_1} n)\varpi(h) = \varpi(h)(h \cdot_{\zeta_2} n),$$

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

DEMOSTRACIÓN. Evidentemente para cada función $\chi: N \times_{\varsigma_1} H \rightarrow N \times_{\varsigma_1} H$, la conmutatividad del diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\iota_N} & N \times_{\varsigma_1} H & \xrightarrow{\pi_H} & H & \longrightarrow & 1 \\ & & \downarrow \text{id}_N & & \downarrow \chi & & \downarrow \text{id}_H & & \\ 1 & \longrightarrow & N & \xrightarrow{\iota_N} & N \times_{\varsigma_2} H & \xrightarrow{\pi_H} & H & \longrightarrow & 1 \end{array}$$

equivale a que existe una función $\omega: N \times_{\varsigma_1} H \rightarrow N$ tal que

$$\chi(n, h) = (\omega(n, h), h) \quad \text{para todo } n \in N \text{ y } h \in H$$

y

$$(17) \quad \omega(n, 1) = n \quad \text{para todo } n \in N.$$

Es fácil ver ahora que

$$(18) \quad \chi((n, 1)(1, h)) = \chi(n, 1)\chi(1, h) \quad \text{para todo } n \in N \text{ y } h \in H$$

si y sólo si ω es de la forma $\omega(n, h) = n\varpi(h)$, donde ϖ es una función de H en N . En efecto, si esto es así, entonces

$$\chi((n, 1)(1, h)) = \chi(n, h) = (n\varpi(h), h) = (n, 1)(\varpi(h), h) = \chi(n, 1)\chi(1, h),$$

mientras que si (18) se satisface, entonces

$$\chi(n, h) = \chi((n, 1)(1, h)) = \chi(n, 1)\chi(1, h) = (n, 1)(\omega(1, h), h) = (n\omega(1, h), h),$$

y, en consecuencia podemos tomar a $\varpi(h)$ como $\omega(1, h)$. Supongamos que estamos en esta situación. Entonces,

$$\chi((n, h)(n', h')) = \chi(n(h \cdot_{\varsigma_1} n'), hh') = (n(h \cdot_{\varsigma_1} n')\varpi(hh'), hh')$$

y

$$\chi(n, h)\chi(n', h') = (n\varpi(h), h)(n'\varpi(h'), h') = (n\varpi(h)(h \cdot_{\varsigma_2} (n'\varpi(h'))), hh').$$

Por lo tanto χ es un morfismo de grupos si y sólo si

$$(h \cdot_{\varsigma_1} n')\varpi(hh') = \varpi(h)(h \cdot_{\varsigma_2} (n'\varpi(h'))).$$

Tomando $n' = 1$ y $h' = 1$, obtenemos respectivamente que

$$\varpi(hh') = \varpi(h)(h \cdot_{\varsigma_2} \varpi(h')) \quad \text{y} \quad (h \cdot_{\varsigma_1} n')\varpi(h) = \varpi(h)(h \cdot_{\varsigma_2} (n'\varpi(1))).$$

Pero entonces, por la primera de estas igualdades $\varpi(1) = \varpi(1)\varpi(1)$, lo que implica que $\varpi(1) = 1$ y, en consecuencia, (16) se satisface. Recíprocamente si este es el caso, entonces

$$(h \cdot_{\varsigma_1} n')\varpi(hh') = (h \cdot_{\varsigma_1} n')\varpi(h)(h \cdot_{\varsigma_2} \varpi(h')) = \varpi(h)(h \cdot_{\varsigma_2} n')(h \cdot_{\varsigma_2} \varpi(h')) = \varpi(h)(h \cdot_{\varsigma_2} (n'\varpi(h'))),$$

como queremos. \square

Notemos que la primera igualdad en (16) aparece también en la Observación 1.141. Esto no es casualidad, se debe a que la composición de χ con la inclusión canónica de H en $N \times_{\varsigma_1} H$ es una sección del epimorfismo canónica $\pi: N \times_{\varsigma_2} H \rightarrow H$.

TEOREMA 1.153. *Si una sucesión exacta corta*

$$(19) \quad 1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow 1$$

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

$$(\gamma, \pi): G \rightarrow N \times H.$$

Como

$$(\gamma, \pi) \circ \iota(n) = (n, 1) \quad \text{y} \quad \pi_H \circ (\gamma, \pi)(g) = \pi(g) \quad \text{para todo } n \in N \text{ y } g \in G,$$

el diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\iota} & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \\ & & \downarrow \text{id}_N & & \downarrow (\gamma, \pi) & & \downarrow \text{id}_H & & \\ 1 & \longrightarrow & N & \xrightarrow{\iota_N} & N \times H & \xrightarrow{\pi_H} & H & \longrightarrow & 1 \end{array}$$

conmuta, lo que prueba el resultado. □

17. Automorfismos interiores y subgrupos característicos

Un elemento g de un grupo G es *central* si $gh = hg$ para todo $h \in G$. El *centro* ZG de G es el conjunto de todos los elementos centrales de G .

OBSERVACIÓN 1.154. Para toda familia $(G_i)_{i \in I}$ de grupos,

$$Z\left(\prod G_i\right) = \prod Z(G_i) \quad \text{y} \quad Z\left(\bigsqcup G_i\right) = \bigsqcup Z(G_i).$$

EJEMPLO 1.155. A continuación calculamos el centro de los grupos diedrales y cuaterniónicos. Recordemos que el grupo diedral D_n está generado por dos elementos x e y sujetos a las relaciones $x^n = 1$, $y^2 = 1$ e $xyx^{-1} = y$, y que

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

Es claro que D_2 es conmutativo. Consideremos el caso $n > 2$. Entonces $x^2 \neq 1$ y, así, de la igualdad $x(x^i y)x^{-1} = x^{i+2}y$ se sigue que $x^i y \notin ZD_n$ para ningún i . Por otro lado, dado que

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

obtenemos que $x^i \in ZD_n$ si y sólo si $i = n/2$. Por lo tanto,

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

Recordemos ahora que H_n es un grupo generado por dos elementos x, y sujetos a las relaciones $x^n y^{-2} = 1$ e $xyx^{-1} = y$ 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 $x^i y \notin ZH_n$ para ningún i , y puesto que

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

es claro que $x^i \in ZH_n$ si y sólo si $i = 0$ o $i = n$. Por consiguiente, $ZH_n = \{1, x^n\}$.

EJERCICIO 1.156. Muestre que si $f: G \rightarrow G$ es un endomorfismo de grupos, entonces no necesariamente $f(ZG) \subseteq ZG$.

EJERCICIO 1.157. Pruebe que si $f: G \rightarrow G'$ es un morfismo sobreyectivo de grupos, entonces $f(ZG) \subseteq ZG'$.

EJERCICIO 1.158. 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 $N \subseteq Z(H \times L)$.

Para cada $g \in G$, consideremos la función $\Phi_g: G \rightarrow G$, definida por $\Phi_g(h) := ghg^{-1}$. Es claro que Φ_g es biyectiva, con inversa $\Phi_{g^{-1}}$, y la igualdad

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

muestra que, de hecho, es un automorfismo, llamado *el automorfismo interior de G asociado a g* . Además es fácil ver que la aplicación

$$\begin{array}{ccc} G & \xrightarrow{\Phi} & \text{Aut}(G) \\ g & \longmapsto & \Phi_g \end{array}$$

es un morfismo de grupos cuya imagen es el conjunto $\text{Int}(G)$ de los automorfismos interiores de G , y cuyo núcleo es el centro de G . En consecuencia ZG es un subgrupo normal de G . Hasta ahora nos hemos limitado a repetir el razonamiento hecho en la demostración del Teorema 1.149. Aunque sencillo, el siguiente es el primer resultado esencialmente nuevo.

PROPOSICIÓN 1.159. La igualdad $\varphi \circ \Phi_g \circ \varphi^{-1} = \Phi_{\varphi(g)}$ vale para cada $\varphi \in \text{Aut}(G)$ y $g \in G$. En particular, $\text{Int}(G) \triangleleft \text{Aut}(G)$.

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

$$1 \longrightarrow ZG \xrightarrow{\iota} G \xrightarrow{\Phi} \text{Aut}(G) \xrightarrow{\pi} \text{Out}(G) \longrightarrow 1,$$

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

EJEMPLO 1.160. Consideremos al grupo diedral D_n presentado como en el Ejemplo 1.155. Un cálculo directo muestra que

$$\Phi_{x^j}(x) = x, \quad \Phi_{x^j}(y) = x^{2j}y, \quad \Phi_{x^j y}(x) = x^{-1} \quad y \quad \Phi_{x^j y}(y) = x^{2j}y.$$

En consecuencia si $n > 2$ y ϕ es como en el Ejemplo 1.114, entonces

$$\phi(\text{Int}(D_n)) = \begin{cases} \{(j, 1) : 0 \leq j < n\} \cup \{(j, n-1) : 0 \leq j < n\} & \text{si } n \text{ es impar,} \\ \{(2j, 1) : 0 \leq j < n/2\} \cup \{(2j, n-1) : 0 \leq j < n/2\} & \text{si } n \text{ es par.} \end{cases}$$

Consideremos ahora al grupo cuaterniónico H_n presentado también como en el Ejemplo 1.155. De la misma manera que para D_n

$$\Phi_{x^j}(x) = x, \quad \Phi_{x^j}(y) = x^{2j}y, \quad \Phi_{x^j y}(x) = x^{-1} \quad y \quad \Phi_{x^j y}(y) = x^{2j}y,$$

y, en consecuencia, si $n > 2$ y ϕ es como en el Ejemplo 1.115, entonces

$$\phi(\text{Int}(H_n)) = \{(2j, 1) : 0 \leq j < n\} \cup \{(2j, n-1) : 0 \leq j < n\}.$$

El siguiente es un resultado sencillo pero muy útil.

PROPOSICIÓN 1.161. Si G/ZG es cíclico, entonces G es abeliano.

DEMOSTRACIÓN. Por hipótesis existe $g \in G$ tal que $G = \langle g \rangle ZG$. Como

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

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

Dos elementos g y h de un grupo G son *conjugados* si existe $k \in G$ tal que

$$h = \Phi_k(g) = k g k^{-1}.$$

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 1.162. 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 $h = k g k^{-1} = k(g k^{-1})$, entonces $(g k^{-1})k = g$. \square

EJERCICIO 1.163. Calcule las clases de conjugación en los grupos D_n y H_n .

EJERCICIO 1.164. Pruebe que si un grupo G contiene un elemento de orden $n > 1$ y dos clases de conjugación, entonces $|G| = 2$.

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 $\varphi \in \text{Aut}(G)$. Entonces $\varphi(H) = H$ para todo $\varphi \in \text{Aut}(G)$. En efecto,

$$\varphi^{-1}(H) \subseteq H \Rightarrow H \subseteq \varphi(H).$$

Es evidente que todo subgrupo característico de G es normal. Afirmamos que ZG es un subgrupo característico de G . Para probarlo debemos mostrar que si $g \in ZG$ y $\varphi \in \text{Aut}(G)$, entonces $\varphi(g) \in ZG$. 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 $h \in G$.

EJERCICIO 1.165. Pruebe que todos los subgrupos de H_2 son normales.

EJEMPLO 1.166. Consideremos al grupo diedral D_n presentado como en el Ejemplo 1.155. De los cálculos realizados en los Ejemplos 1.46 y 1.114 se sigue fácilmente que si $n > 2$, entonces los subgrupos característicos de D_n son D_n y los subgrupos de $\langle x \rangle$. Algo similar ocurre con el grupo H_n , pero en este caso hay que usar los cálculos realizados en los Ejemplos 1.47 y 1.115 en lugar de los realizados en los Ejemplos 1.46 y 1.114.

OBSERVACIÓN 1.167. Puede suceder que $H \triangleleft L \triangleleft G$, pero que H no sea normal en G . Por ejemplo, este es el caso cuando $G = S_4$, $L = \{\text{id}, \sigma_1, \sigma_2, \sigma_3\}$, donde σ_1, σ_2 y σ_3 son las permutaciones definidas por

$$\begin{aligned} \sigma_1(1) &= 2, & \sigma_1(2) &= 1, & \sigma_1(3) &= 4, & \sigma_1(4) &= 3, \\ \sigma_2(1) &= 3, & \sigma_2(2) &= 4, & \sigma_2(3) &= 1, & \sigma_2(4) &= 2, \\ \sigma_3(1) &= 4, & \sigma_3(2) &= 3, & \sigma_3(3) &= 2, & \sigma_3(4) &= 1, \end{aligned}$$

y $H = \{\text{id}, \sigma_1\}$. Esto no ocurre si H es un subgrupo característico de L . En efecto, como $L \triangleleft G$, para cada $g \in G$ el automorfismo interior Φ_g de G define por restricción un automorfismo ψ (no necesariamente interior) de L . Pero entonces

$$\Phi_g(H) = \psi(H) = H,$$

porque H es característico en L . También vale que si H es un subgrupo característico de L y L un subgrupo característico de G , entonces H es un subgrupo característico de G . La demostración es la misma, pero en lugar de automorfismos interiores de G hay que considerar automorfismos arbitrarios.

Decimos que un subgrupo H de un grupo G es *completamente normal* si $\varphi(H) \subseteq H$ para todo $\varphi \in \text{End}(G)$. Claramente todo subgrupo completamente normal de G es característico. Por el Ejercicio 1.156 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 1.168. 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 1.169. Supongamos que $H \leq L \leq G$.

1. Si H es normal en G y L/H es normal en G/H , entonces L es normal en G .
2. Si H es característico en G y L/H es característico en G/H , entonces L es característico en G .
3. Si H es completamente normal en G y L/H es completamente normal en G/H , entonces L es completamente normal en G .

DEMOSTRACIÓN. Recordemos que para cada $g \in G$ denotamos con $[g]$ a su clase en G/H . Como $\Phi_{[g]}(L/H) = \Phi_g(L)/H$ y L/H es normal en G/H ,

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

lo cual implica que $\Phi_g(L) = L$. Esto prueba el ítem 1). Los ítems 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. \square

17.1. 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 $\varphi: G \rightarrow G'$ y todo par de elementos g y h de G . Por lo tanto, $\varphi([G, G]) \subseteq [G', G']$. En particular, tomando $G' = G$ se deduce que $[G, G]$ es un subgrupo completamente normal de G . Al cociente $G/[G, G]$ se lo denomina el *abelianizado* de G . Es un grupo conmutativo, porque $gh = [g, h]hg$. En consecuencia, por el teorema de la correspondencia, si H es un subgrupo de G que contiene a $[G, G]$, entonces H es normal y G/H es conmutativo. Recíprocamente, si H es un subgrupo normal de G y G/H es conmutativo, entonces $[G, G] \subseteq H$ puesto que la clase de $[g, h] = ghg^{-1}h^{-1}$ en G/H es el elemento neutro de G/H , para todo $g, h \in G$. Una consecuencia de esta reflexión es que $[G, G] = 1$ si y sólo si G es conmutativo (lo que por otra parte es obvio).

Si φ es un morfismo de G en un grupo conmutativo G' , entonces $\varphi([G, G]) = 1$. Por consiguiente existe un único morfismo $\varphi': G/[G, G] \rightarrow G'$ tal que el diagrama

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow \pi & \nearrow \varphi' & \\ G/[G, G] & & \end{array},$$

donde π denota a la proyección canónica, conmuta. Esta es la propiedad universal del abelianizado de G .

Por el comentario que precede a la Proposición 1.95, para cada morfismo de grupos

$$\varphi: G \rightarrow G'$$

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

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow \pi & & \downarrow \pi' \\ G/[G, G] & \xrightarrow{\bar{\varphi}} & G'/[G', G'] \end{array},$$

conmuta. Es evidente que $\overline{\text{id}_G} = \text{id}_{G/[G, G]}$ y que si $\varphi: G \rightarrow G'$ y $\psi: G' \rightarrow G''$ son dos morfismos de grupos, entonces $\overline{\psi \circ \varphi} = \bar{\psi} \circ \bar{\varphi}$.

EJEMPLO 1.170. Consideremos el grupo diedral D_n , presentado como en el Ejemplo 1.155. Vamos a determinar su subgrupo conmutador. Puesto que $[x, y] = x^2$, el subgrupo $\langle x^2 \rangle$ de D_n está incluido en $[D_n, D_n]$. Pero como $\langle x^2 \rangle$ es un subgrupo normal de D_n y $D_n/\langle x^2 \rangle \simeq D_2$ es conmutativo, $[D_n, D_n] = \langle x^2 \rangle$. Consideremos ahora el grupo cuaterniónico generalizado, también con la presentación dada en el Ejemplo 1.155. Como $\langle x^2 \rangle \triangleleft H_n$, el cociente $H_n/\langle x^2 \rangle$ es conmutativo y $[x, y] = x^2$, el subgrupo conmutador de H_n es $\langle x^2 \rangle$.

17.2. 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 $\varphi: G \rightarrow G'$.

PROPOSICIÓN 1.171. Si H y L son subgrupos normales, característicos o completamente normales de G , entonces $[H, L]$ también lo es.

DEMOSTRACIÓN. Supongamos que H y L son normales en G . Entonces

$$\Phi_g([H, L]) = [\Phi_g(H), \Phi_g(L)] = [H, L]$$

para todo $g \in G$. Esto prueba que $[H, L]$ es un subgrupo normal de G . Los otros casos pueden tratarse de manera similar. \square

OBSERVACIÓN 1.172. Si H y L son subgrupos de un grupo G y $K \triangleleft G$, entonces $[H, L] \subseteq K$ si y sólo si las clases en G/K de los elementos de H conmutan con las de los de L . En particular $[G, H] \subseteq K$ si y sólo si $HK/K \subseteq Z(G/K)$. Denotemos con \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 K tal que $[H, L] \subseteq K$ es $\overline{[H, L]}$. Como $[H, L] \subseteq [\overline{H}, \overline{L}]$ y, por la Proposición 1.171, el subgrupo $[\overline{H}, \overline{L}]$ de G es normal, $\overline{[H, L]}$ está incluido en $[\overline{H}, \overline{L}]$.

Supongamos que H y L son subgrupos normales de un grupo G . Si $\varphi: G \rightarrow G'$ es un morfismo de grupos y los elementos de $\varphi(H)$ conmutan con los de $\varphi(L)$, entonces existe un único morfismo $\varphi': G/[H, L] \rightarrow G'$ tal que el diagrama

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow \pi & \nearrow \varphi' & \\ G/[H, L] & & \end{array}$$

donde π denota a la proyección canónica, conmuta.

Consideremos ahora un morfismo de grupos $\varphi: G \rightarrow G'$, y subgrupos normales H, L de G y H', L' de G' . Por el comentario que precede a la Proposición 1.95, si $\varphi(H) \subseteq H'$ y $\varphi(L) \subseteq L'$, entonces existe un único morfismo $\overline{\varphi}: \frac{G}{[H, L]} \rightarrow \frac{G'}{[H', L']}$ tal que el diagrama

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

conmuta. Es claro que $\overline{\text{id}_G} = \text{id}_{G/[H, L]}$ y que si $\varphi: G \rightarrow G'$ es como arriba y $\psi: G' \rightarrow G''$ es un morfismo de grupos que satisface $\psi(H') \subseteq H''$ y $\psi(L') \subseteq L''$, donde H'' y L'' son subgrupos normales de G'' , entonces $\overline{\psi \circ \varphi} = \overline{\psi} \circ \overline{\varphi}$.

OBSERVACIÓN 1.173. Para cada terna $(H_i)_{i \in I}, (L_i)_{i \in I}$ y $(G_i)_{i \in I}$, de familias de grupos tal que $H_i, L_i \leq G_i$ para todo i ,

$$\left[\prod H_i, \prod L_i \right] = \prod [H_i, L_i] \quad \text{y} \quad \left[\bigsqcup H_i, \bigsqcup L_i \right] = \bigsqcup [H_i, L_i].$$

EJERCICIO 1.174. Pruebe que el conmutador $[-, -]: G \times G \rightarrow G$ 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. $[cac^{-1}, [b, c]][cbcb^{-1}, [a, b]][aba^{-1}, [c, a]] = 1$ (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).

17.3. Subgrupos conjugados

Dos subgrupos L y H de un grupo G son *conjugados* si existe $g \in G$ tal que $L = gHg^{-1}$. Es evidente que los ordenes de dos subgrupos conjugados coinciden. Además, puesto que $gHg^{-1} = \Phi_g(H)$, se sigue del Teorema 1.90 que también coinciden sus índices. Claramente la relación \sim , definida en el conjunto de los subgrupos de G por $L \sim H$ si L y H son conjugados, es de equivalencia. Los elementos de la partición asociada son llamados *clases de conjugación de subgrupos de G* . De la definición se sigue fácilmente que un subgrupo H de G es normal si y sólo si es el único elemento de su clase de conjugación. Más aún, para cada subgrupo H de G , la intersección

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

de todos los subgrupos conjugados a H , es el máximo subgrupo normal de G incluido 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 incluidos 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 exactamente un elemento para cada $g \in G$), entonces

$$N = \bigcap_{i \in I} g_i H g_i^{-1},$$

puesto que $(g_i h)H(g_i h)^{-1} = g_i H g_i^{-1}$, para todo $i \in I$ y $h \in H$.

OBSERVACIÓN 1.175. *Es evidente que si g es un elemento de orden 2 de G , entonces $\langle g' \rangle$ es conjugado de $\langle g \rangle$ si y sólo si g' lo es de g .*

OBSERVACIÓN 1.176. *Supongamos que H es un subgrupo de G de índice finito n . Consideremos un conjunto de representantes $\{g_1, \dots, g_n\}$ de las coclases a izquierda de H en G . Por la Observación 1.38*

$$|G/N| \leq \prod_{i=1}^n |G/g_i H g_i^{-1}| = n^n.$$

Esta desigualdad será mejorada más adelante.

17.4. El normalizador y el centralizador

El *normalizador* y el *centralizador* de un subconjunto H de G son los subgrupos

$$N_G(H) := \{g \in G : gHg^{-1} = H\} \quad \text{y} \quad C_G(H) := \{g \in G : ghg^{-1} = h \text{ para todo } h \in H\}$$

de G , respectivamente. Es obvio que $C_G(H) \leq N_G(H)$. Además, si $g \in N_G(H)$ y $l \in C_G(H)$, 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, $C_G(H) \triangleleft N_G(H)$. De las definiciones se sigue que:

1. $C_G(gHg^{-1}) = g C_G(H) g^{-1}$ y $N_G(gHg^{-1}) = g N_G(H) g^{-1}$ para todo $g \in G$.
2. $H \subseteq C_G(H)$ si y sólo si los elementos de H conmutan entre si y, en ese caso, $C_G(H)$ es el máximo subgrupo de G en el que los elementos de H son centrales.
3. Si H es un subgrupo de G , entonces $N_G(H)$ es máximo subgrupo de G en el que H es normal.
4. $C_G(H) = C_G(\langle H \rangle)$ y $N_G(H) \subseteq N_G(\langle H \rangle)$.
5. $\bigcap_{i \in I} C_G(H_i) = C_G(\bigcup_{i \in I} H_i)$ para cada familia $(H_i)_{i \in I}$ de subconjuntos de G .
6. $\bigcup_{i \in I} C_G(H_i) \subseteq C_G(\bigcap_{i \in I} H_i)$ para cada familia $(H_i)_{i \in I}$ de subconjuntos de G .
7. $\bigcap_{i \in I} N_G(H_i) \subseteq N_G(\bigcap_{i \in I} H_i)$ para cada familia $(H_i)_{i \in I}$ de subconjuntos de G .
8. $\bigcup_{i \in I} N_G(H_i) \subseteq N_G(\bigcup_{i \in I} H_i)$ para cada familia $(H_i)_{i \in I}$ de subconjuntos de G .

OBSERVACIÓN 1.177. Si $(H_i)_{i \in I}$ y $(G_i)_{i \in I}$ es un par de familias de grupos, tal que $H_i \leq G_i$ para todo i , entonces

$$\begin{aligned} N_{\prod G_i} \left(\prod H_i \right) &= \prod N_{G_i}(H_i), & N_{\sqcup G_i} \left(\sqcup H_i \right) &= \sqcup N_{G_i}(H_i), \\ C_{\prod G_i} \left(\prod H_i \right) &= \prod C_{G_i}(H_i) & \text{y} & & C_{\sqcup G_i} \left(\sqcup H_i \right) &= \sqcup C_{G_i}(H_i). \end{aligned}$$

OBSERVACIÓN 1.178. Es evidente que si $g \in G$ tiene orden 2, entonces $C_G(g) = N_G(\langle g \rangle)$. En consecuencia $\langle g \rangle \triangleleft G$ si y sólo si $g \in ZG$.

EJERCICIO 1.179. Calcule los centralizadores de los elementos de D_n y H_n .

Decimos que un subgrupo L de G normaliza a otro subgrupo H si $L \subseteq N_G(H)$. Similarmente, decimos que L centraliza a H si $L \subseteq C_G(H)$. 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 $H, L \subseteq N_G(H)$ y H es normal en $N_G(H)$, el conjunto HL es un subgrupo de $N_G(H)$ y, por lo tanto, de G . Además $H/(H \cap L) \simeq HL/H$, porque $H \triangleleft HL$.

OBSERVACIÓN 1.180. 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 $H \subseteq ZG$.

EJERCICIO 1.181. Supongamos que H y L son subgrupos de un grupo G y que L está incluido en $N_G(H)$. Pruebe que si K es un subgrupo normal de L , entonces HK es un subgrupo normal de HL .

Capítulo 2

El grupo simétrico

En este capítulo estudiamos los grupos simétricos o de permutaciones S_n para $n \geq 2$. En particular probamos que S_n tiene un subgrupo canónico A_n , de índice 2, llamado grupo alternado en n símbolos. También encontramos conjuntos de generadores y presentaciones de S_n y A_n , calculamos sus centros y subgrupos conmutadores y probamos que A_n es simple para todo $n \geq 3$ y distinto de 4, siendo este el resultado más importante que obtendremos.

Empecemos recordando que el orden de S_n es $n!$. Una forma bastante usual (pero que nosotros no utilizaremos nunca) de describir una permutación σ es escribiendo:

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

Recordemos que \mathbb{I}_n denota al conjunto $\{1, \dots, n\}$, de modo que $S_n = S_{\mathbb{I}_n}$. Para cada $\sigma \in S_n$ 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 sí y $\sigma \circ \tau$ satisface

$$\sigma(\tau(j)) = \begin{cases} \sigma(j) & \text{si } \tau \text{ fija } j, \\ \tau(j) & \text{si } \sigma \text{ fija } j. \end{cases}$$

Es evidente que si σ se escribe como un producto $\sigma = \sigma_1 \circ \dots \circ \sigma_s$ de permutaciones disjuntas dos a dos, entonces el conjunto de puntos movidos por σ es la unión disjunta de los conjuntos de puntos movidos por cada σ_i .

1. Estructura cíclica

Una permutación $\sigma \in S_n$ 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

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

Es fácil ver que el orden de un r -ciclo es r y que hay

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

r -ciclos en S_n . El único 1-ciclo es la permutación identidad. A los 2 ciclos también se los llama *transposiciones*. El hecho que el mismo símbolo (i, j) designe a un par ordenado y a una permutación no es grave, porque en cada caso el significado quedará claro por el contexto.

TEOREMA 2.1. *Toda permutación $\sigma \in S_n$ se escribe como un producto $\sigma = \sigma_1 \circ \dots \circ \sigma_r$ de ciclos de orden mayor que 1 disjuntos dos a dos (y que por lo tanto conmutan entre sí). Además el orden de σ es el mínimo de los múltiplos comunes de los órdenes de los σ_i 's, y esta escritura es única, salvo el orden en que aparecen sus factores.*

DEMOSTRACIÓN. Primero probaremos la existencia, por inducción en la cantidad k de elementos de \mathbb{I}_n que son movidos por σ . Si $k = 0$, entonces σ es la identidad, que puede pensarse como la composición de la familia vacía de ciclos. Supongamos que $k > 0$ y que el resultado vale para las permutaciones que mueven menos que k elementos. Tomemos $i_1 \in \mathbb{I}_n$ tal que $\sigma(i_1) \neq i_1$ y definamos $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$, $i_4 = \sigma(i_3)$, etcétera. Como \mathbb{I}_n es finito existe un mínimo número natural r tal que $i_{r+1} \in \{i_1, \dots, i_r\}$ y, como σ es inyectiva, forzosamente debe ser $i_{r+1} = i_1$. Consideremos el r -ciclo σ_1 definido por

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

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

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

Como $\{i_1, \dots, i_r\}$ es dejado fijo por cada uno de los ciclos $\sigma_2, \dots, \sigma_s$ la expresión

$$\sigma = \sigma_1 \circ \dots \circ \sigma_s$$

es un producto de ciclos disjuntos dos a dos.

Veamos ahora la unicidad. Supongamos que

$$\sigma = \sigma_1 \circ \dots \circ \sigma_s = \sigma'_1 \circ \dots \circ \sigma'_{s'}$$

Si $s = 0$, entonces σ es la identidad, y también $s' = 0$. Supongamos que $s > 0$. Tomemos un elemento i_1 movido por σ_1 . Entonces i_1 también es movido por un σ'_i y, como los σ'_j conmutan entre sí, podemos suponer que $i = 1$. Es fácil ver que $\sigma_1^k(i_1) = \sigma^k(i_1) = \sigma'^k_1(i_1)$ para todo $k \in \mathbb{N}$. Pero entonces $\sigma_1 = \sigma'_1$ y, por lo tanto,

$$\sigma_2 \circ \dots \circ \sigma_s = \sigma_2 \circ \dots \circ \sigma'_{s'}.$$

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 $\sigma^r = \sigma_1^r \circ \dots \circ \sigma_s^r = \text{id}$. 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' . \square

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 $\sigma \in S_n$ como un producto de ciclos distintos de la identidad y disjuntos dos a dos

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

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

$$r_1 + \cdots + r_s \leq n \quad \text{y} \quad n - r_1 - \cdots - r_s$$

es la cantidad de puntos dejados fijos por σ . Denotemos con α_1 a este número y con α_j , para $1 < j \leq n$, 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 $r_1 \leq r_2 \leq \cdots \leq r_s$ con $r_1 \geq 2$ tales que $r_1 + \cdots + r_s \leq n$ y el de los enteros no negativos $\alpha_1, \dots, \alpha_n \geq 0$ 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 .

TEOREMA 2.2. *Dos permutaciones son conjugadas en S_n si y sólo si tienen la misma estructura cíclica. Además si*

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

y τ es una permutación arbitraria, entonces

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

DEMOSTRACIÓN. Un cálculo sencillo muestra que

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

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

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

tiene la misma estructura cíclica que σ . Recíprocamente, supongamos que σ y σ' son dos permutaciones que tienen la misma estructura cíclica y, más precisamente, que

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

y

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

Entonces la permutación $\tau \in S_n$ definida por

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

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

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

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

Para cada una de estas sucesiones, consideremos los números $\mu_j := \alpha_j + \dots + \alpha_n$. Por su misma definición

$$(20) \quad \mu_1 \geq \mu_2 \geq \dots \geq \mu_n \quad \text{y} \quad \mu_1 + \dots + \mu_n = n.$$

Las sucesiones de enteros no negativos que satisfacen (20) son llamadas *particiones* de n porque dan las formas de “partir” n como suma de n o menos números naturales. Por otro lado, dada una partición $\mu_1 \geq \mu_2 \geq \dots \geq \mu_n$ de n , podemos definir

$$\alpha_j := \begin{cases} \mu_j - \mu_{j+1} & \text{si } j < n, \\ \mu_n & \text{si } j = n, \end{cases}$$

y claramente

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

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

EJEMPLO 2.3. *Las particiones de 5 son*

$(1, 1, 1, 1, 1)$, $(2, 1, 1, 1, 0)$, $(2, 2, 1, 0, 0)$, $(3, 1, 1, 0, 0)$, $(3, 2, 0, 0, 0)$, $(4, 1, 0, 0, 0)$ y $(5, 0, 0, 0, 0)$.

Por lo tanto S_5 tiene 7 clases de conjugación.

Por último, la cantidad de elementos que tiene la clase de conjugación asociada a la estructura cíclica $[\alpha_1, \dots, \alpha_n]$ es

$$(21) \quad \frac{n!}{1^{\alpha_1}\alpha_1! 2^{\alpha_2}\alpha_2! \dots n^{\alpha_n}\alpha_n!}.$$

En efecto, esto se sigue de que cada j -ciclo se puede obtener de j formas distintas

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

y de que si permutamos entre sí los α_j ciclos de orden j obtenemos la misma permutación de S_n . La expresión (21) es conocida como fórmula de Cauchy.

OBSERVACIÓN 2.4. *El Teorema 2.2 puede usarse para probar que si un morfismo de grupos $f: G \rightarrow H$ no es sobreyectivo, entonces tampoco es un epimorfismo. Con este fin escribamos $K := \text{Im } f$ y supongamos que K es un subgrupo propio de H . Debemos mostrar que hay un grupo N y morfismos distintos $\alpha, \beta: H \rightarrow N$ tales que $\alpha|_K = \beta|_K$. Tomemos $N := S_X$, donde X es el conjunto de las coclases a izquierda de K en H , junto con un elemento adicional $*$. Definamos α por*

$$\alpha(h)(x) := \begin{cases} * & \text{si } x = *, \\ hx & \text{si } x \neq *, \end{cases}$$

y β como la composición $\Phi_\tau \circ \alpha$, donde Φ_τ es la conjugación por la transposición τ de X que intercambia K con $*$. Es fácil ver que α es un morfismo de grupos y es evidente que $*$ es un punto fijo de $\alpha(h)$ para todo $h \in H$, mientras que K es un punto fijo de $\alpha(h)$ si y sólo si $h \in K$. En consecuencia, por la segunda afirmación del Teorema 2.2,

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

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

En los ejemplos que siguen encontramos condiciones sobre n para que S_n contenga un subgrupo isomorfo a \mathbb{Z}_n y a D_n respectivamente. Para realizar los cálculos es conveniente usar la estructura cíclica de las permutaciones involucradas en ellos.

EJEMPLO 2.5. Supongamos que $n \geq 2$ y tomemos $\sigma := (1, \dots, n)$. Como $|\sigma| = n$ el grupo $\langle \sigma \rangle$ es cíclico y tiene orden n . Supongamos ahora que $n \geq 2$ y que $n = n_1 \cdots n_r$ con los n_i coprimos dos a dos. De la misma manera que arriba, para cada i podemos elegir $\sigma_i \in S_n$ tal que $|\sigma_i| = n_i$ y

$$\sigma_i(j) = j \quad \text{para todo } j \text{ tal que } j \leq n_1 + \cdots + n_{i-1} \text{ o } j > n_1 + \cdots + n_i.$$

Como evidentemente $\sigma := \sigma_1 \circ \cdots \circ \sigma_r$ tiene orden n , el grupo $S_{n_1+\dots+n_r}$ contiene un subgrupo isomorfo a \mathbb{Z}_n .

EJEMPLO 2.6. Supongamos que $n > 2$ y tomemos τ y σ en S_n definidos por

$$\sigma := (1, \dots, n) \quad \text{y} \quad \tau := \begin{cases} (1, n) \circ (2, n-1) \circ \cdots \circ ((n-1)/2, (n+1)/2) & \text{si } n \text{ es impar,} \\ (1, n) \circ (2, n-1) \circ \cdots \circ (n/2, (n+2)/2) & \text{si } n \text{ es par.} \end{cases}$$

Como

$$(22) \quad |\tau| = 2, \quad |\sigma| = n \quad \text{y} \quad \tau \circ \sigma \circ \tau = \sigma^{-1}$$

el grupo $\langle \sigma, \tau \rangle$ no es conmutativo y tiene orden menor o igual a $2n$. Dado que por otra parte $\langle \sigma \rangle$ es un subgrupo conmutativo de orden n de $\langle \sigma, \tau \rangle$, se sigue del teorema de Lagrange que necesariamente $|\langle \sigma, \tau \rangle| = 2n$. Así, debido a la Observación 1.108, el subgrupo $\langle \sigma, \tau \rangle$ de S_n es isomorfo a D_n . Supongamos ahora que $n > 2$ y que $n = n_1 \cdots n_r$ con los n_i coprimos dos a dos. De la misma manera que arriba, para cada i podemos elegir σ_i y τ_i en S_n tales que

$$|\tau_i| = 2, \quad |\sigma_i| = n_i, \quad \tau_i \circ \sigma_i \circ \tau_i = \sigma_i^{-1}$$

y

$$\sigma_i(j) = \tau_i(j) = j \quad \text{para todo } j \text{ tal que } j \leq n_1 + \cdots + n_{i-1} \text{ o } j > n_1 + \cdots + n_i$$

Es evidente que $\sigma := \sigma_1 \circ \cdots \circ \sigma_r$ y $\tau := \tau_1 \circ \cdots \circ \tau_r$ satisfacen las condiciones de (22). En consecuencia el mismo argumento que antes muestra que $S_{n_1+\dots+n_r}$ contiene un subgrupo isomorfo a D_n .

2. Generadores de S_n

Un cálculo directo muestra que

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

Como cada permutación es producto de ciclos se sigue de esto que

$$S_n = \langle (1, 2), (1, 3), \dots, (1, n) \rangle.$$

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

$$S_n = \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle.$$

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

$$S_n = \langle (1, 2), (1, \dots, n) \rangle.$$

3. El signo de una permutación

Un par $(i, j) \in \mathbb{I}_n \times \mathbb{I}_n$ es un *descenso* de una permutación $\sigma \in S_n$ si $i < j$ y $\sigma(i) > \sigma(j)$. Designamos con $\text{Des}(\sigma)$ al conjunto de descensos de σ . Por definición el *signo* de σ es

$$\text{sg}(\sigma) := (-1)^{|\text{Des}(\sigma)|}.$$

La propiedad más importante de la función $\text{sg}: S_n \rightarrow \{-1, 1\}$ es que, como estableceremos en el Teorema 2.9, es un morfismo sobreyectivo de grupos.

PROPOSICIÓN 2.7. *Para cada $\sigma \in S_n$ y cada $k < n$, la cantidad de descensos de $(k, k+1) \circ \sigma$ difiere en ± 1 de la de σ .*

DEMOSTRACIÓN. Es evidente que:

- Si $\sigma(\{i, j\}) \neq \{k, k+1\}$, entonces $(i, j) \in \text{Des}((k, k+1) \circ \sigma)$ si y sólo si $(i, j) \in \text{Des}(\sigma)$.
- Si $\sigma(\{i, j\}) = \{k, k+1\}$, entonces $(i, j) \in \text{Des}((k, k+1) \circ \sigma)$ si y sólo si $(i, j) \notin \text{Des}(\sigma)$.

El resultado se sigue fácilmente de estas observaciones. \square

COROLARIO 2.8. *Si $\sigma = \sigma_1 \circ \dots \circ \sigma_s$, donde las σ_i 's son transposiciones de elementos consecutivos, entonces s es congruente a $|\text{Des}(\sigma)|$ módulo 2.*

DEMOSTRACIÓN. Se sigue fácilmente de la Proposición 2.7 haciendo inducción en s . \square

TEOREMA 2.9. *La función $\text{sg}: S_n \rightarrow \{-1, 1\}$ es un morfismo sobreyectivo.*

DEMOSTRACIÓN. Por el Corolario 2.8, si $\sigma = \sigma_1 \circ \dots \circ \sigma_s$, donde las σ_i 's son transposiciones de elementos consecutivos, entonces $\text{sg}(\sigma) = (-1)^s$. Usando esta caracterización es muy fácil ver que sg es un morfismo. Además es sobreyectivo porque $\text{sg}(\text{id}) = 1$ y $\text{sg}(1, 2) = -1$. \square

PROPOSICIÓN 2.10. *Si σ es un r -ciclo (i_1, \dots, i_r) , entonces $\text{sg}(\sigma) = (-1)^{r-1}$.*

DEMOSTRACIÓN. Supongamos que σ es el r -ciclo (i_1, \dots, i_r) . Como

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

debido al teorema anterior es suficiente probar que el signo de cada transposición es -1 . Es evidente que esto pasa para las transposiciones $(i, i+1)$ de elementos consecutivos. Supongamos ahora que ya sabemos que el signo de (i, j) es -1 y que $j < n$. Entonces dado que $(i, j+1) = (j, j+1) \circ (i, j) \circ (j, j+1)$ se sigue nuevamente del teorema anterior que también el signo de $(i, j+1)$ es -1 . \square

PROPOSICIÓN 2.11. *Si $\sigma \in S_n$ tiene estructura cíclica $[\alpha_1, \dots, \alpha_n]$, entonces*

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

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

DEMOSTRACIÓN. Escribamos $\sigma = \sigma_1 \circ \dots \circ \sigma_s$, de σ como producto de ciclos disjuntos, donde los primeros α_2 ciclos tienen orden 2, los siguientes α_3 tienen orden 3, etcétera. Por el Teorema 2.9 y la Proposición 2.10

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

como queríamos. \square

Decimos que una permutación es par si su signo es 1 e impar si es -1 . El *grupo alternado* A_n es, por definición, el subgrupo de S_n formado por las permutaciones pares. Como A_n es el núcleo de sg , es un subgrupo normal de orden $n!/2$ de S_n .

OBSERVACIÓN 2.12. La aplicación $\theta: S_n \rightarrow A_{n+2}$, definida por

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

es un morfismo inyectivo de grupos.

PROPOSICIÓN 2.13. Si H es un subgrupo de S_n y $H \not\subseteq A_n$, entonces $H \cap A_n$ 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 $H \cap A_n$ y $\{\text{id}, \sigma\}$. En particular S_n es el producto semidirecto de A_n y $\{\text{id}, (1, 2)\}$.

DEMOSTRACIÓN. Tomemos $\sigma \in H \setminus A_n$. Como la función

$$\begin{array}{ccc} H \cap A_n & \longrightarrow & H \setminus A_n \\ \tau & \longmapsto & \tau \circ \sigma \end{array}$$

es biyectiva, $H \cap A_n$ es un subgrupo de índice 2 de H y, por lo tanto, es normal. Supongamos ahora que σ es una permutación impar de orden dos. Como

$$(H \cap A_n) \cap \{\text{id}, \sigma\} = \{\text{id}\} \quad \text{y} \quad (H \cap A_n)\{\text{id}, \sigma\} = H,$$

el grupo H es el producto semidirecto interno de $H \cap A_n$ y $\{\text{id}, \sigma\}$. □

4. Generadores de A_n

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

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

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 los cuadrados de $(1, 3, 2), (1, 4, 2), \dots, (1, n, 2)$ generan a A_n .

TEOREMA 2.14. Para todo $n \in \mathbb{N}$,

$$A_n = \langle (1, 2, 3), (1, 2, 4), \dots, (1, 2, n) \rangle.$$

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

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

se sigue que A_n está generado por los 3-ciclos. Como, para cada terna a, b, c de elementos de \mathbb{I}_n distintos de 1,

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

para concluir la demostración será suficiente mostrar que cada 3-ciclo $(1, a, b)$ con $a \neq 2$ es producto de 3-ciclos de la forma $(1, 2, i)$ con $3 \leq i \leq n$. Pero esto es así, porque

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

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

COROLARIO 2.15. A_n es un subgrupo completamente normal de S_n .

DEMOSTRACIÓN. Para cada endomorfismo $f: S_n \rightarrow S_n$ y cada 3-ciclo $\tau \in S_n$ el orden de $f(\tau)$ es 1 o 3. Por lo tanto en la descomposición cíclica de $f(\tau)$ sólo hay 3-ciclos y puntos fijos y, en consecuencia, $f(\tau) \in A_n$. \square

TEOREMA 2.16. Para todo $n \in \mathbb{N}$,

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

DEMOSTRACIÓN. Como

$$(1, 2) \circ (2, 3) = (2, 3) \circ (1, 2) \circ (2, 3) \circ (1, 2)$$

y

$$(1, 2) \circ (j, j+1) = (j, j+1) \circ (1, 2) \quad \text{para todo } j > 2,$$

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

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

para todo $j \geq 3$. \square

5. El conmutador y el centro de S_n y A_n

En esta sección calculamos conmutador y el centro de S_n y A_n .

TEOREMA 2.17. $[S_n, S_n] = A_n$ para todo $n \in \mathbb{N}$ y $[A_n, A_n] = A_n$ para todo $n \geq 5$.

DEMOSTRACIÓN. El subgrupo conmutador de S_n está incluido en A_n , porque

$$\text{sg}([\sigma, \tau]) = \text{sg}(\sigma) \text{sg}(\tau) \text{sg}(\sigma^{-1}) \text{sg}(\tau^{-1}) = 1 \quad \text{para todo } \sigma, \tau \in S_n,$$

debido a que $\text{sg}(\sigma) = \text{sg}(\sigma^{-1})$ y $\text{sg}(\tau) = \text{sg}(\tau^{-1})$. Por el Teorema 2.14, para probar que vale la inclusión opuesta será suficiente mostrar que los 3-ciclos son conmutadores, lo cual es cierto, porque de hecho,

$$(a, b, c) = [(a, b), (a, c)] \quad \text{para toda terna } a, b, c \text{ de elementos de } \mathbb{I}_n.$$

Para probar que $[A_n, A_n] = A_n$ para todo $n \geq 5$, es suficiente observar que si $a, b, c, d, e \in \mathbb{I}_n$ son todos distintos, entonces

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

lo que se comprueba por cálculo directo. \square

OBSERVACIÓN 2.18. Como A_2 y A_3 son conmutativos, $[A_i, A_i] = 1$ cuando $i \leq 3$. En cuanto a $[A_4, A_4]$, debido a que el subgrupo

$$H := \{\text{id}, (1, 2) \circ (3, 4), (1, 3) \circ (2, 4), (1, 4) \circ (2, 3)\}$$

de A_4 es normal y A_4/H es abeliano, $[A_4, A_4] \subseteq H$. Por otro lado, las igualdades

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

muestran que la inclusión opuesta también vale.

TEOREMA 2.19. Si $n \geq 3$, entonces $ZS_n = 1$ y si $n \geq 4$, entonces $ZA_n = 1$.

DEMOSTRACIÓN. Primero consideramos el grupo simétrico. Tomemos $\sigma \in S_n$. Si en la descomposición cíclica de σ hay dos ciclos no triviales,

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

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

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

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

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

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

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

Ahora consideramos el grupo alternado. Tomemos $\sigma \in A_n$. 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 $\tau := (i_1, i_2) \circ (i_3, i_4)$ obtenemos

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

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

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

lo que termina la demostración. □

OBSERVACIÓN 2.20. Como S_2, A_2 y A_3 son conmutativos,

$$ZS_2 = S_2 \quad y \quad ZA_i = A_i \quad \text{para } i \in \{2, 3\}.$$

Simplicidad de A_n

Claramente 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 2.21. El grupo alternado A_n es simple para todo $n \geq 3$ y distinto de 4.

DEMOSTRACIÓN. El grupo A_3 es simple porque es cíclico de orden 3. Asumamos entonces que $n \geq 5$ y tomemos un subgrupo normal $H \neq 1$ de A_n . Afirmamos que H contiene a todos los 3-ciclos y que, por lo tanto, es igual a A_n . Veamos primero que H contiene a un 3-ciclo. Para ello fijemos $\sigma \in H$ distinto de la identidad. Si σ es un 3-ciclo no hay nada que probar y si σ tiene un ciclo $(i_1, i_2, i_3, i_4, i_5, \dots, i_r)$ de longitud al menos 4 en su descomposición cíclica, entonces tomando $\tau := (i_1, i_2, i_3)$ obtenemos que H contiene a

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

Podemos suponer entonces que todos los ciclos de la descomposición cíclica de σ tienen longitud menor que 3 y que en esta descomposición hay al menos 2 ciclos.

1. Si $\sigma = (i_1, i_2, i_3) \circ (j_1, j_2, j_3) \circ \dots \circ \sigma = (i_1, i_2) \circ (j_1, j_2, j_3) \circ \dots$ tiene al menos un ciclo de longitud 3 en su descomposición cíclica, entonces tomando $\tau := (i_1, j_1, j_2)$, obtenemos que H contiene a

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

lo que nos reduce al caso ya tratado.

2. Si $\sigma = (i_1, i_2) \circ (i_3, i_4) \circ \dots$ tiene al menos dos ciclos de longitud 2 en su descomposición cíclica, entonces tomando $\tau := (i_1, i_5, i_3)$ con $i_5 \notin \{i_1, i_2, i_3, i_4\}$, obtenemos que

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

está en H , lo que nuevamente nos reduce al caso ya tratado.

Por lo tanto, concluimos 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 2.2, existe $t \in S_n$ tal que $(j_1, j_2, j_3) = t \circ (i_1, i_2, i_3) \circ t^{-1}$. Si $t \in A_n$ 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

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

Como $(k_1, k_2) \circ t \in A_n$, esto implica que $(j_1, j_2, j_3) \in H$. \square

TEOREMA 2.22. 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 $H \cap A_n$ es un subgrupo invariante de A_n y, por el teorema anterior, forzosamente $H \cap A_n = A_n$ o $H \cap A_n = 1$. Como A_n tiene índice 2, en el primer caso $H = A_n$. Para terminar la demostración, debemos ver que la intersección de H con A_n no puede ser 1. Pero si $H \cap A_n = 1$, entonces por la Proposición 2.13, existe $\tau \in S_n$ tal que $H = \{\text{id}, \tau\}$, lo que se contradice con que H es normal pues, como τ tiene orden 2 es un producto de 2-ciclos disjuntos y, en consecuencia, por el Teorema 2.2, su clase de conjugación tiene más de un elemento. \square

Debido a que todo subgrupo de índice 2 de un grupo es invariante, del Teorema 2.21 se sigue que A_n no tiene subgrupos de orden $n!/4$ para ningún $n \geq 5$. El primer ítem 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 2.23. El grupo A_4 tiene las siguientes propiedades:

1. No tiene subgrupos de orden 6.
2. Es el único subgrupo de orden 12 de S_4 .

DEMOSTRACIÓN. 1) Si H es un subgrupo de orden 6 de A_4 , entonces es normal porque tiene índice 2. Pero entonces $\tau^2 \in H$ para todo $\tau \in A_4$ pues la clase de τ^2 en A_4/H es 1. Dado que si τ es un 3-ciclo, $\tau = \tau^4 = (\tau^2)^2$, esto implica que H contiene a todos los 3-ciclos de S_4 , lo que es absurdo porque hay 8.

2) Supongamos que $H \neq A_4$ es un subgrupo de orden 12 de S_4 . Entonces, por la Proposición 2.13, el subgrupo $H \cap A_4$ de A_4 tiene orden 6, lo que se contradice con el ítem 1). \square

6. Presentaciones de S_n y A_n

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

TEOREMA 2.24. *Para cada $n \geq 2$, el grupo simétrico S_n es canónicamente isomorfo al grupo generado por los elementos 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 los elementos s_1, \dots, s_{n-1} sujetos a las relaciones mencionadas arriba. Es evidente que la función $\psi: G \rightarrow S_n$, 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, 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 $j - 1 < n - 1$. 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,

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

y

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

En consecuencia, 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 $|G| \leq \sum_{i=1}^n |C_i| = n|G'| \leq n!$. \square

OBSERVACIÓN 2.25. *Las relaciones que satisfacen s_1, \dots, s_{n-1} pueden expresarse en la forma*

$$\begin{aligned} s_i^2 &= 1, & \text{para todo } i, \\ (s_i s_j)^2 &= 1, & \text{si } j - i \geq 2, \\ (s_i s_{i+1})^3 &= 1, & \text{para } i < n - 1, \end{aligned}$$

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

TEOREMA 2.26. *Para cada $n \geq 3$, el grupo alternado A_n es canónicamente isomorfo al grupo generado por los elementos t_1, \dots, t_{n-2} sujetos a las relaciones*

$$\begin{aligned} t_1^3 &= 1, \\ t_i^2 &= 1, & \text{para } i > 1, \\ (t_i t_j)^2 &= 1, & \text{si } j - i \geq 2, \\ (t_i t_{i+1})^3 &= 1, & \text{para } i < n - 2. \end{aligned}$$

DEMOSTRACIÓN. Consideremos el grupo G generado por los elementos t_1, \dots, t_{n-2} sujetos a las relaciones mencionadas arriba. Es evidente que la función

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

se extiende univocamente a un morfismo $\psi: G \rightarrow A_n$. Como, por el Teorema 2.16, este morfismo es sobreyectivo, para terminar la demostración será suficiente ver que $|G| \leq n!/2$. Probaremos esto mostrando que hay un producto semidirecto $G \times_{\vartheta} \mathbb{Z}_2$ y un morfismo sobreyectivo $S_n \rightarrow G \times_{\vartheta} \mathbb{Z}_2$. Para empezar, es fácil ver que la función $\vartheta: \mathbb{Z}_2 \rightarrow \text{Aut}(G)$, dada por $\vartheta(1)(t_i) := t_i^{-1}$, es un morfismo bien definido. Por ejemplo, la relación $(t_1 t_2)^3 = 1$ se transforma por $\vartheta(1)$ en la relación $(t_1^{-1} t_2^{-1})^3 = 1$, la cual vale porque

$$t_1 t_2 t_1 t_2 t_1 t_2 = 1 \Rightarrow t_2^{-1} t_1^{-1} t_2^{-1} t_1^{-1} t_2^{-1} t_1^{-1} = 1 \Rightarrow t_1^{-1} t_2^{-1} t_1^{-1} t_2^{-1} t_1^{-1} t_2^{-1} = 1.$$

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

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

y escribamos $s_{i+1} = t_i s_1$ para $1 \leq i < n - 1$. Las relaciones dadas arriba para s_1, t_1, \dots, t_{n-2} son equivalentes a las dadas en la Observación 2.25 para s_1, \dots, s_{n-1} . Por lo tanto,

$$G' = \langle s_1, t_1, \dots, t_{n-2} \rangle = \langle s_1, \dots, s_{n-1} \rangle \simeq S_n.$$

Por consiguiente, para terminar la demostración es suficiente notar que existe un morfismo de grupos $\varphi: G' \rightarrow G \times_{\vartheta} \mathbb{Z}_2$, tal que $\varphi(t_i) = (t_i, 0)$ y $\varphi(s_1) = (0, 1)$, puesto que este necesariamente será sobreyectivo. \square

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

$$\rho: G \times X \rightarrow X$$

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

$$\rho: X \times G \rightarrow X$$

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 $\rho: X \times G \rightarrow X$ es una acción a derecha de G sobre X si y sólo si la función $\rho^{\text{op}}: G^{\text{op}} \times X \rightarrow X$, definida por $\rho^{\text{op}}(g, x) := \rho(x, g)$, 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 $\rho: G \times X \rightarrow X$ es “lo mismo” que tener una función $\tilde{\rho}: G \rightarrow \text{Fun}(X, X)$. Dicho en forma más precisa, la correspondencia

$$\begin{array}{ccc} \text{Fun}(G \times X, X) & \longrightarrow & \text{Fun}(G, \text{Fun}(X, X)) \\ \rho \longmapsto & & \tilde{\rho} \end{array}$$

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

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

En particular

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

Por lo tanto, dar una acción de G sobre X es equivalente a dar un morfismo de G en S_X .

2. Núcleo de una acción, teorema de Cayley y aplicaciones

El *núcleo de una acción* $\rho: G \times X \rightarrow X$ 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

$$\tilde{\rho}: G \rightarrow S_X$$

asociado a ρ . Una acción es *fiel* si su núcleo es 1. En este caso el morfismo asociado $\tilde{\rho}: G \rightarrow S_X$ es inyectivo y, por lo tanto, G es isomorfo a un subgrupo de S_X . Para cada acción

$$\rho: G \times X \rightarrow X$$

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

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

Se comprueba fácilmente que el triángulo

$$\begin{array}{ccc} G & \xrightarrow{\tilde{\rho}} & S_X \\ \pi \downarrow & \nearrow \tilde{\bar{\rho}} & \\ \frac{G}{\ker \rho} & & \end{array},$$

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 sobre el conjunto G/L , de las coclases a izquierda de un subgrupo L de G , vía traslaciones a izquierda. En otras palabras, $g \cdot (hL) = ghL$. El núcleo de esta acción es el máximo subgrupo*

$$N := \bigcap_{h \in G} hLh^{-1}$$

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

TEOREMA 3.2 (Cayley). *La función*

$$\begin{aligned} G &\longrightarrow S_G \\ g &\longmapsto l_g \end{aligned}$$

es un morfismo inyectivo.

DEMOSTRACIÓN. Tómese $L = 1$ en el ejemplo anterior. \square

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 de S_n y, como vimos en la Sección 2 del Capítulo 2, el grupo simétrico S_n está generado por los ciclos $(1, 2)$ y $(1, \dots, n)$. \square

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

DEMOSTRACIÓN. Por el teorema de Cayley y la Observación 2.12, sabemos que G es isomorfo a un subgrupo de A_n , para un $n \geq 5$. Para terminar la demostración basta observar que por el Teorema 2.21, el grupo alternado A_n es simple. \square

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 esencial 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 $l_g \in S_G$ 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 $2^{k'} m'$. 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 $k' = k \geq 1$. \square

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 incluido en A_G . En este caso el resultado se sigue inmediatamente de la Proposición 2.13. \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

$$\begin{aligned} G &\longrightarrow S_{G/L} \ , \\ g &\longmapsto l_g \end{aligned}$$

asociado a la acción de G sobre G/L vía traslaciones a izquierda, induce un morfismo inyectivo de G/N en $S_{G/L}$, donde $N := \bigcap_{g \in G} gLg^{-1}$. Por consiguiente el índice de N en G es menor que infinito y divide a $|S_{G/L}| = |G : L|!$. 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 $S_{G/L}$ que manda g en l_g .*

El Teorema 3.8 generaliza el teorema de Cayley. También generaliza la Proposición 1.51, porque cuando $n = 2$, entonces $h = 1$ y $N = L$.

COROLARIO 3.9. *Si un grupo G tiene un subgrupo de índice finito $n > 1$ que no contiene a ningún subgrupo normal de G distinto de 1, entonces $|G| = nh$ con h un divisor de $(n-1)!$. Además hay un morfismo inyectivo de G en S_n .*

DEMOSTRACIÓN. Porque debido a la hipótesis el subgrupo normal N de G mencionado en el Teorema 3.8 necesariamente es 1. \square

COROLARIO 3.10. *Si un grupo simple G tiene un subgrupo de índice finito $n > 1$, entonces $|G| = nh$ con h un divisor de $(n-1)!$. Además hay un morfismo inyectivo de G en S_n .*

DEMOSTRACIÓN. Se sigue inmediatamente del corolario anterior. \square

Notemos que, debido a la Proposición 2.13, si $n > 2$, entonces la imagen del morfismo inyectivo de G en S_n , mencionado en el corolario anterior, está incluida en A_n .

COROLARIO 3.11. *Los grupos infinitos simples no tienen subgrupos propios de índice finito.*

COROLARIO 3.12. *Supongamos que G es un grupo finito y que $|G| = nm$. Todo subgrupo H 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 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 $n \neq 4$, entonces S_n no tiene subgrupos de índice t con $2 < t < n$. Pruebe también que esto es falso si $n = 4$.*

EJEMPLO 3.15. *Recordemos que el grupo diedral D_n tiene orden $2n$ y está generado por dos elementos x e y sujetos las relaciones $x^n = y^2 = yxy^{-1}x = 1$. Supongamos que $n > 2$. Como en este caso $\langle y \rangle$ tienen orden 2 y no es normal en D_n , la acción de D_n en $D_n/\langle y \rangle$ definida via traslaciones a izquierda es fiel. Por lo tanto hay un morfismo inyectivo de D_n en S_n (lo que ya fue obtenido en el Ejemplo 2.6).*

3. Subconjuntos estables y morfismos

Decimos que un subconjunto Y de un G -espacio X es *estable bajo la acción de G* o simplemente *estable* si $g \cdot y \in Y$ para todo $g \in G$ e $y \in Y$. En este caso Y en si mismo es un G -espacio con la acción inducida y, debido a eso, decimos también que Y es un G -subespacio de X .

Un morfismo $\varphi: X \rightarrow X'$, de un G -espacio X en otro X' , es una terna (X, φ, X') , donde φ es una función de X en X' que satisface

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

En términos de los morfismos $\tilde{\rho}: G \rightarrow S_X$ y $\tilde{\rho}': G \rightarrow S_{X'}$ inducidos por las acciones de G sobre X y X' respectivamente, esta condición queda

$$\varphi \circ \tilde{\rho}(g) = \tilde{\rho}'(g) \circ \varphi \quad \text{para todo } g \in G.$$

Por ejemplo, la identidad $\text{id}: X \rightarrow X$ y, más generalmente, la inclusión canónica $i: Y \rightarrow X$, de un subconjunto estable Y de un G -espacio X en X , es un morfismo de G -espacios. También lo es la composición $\psi \circ \varphi: X \rightarrow X''$ de dos morfismos de G -espacios $\varphi: X \rightarrow X'$ y $\psi: X' \rightarrow X''$.

Las definiciones de endomorfismo, isomorfismo, G -espacios isomorfos, automorfismo, monomorfismo, epimorfismo, sección y retracción son las idénticas a las dadas para monoides y grupos, y las propiedades básicas son las mismas. Los monomorfismos, epimorfismos, secciones y retracciones son cerrados bajo la composición, toda retracción es sobreyectiva, toda sección inyectiva, todo morfismo inyectivo un monomorfismo, y todo morfismo sobreyectivo un epimorfismo. Un morfismo $\varphi: X \rightarrow X'$ es un isomorfismo si y sólo si es biyectivo.

Dados G -espacios X y X' , designaremos con los símbolos $\text{Hom}_G(X, X')$, $\text{Iso}_G(X, X')$, $\text{End}_G(X)$ y $\text{Aut}_G(X)$ 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, $\text{End}_G(X)$ es un monoide (cuyo elemento neutro es la función identidad) vía la composición y $\text{Aut}_G(X)$ es su grupo de unidades.

OBSERVACIÓN 3.16. *Si X es un G -espacio y $\sigma: X \rightarrow X'$ es una función, entonces hay una única acción de G sobre X' que convierte a σ en un isomorfismo de G -espacios. En efecto, si este es el caso, entonces*

$$g \cdot x' = \sigma(\sigma^{-1}(g \cdot x')) = \sigma(g \cdot \sigma^{-1}(x'))$$

y es fácil ver que esta igualdad define una tal acción de G sobre X' , que diremos es obtenida a partir de la acción de G sobre X por traslación de estructura.

4. Más ejemplos

Hasta ahora hemos visto un sólo ejemplo de acción de un grupo sobre un conjunto, el dado por la acción, vía traslaciones a izquierda, de un grupo G sobre el conjunto G/L , de las coclases a izquierda de un subgrupo L . El objetivo de esta breve subsección es proveernos de muchos otros.

EJEMPLO 3.17. *Cada conjunto X es un G -espacio vía la acción trivial $g \cdot x := x$.*

EJEMPLO 3.18. *G actúa sobre si mismo por conjugación. Esto es, $g \cdot h := ghg^{-1}$. Más generalmente, G actúa por conjugación sobre cada uno de sus subgrupos normales N . El núcleo de esta acción es $C_G(N)$.*

EJEMPLO 3.19. Si N y K son subgrupos de un grupo G y $K \subseteq N_G(N)$, entonces K actúa sobre N por conjugación. El núcleo de esta acción es $K \cap C_G(N)$. Cuando $K = G$ nos reducimos al Ejemplo 3.18.

EJEMPLO 3.20. Todo subgrupo H de un grupo G actúa fielmente sobre G por traslaciones a izquierda. En símbolos, $h \cdot g := hg$ para todo $h \in H$ y $g \in G$. Más generalmente el subgrupo H actúa sobre G/L para cada subgrupo L de G vía $h \cdot gL := hgL$. El núcleo de esta acción es $H \cap \bigcap_{h \in G} hLh^{-1}$.

EJEMPLO 3.21. G actúa sobre el conjunto $P(G)$, de partes de G , por conjugación. Esto es, $g \cdot S := gSg^{-1}$. El núcleo de esta acción es ZG .

EJEMPLO 3.22. El subconjunto $\text{Sub}(G)$ de $P(G)$ de los subgrupos de G es estable por la acción del ejemplo anterior y, así, G también actúa sobre $\text{Sub}(G)$ por conjugación. El núcleo de esta acción es $\bigcap_{H \in \text{Sub}(G)} N_G(H)$.

EJEMPLO 3.23. La clase de conjugación de un subgrupo L de G es un G -espacio via

$$g \cdot hLh^{-1} := ghLh^{-1}g^{-1}.$$

El núcleo de esta acción es $\bigcap_{h \in G} N_G(hLh^{-1})$.

EJEMPLO 3.24. G actúa fielmente sobre $P(G)$ vía $g \cdot S := gS$. Esto es, por traslaciones a izquierda.

EJEMPLO 3.25. G actúa sobre el conjunto $G \setminus L$ de las coclases a derecha de un subgrupo L de G vía $g \cdot (Lh) := Lhg^{-1}$. El núcleo de esta acción es $\bigcap_{h \in G} hLh^{-1}$.

EJEMPLO 3.26. S_n actúa fielmente 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 3.27. S_n actúa sobre el producto cartesiano $X \times \dots \times X$ de n copias de un conjunto arbitrario X , via

$$\sigma \cdot (x_1, \dots, x_n) := (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)}).$$

EJEMPLO 3.28. Cada subgrupo G de $GL(V)$ actúa fielmente sobre V vía $g \cdot v := g(v)$. Esta es la acción natural de G sobre V .

EJEMPLO 3.29. El grupo ortogonal $O(\mathbb{R}^n)$ actúa fielmente sobre la esfera

$$S^{n-1} := \{x \in \mathbb{R}^n : \|x\| = 1\},$$

via $g \cdot x := g(x)$.

EJEMPLO 3.30. La acción natural de S_X sobre X es la definida por $\sigma \cdot x := \sigma(x)$.

EJEMPLO 3.31. Para cada par de grupos G y N hay una acción de G en $\text{Hom}(N, G)$, que está dada por $(g \cdot f)(n) := gf(n)g^{-1}$, para todo $g \in G$, $f \in \text{Hom}(N, G)$ y $n \in N$.

OBSERVACIÓN 3.32. Tomemos un grupo G y consideremos a $\text{Hom}(G, S_n)$ con la acción de S_n obtenida en el último ejemplo. Para cada $f \in \text{Hom}(G, S_n)$ denotemos con \mathbb{I}_n^f al conjunto \mathbb{I}_n provisto de la acción de G determinada por f . Tomemos $\sigma \in S_n$. Como

$$\sigma \circ f(g) = (\sigma \cdot f)(g) \circ \sigma \quad \text{para todo } g \in G,$$

la aplicación

$$\sigma: \mathbb{I}_n^f \rightarrow \mathbb{I}_n^{\sigma \cdot f}$$

es un isomorfismo de G -espacios. En consecuencia queda definida una aplicación del conjunto de las órbitas de $\text{Hom}(G, S_n)$ en el conjunto de las clases de isomorfía de G -espacios de n elementos, que a la órbita que contiene a f le asigna la clase que contiene a \mathbb{I}_n^f . Esta aplicación es inyectiva pues si $\sigma: \mathbb{I}_n^f \rightarrow \mathbb{I}_n^{f'}$ es un isomorfismo de G -espacios, entonces

$$\sigma \circ f(g) = f'(g) \circ \sigma \quad \text{para todo } g \in G$$

y así, $f' = \sigma \circ f$. Pero también es sobreyectiva pues si X es un G -espacio de n elementos, entonces tomando una biyección $\sigma: X \rightarrow \mathbb{I}_n$, obtenemos por traslación de estructura, una acción de G sobre \mathbb{I}_n que convierte a σ en un isomorfismo de G -espacios.

5. Órbitas, puntos fijos y estabilizadores

Dos elementos x e y de un G -espacio X son *conjugados* si existe $g \in G$ tal que $g \cdot x = y$. Se comprueba fácilmente que la relación \sim , definida por $x \sim y$ si x e y son conjugados, es de equivalencia. Por consiguiente determina una partición de X en clases llamadas *clases de conjugación* u *órbitas*. Denotamos con \mathcal{O}_x a la órbita que contiene a x y con $\mathcal{O}X$ o X/G al conjunto de todas las órbitas de X . Por definición

$$\mathcal{O}_x = \{g \cdot x : g \in G\}$$

y $\mathcal{O}_x = \mathcal{O}_y$ si y sólo si x e y son conjugados.

Es evidente que si consideramos a X/G provisto de la acción trivial de G , entonces la aplicación canónica $\pi: X \rightarrow X/G$, definida por $\pi(x) := \mathcal{O}_x$, es un morfismo de G -espacios. Además para cada G -morfismo $f: X \rightarrow Y$, de X en un conjunto Y provisto de la acción trivial de G , existe un único G -morfismo $\bar{f}: X/G \rightarrow Y$ tal que $f = \bar{f} \circ \pi$.

Para cada subconjunto H de G denotamos con X^H al conjunto de los puntos de X que son dejados fijos por H . En símbolos

$$X^H := \{x \in X : h \cdot x = x \text{ para todo } h \in H\}.$$

Decimos que $x \in X$ es un *punto fijo* si $g \cdot x = x$ para todo $g \in G$, es decir si $x \in X^G$ o, equivalentemente, si $\mathcal{O}_x = \{x\}$. Claramente un subconjunto de X es un G -subespacio si y sólo si es una unión de órbitas. Supongamos que X' es un conjunto de representantes de las clases de conjugación de X . Es decir, que para cada $x \in X$ la intersección $X' \cap \mathcal{O}_x$ tiene exactamente un elemento. Notemos que X^G , está incluido en X' . Es obvio que

$$(23) \quad |X| = \sum_{x \in X'} |\mathcal{O}_x| = |X^G| + \sum_{x \in X' \setminus X^G} |\mathcal{O}_x|.$$

Decimos que la acción de un grupo G sobre un conjunto X es *transitiva* o que G *opera transitivamente* sobre X si tiene una sólo órbita. Por ejemplo la acción de un grupo G sobre el conjunto G/L de las coclases a izquierda de uno de sus subgrupos L , dada por traslaciones a izquierda, es transitiva. El *estabilizador* o *grupo de isotropía* de un elemento x de X es el conjunto

$$G_x := \{g \in G : g \cdot x = x\}.$$

Es evidente que G_x es un subgrupo de G y que el núcleo de la acción de G sobre X es la intersección de los estabilizadores de todos los elementos de X .

A continuación calculamos los estabilizadores en algunos de los ejemplos introducidos en la subsección anterior.

EJEMPLO 3.33. *Para el caso de la acción de un grupo G sobre el conjunto G/L de las clases a izquierda de uno de sus subgrupos L dada por traslaciones a izquierda, el estabilizador de cada hL es hLh^{-1} . Esta acción no tiene puntos fijos a menos que L sea G .*

EJEMPLO 3.34. *Para el caso de la acción de un grupo G sobre uno de sus subgrupos normales N dada por conjugación, el estabilizador de cada $n \in N$ es $C_G(n)$. Más generalmente si N y K son subgrupos de G tales que $K \subseteq N_G(N)$ y K actúa sobre N por conjugación, entonces el estabilizador de cada $n \in N$ es $K \cap C_G(n)$.*

EJEMPLO 3.35. *En el caso de la acción de un grupo G sobre $P(G)$ dada por conjugación, el estabilizador de cada subconjunto S de G es $N_G(S)$. Un subconjunto S de G es un punto fijo para esta acción si y sólo si $gSg^{-1} = S$ para todo $g \in G$.*

PROPOSICIÓN 3.36. *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} . \square

COROLARIO 3.37. *Si x e y están en la misma órbita, entonces sus estabilizadores son isomorfos.*

OBSERVACIÓN 3.38. *Supongamos que X es un G -espacio y tomemos $x \in X$. Por la Proposición 3.36, para cada H conjugado a G_x existe $y \in \mathcal{O}_x$ tal que $G_y = H$. En consecuencia, por los comentarios que preceden a la Observación 1.176,*

$$N = \bigcap_{y \in \mathcal{O}_x} G_y$$

es el máximo subgrupo normal de G_x .

PROPOSICIÓN 3.39. *Si $f: X \rightarrow Y$ es un morfismo de G -espacios, entonces $G_x \subseteq G_{f(x)}$ para todo $x \in X$. Además si f es inyectivo, entonces elementos de órbitas distintas de X van a parar a órbitas distintas de Y y $G_x = G_{f(x)}$ para todo $x \in X$.*

DEMOSTRACIÓN. Si $g \in G_x$, entonces

$$g \cdot f(x) = f(g \cdot x) = f(x)$$

y, así, $g \in G_{f(x)}$. Supongamos ahora que f es inyectiva y que $f(x)$ y $f(x')$ están en la misma órbita. Entonces existe $g \in G$ tal que $g \cdot f(x) = f(x')$ y, de la igualdad

$$f(g \cdot x) = g \cdot f(x) = f(x')$$

se sigue que $g \cdot x = x'$. Por último si f es inyectiva y $g \in G_{f(x)}$, entonces de la igualdad

$$f(g \cdot x) = g \cdot f(x) = f(x)$$

obtenemos inmediatamente que $g \in G_x$. \square

TEOREMA 3.40. *Consideremos dos G -espacios X e Y , un subconjunto X' de representantes de las clases de conjugación de X y una familia $(y_x)_{x \in X'}$ de elementos de Y . Son equivalentes:*

1. Hay un único morfismo de G -espacios $\Phi: X \rightarrow Y$, tal que $\Phi(x) = y_x$ para todo $x \in X'$.
2. Hay un morfismo de G -espacios $\Phi: X \rightarrow Y$, tal que $\Phi(x) = y_x$ para todo $x \in X'$.
3. $G_x \subseteq G_{y_x}$ para todo $x \in X'$.

Además f es inyectivo si y sólo si todos los y_x 's están en órbitas distintas y $G_x = G_{y_x}$ para todo $x \in X'$.

DEMOSTRACIÓN. Es evidente que 1) implica 2) y debido a la proposición anterior también que 2) implica 3) y que se satisface la parte "sólo si" de la afirmación adicional. Veamos que 3) implica 1). Notemos que si Φ existe, entonces

$$\Phi(g \cdot x) = g \cdot y_x \quad \text{para todo } x \in X',$$

y, por lo tanto, es único. Para terminar la demostración, sólo debemos ver que esta definición de Φ es correcta, lo cual se sigue inmediatamente de que

$$g \cdot x = g' \cdot x \implies \text{existe } h \in G_x \text{ tal que } g' = gh \implies g' \cdot y_x = g \cdot (h \cdot y_x) = g \cdot y_x,$$

para todo $x \in X'$. Resta probar que si todos los y_x 's están en órbitas distintas y $G_x = G_{y_x}$ para todo $x \in X'$, entonces $\Phi: X \rightarrow Y$ es inyectiva. Para ello tomemos $z, z' \in X$ tales que $f(z) = f(z')$ y escribamos $z = g \cdot x$ y $z' = g' \cdot x'$ con $x, x' \in X'$ y $g, g' \in G$. Como $f(z)$ y $f(z')$ están en la órbita de y_x y de $y_{x'}$ respectivamente, de la igualdad $f(z) = f(z')$ se sigue que $x = x'$. Por lo tanto

$$g \cdot y_x = f(z) = f(z') = g' \cdot y_{x'} = g' \cdot y_x$$

de donde existe $h \in G_{y_x}$ tal que $g' = gh$. Pero entonces

$$z' = g' \cdot x' = gh \cdot x' = gh \cdot x = g \cdot x = z,$$

pues, debido a la hipótesis, $h \in G_x$. □

OBSERVACIÓN 3.41. Un morfismo de G -espacios $f: X \rightarrow Y$ es isovariante si $G_x = G_{f(x)}$ para todo $x \in X$. Debido a la Proposición 3.39 y al Teorema 3.40 son equivalentes:

1. $f: X \rightarrow Y$ es isovariante.
2. La restricción de f a cada órbita de X es inyectiva.
3. Existe un conjunto de representantes X' de las clases de conjugación de X tal que

$$G_x = G_{f(x)} \quad \text{para todo } x \in X'.$$

OBSERVACIÓN 3.42. Del Teorema 3.40 se sigue inmediatamente que hay una correspondencia biyectiva entre X^H y el conjunto de los morfismos de G -espacios de G/H en X , que a cada $x \in X^H$ le asigna el único morfismo $f: G/H \rightarrow X$ tal que $f(H) = x$. Notemos además que f siempre es sobreyectivo y que es inyectivo si y sólo si $G_x = H$.

EJEMPLO 3.43. Como

$$(G/H)^H = \{lH : H \subseteq lHl^{-1}\}$$

hay un morfismo de G -espacios $f: G/H \rightarrow G/H$ tal que $f(H) = lH$ si y sólo si $H \subseteq lHl^{-1}$. Además este morfismo es inyectivo si y sólo si $H = lHl^{-1}$. Notemos que si H es finito esto es trivial y así, en este caso, $(G/H)^H = N_G(H)/H$.

COROLARIO 3.44. Para cada G -espacio X y cada $x \in X$, hay un isomorfismo de G -espacios $\Phi: G/G_x \rightarrow \mathcal{O}_x$, tal que $\Phi(gG_x) = g \cdot x$ para cada $g \in G$. En consecuencia $|\mathcal{O}_x| = |G : G_x|$ para cada $x \in X$.

Por ejemplo para cada elementos h de G y cada subgrupo H de G ,

$$|G : C_G(h)| = |\{ghg^{-1} : g \in G\}| \quad \text{y} \quad |G : N_G(H)| = |\{gHg^{-1} : g \in G\}|.$$

Como aplicación del corolario anterior obtenemos la siguiente

PROPOSICIÓN 3.45. *Si k es un cuerpo finito con q elementos, entonces*

$$|\mathrm{GL}(n, k)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) = q^{n(n-1)/2} (q^n - 1)(q^{n-1} - 1) \cdots (q - 1).$$

DEMOSTRACIÓN. Procedemos por inducción en n . Es claro que $\mathrm{GL}(1, k) = k^*$ tiene $q - 1$ elementos. Supongamos que el resultado vale para n . Designemos con el símbolo ${}^t k^{n+1}$ al espacio de los vectores columna de $n + 1$ coordenadas y con e_1 al primer elemento de la base canónica de ${}^t k^{n+1}$. Como la acción natural de $\mathrm{GL}(n + 1, k)$ sobre ${}^t k^{n+1} \setminus \{0\}$ es transitiva, por el Corolario 3.44,

$$q^{n+1} - 1 = |k^{n+1} \setminus \{0\}| = \frac{|\mathrm{GL}(n + 1, k)|}{|\mathrm{GL}(n + 1, k)_{e_1}|}.$$

Es fácil ver que $\mathrm{GL}(n + 1, k)_{e_1}$ es el conjunto de las matrices cuya primera columna es e_1 y, usando esto, que $|\mathrm{GL}(n + 1, k)_{e_1}| = q^n |\mathrm{GL}(n, k)|$. Así, por hipótesis inductiva

$$|\mathrm{GL}(n + 1, k)| = (q^{n+1} - 1)q^n |\mathrm{GL}(n, k)| = (q^{n+1} - 1)(q^{n+1} - q) \cdots (q^{n+1} - q^n),$$

como queríamos. \square

Veamos otra aplicación del Corolario 3.44.

OBSERVACIÓN 3.46. *Fijemos un elemento h de un grupo G . Es obvio que $\langle h \rangle \subseteq C_G(h)$. Además, por el Corolario 3.44 y el teorema de Lagrange,*

$$|G| = |\{ghg^{-1} : g \in G\}| |C_G(h)|.$$

Por ejemplo, esta fórmula combinada con la (21) debida a Cauchy, nos dice que

$$(24) \quad |C_{S_n}(\sigma)| = 1^{\alpha_1} \alpha_1! 2^{\alpha_2} \alpha_2! \cdots n^{\alpha_n} \alpha_n! \quad \text{para cada permutación } \sigma,$$

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 (24), concluimos que $C_{S_n}(\sigma) = \langle \sigma \rangle$ si y sólo si los órdenes de sus ciclos son coprimos dos a dos (en particular, son todos distintos).

EJERCICIO 3.47. *Supongamos que G es un grupo simple infinito. Pruebe que:*

1. Si $g \in G$ es distinto de 1, entonces la clase de conjugación de g es un conjunto infinito.
2. Si H es un subgrupo no trivial de G , entonces la clase de conjugación de H es un conjunto infinito.

Por último damos dos aplicaciones del Corolario 3.44 que son algo más teóricas que las anteriores.

PROPOSICIÓN 3.48. *Si un subgrupo de un grupo finito G contiene algún elemento de cada clase de conjugación de G , entonces coincide con G .*

DEMOSTRACIÓN. Tomemos un subgrupo propio L de G y consideremos la acción de G sobre $\text{Sub}(G)$ dada por conjugación. Dado que por el Corolario 3.44

$$\left| \bigcup gLg^{-1} \right| \leq |G : N_G(L)|(|L| - 1) + 1 \leq |G : L|(|L| - 1) + 1 = |G| - |G : L| + 1,$$

existe $h \in G$ tal que $h \notin gLg^{-1}$ para ningún $g \in G$ o, lo que es claramente equivalente, que L no corta a la clase de conjugación de h . \square

Por supuesto que en general el teorema de Cayley no es óptimo. Vamos a ver un caso en el que sí lo es. Un subgrupo H de un grupo G es minimal si $H \neq 0$ y $L \leq H$ implica $L = 1$ o $L = H$. Es claro que no todo grupo no trivial tiene subgrupos minimales. Por ejemplo \mathbb{Z} no los tiene. Sin embargo es muy fácil ver que todo grupo finito y no trivial contiene subgrupos minimales. Por último es claro también que si H es un subgrupo minimal de G y $\varphi: G \rightarrow G$ es un automorfismo, entonces $\varphi(H)$ también es un subgrupo minimal de G . En particular si un grupo tiene un único subgrupo minimal, este necesariamente es característico.

PROPOSICIÓN 3.49. *Si G es un grupo finito que tiene un único subgrupo minimal y X es un G -espacio fiel, entonces $|X| \geq |G|$.*

DEMOSTRACIÓN. Denotemos con H al único subgrupo minimal de G . Afirmamos que existe $x \in X$ tal que $G_x = 1$. En efecto, en caso contrario $H \subseteq G_x$ para todo $x \in X$, lo que se contradice con que el núcleo $\bigcap_{x \in X} G_x$, de la acción de G sobre X que estamos considerando es 1. En consecuencia $|X| \geq |\mathcal{O}_x| = |G|$. \square

Notemos que el grupo cuaterniónico H_{2^m} satisface la hipótesis del teorema anterior. Otro ejemplo es \mathbb{Z}_{p^r} , donde $p, r \in \mathbb{N}$ y p es primo. En consecuencia si S_n tiene un subgrupo isomorfo a H_{2^m} , entonces $n \geq 2^{m+1}$ y si S_n tiene un subgrupo isomorfo a \mathbb{Z}_{p^r} , entonces $n \geq p^r$. Dado que D_{p^r} contiene a un subgrupo isomorfo a \mathbb{Z}_{p^r} , se sigue de esto que si S_n tiene un subgrupo isomorfo a D_{p^r} , entonces $n \geq p^r$.

5.1. La ecuación de las clases

Combinando el Corolario 3.44 con la fórmula (23), obtenemos que

$$(25) \quad |X| = |X^G| + \sum_{x \in X' \setminus X^G} |G : G_x|,$$

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.

Acción de G sobre sí mismo por conjugación: En este caso la fórmula (25) da la llamada *ecuación de las clases*

$$|G| = |ZG| + \sum_{g \in X' \setminus ZG} |G : C_G(g)|,$$

en la cual X' es un conjunto de representantes de las clases de conjugación de G .

Acción de G sobre un subgrupo normal N por conjugación: En este se reduce a la igualdad

$$|N| = |N \cap ZG| + \sum_{g \in X' \setminus ZG} |G : C_G(g)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de G incluidas en N .

Acción de G sobre $\text{Sub}(G)$ por conjugación: Dado que en este caso $\text{Sub}(G)^G$ es el subconjunto $\text{SubN}(G)$ de $\text{Sub}(G)$ formado por los subgrupos normales de G y que $G_H = N_G(H)$ para todo subgrupo H de G , la fórmula (25) deviene

$$|\text{Sub}(G)| = |\text{SubN}(G)| + \sum_{H \in X' \setminus \text{SubN}(G)} |G : N_G(H)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de $\text{Sub}(G)$.

Acción de G sobre $\text{P}(G)$ por conjugación: En este caso la fórmula (25) se transforma en

$$2^{|G|} = |\text{PaN}(G)| + \sum_{S \in X' \setminus \text{PaN}(G)} |G : N_G(S)|,$$

donde X' es un conjunto de representantes de las órbitas de $\text{P}(G)$ y $\text{PaN}(G)$ es el conjunto de los subconjuntos S de G tales que $gSg^{-1} = S$ para todo $g \in G$.

A continuación usamos la ecuación de las clases para probar que para ningún $n \in \mathbb{N}$ hay una cantidad infinita de grupos finitos con exactamente n clases de conjugación.

LEMA 3.50. *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 $i_1 \leq \dots \leq i_n$ y $q = \sum_{j=1}^n 1/i_j$. Pero esto es cierto, porque en cada una de estas n -uplas $i_1 \leq n/q$ y, por la hipótesis inductiva, para cada número natural $k \leq n/q$ sólo hay una cantidad finita de $(n - 1)$ -uplas (i_2, \dots, i_n) que satisfacen $q - 1/k = \sum_{j=2}^n 1/i_j$. \square

TEOREMA 3.51. *Para cada $n \geq 1$, sólo hay una cantidad finita de grupos finitos que tienen exactamente 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 $g \in ZG$. Por otra parte, por el Lema 3.50, dicho valor está acotado por un $M > 0$. En consecuencia $|G| \leq M$, y para concluir la demostración basta notar que sólo hay finitos grupos no isomorfos de orden menor o igual que M . \square

5.2. k -transitividad

Consideremos un G -espacio X y un entero positivo k . Decimos que la acción de G sobre X es k -transitiva o que G opera k -transitivamente sobre X , si para cada par $\{x_1, \dots, x_k\}$ e $\{y_1, \dots, y_k\}$ de subconjuntos 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 3.52. *La acción natural de S_n sobre \mathbb{I}_n es n -transitiva. Afirmamos que la acción de A_n sobre \mathbb{I}_n inducida por ella es $n - 2$ transitiva. En efecto, para cada par $\{x_1, \dots, x_{n-2}\}$ e $\{y_1, \dots, y_{n-2}\}$ de subconjuntos de $n - 2$ elementos de \mathbb{I}_n , existe $\sigma \in S_n$ tal que $\sigma(x_i) = y_i$ para todo i . Si $\sigma \in A_n$ ya está. Si no, tomando $z_1, z_2 \in X \setminus \{y_1, \dots, y_{n-2}\}$ y considerando $\sigma' := (z_1, z_2) \circ \sigma$ obtenemos una permutación par σ' que también satisface $\sigma'(x_i) = y_i$.*

PROPOSICIÓN 3.53. *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, para cada par $\{x_1, \dots, x_{k-1}\}$ e $\{y_1, \dots, y_{k-1}\}$ de subconjuntos de $k - 1$ elementos de $X \setminus \{x\}$, existe $g \in G$ tal que $g \cdot x = x$ y $g \cdot x_1 = y_1, \dots, g \cdot x_{k-1} = y_{k-1}$. 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 $(g^{-1}h) \cdot x_1 = y_1, \dots, (g^{-1}h) \cdot x_k = y_k$. \square

5.3. Contando órbitas

Recordemos que para cada G -espacio X el símbolo $\mathcal{O}X$ denota al conjunto de órbitas de la acción y que para cada elemento g de G designamos con X^g al conjunto $\{x \in X : g \cdot x = x\}$ formado por los puntos de X que son dejados fijos por g . El siguiente resultado es conocido como lema de Burnside, pero es debido a Frobenius.

TEOREMA 3.54. *Para cada G -espacio X , los cardinales de los conjuntos X^g y $\mathcal{O}X$ están relacionados por la siguiente igualdad:*

$$|\mathcal{O}X||G| = \sum_{g \in G} |X^g|.$$

DEMOSTRACIÓN. En $\sum_{g \in G} |X^g|$ cada $x \in X$ es contado $|G_x|$ veces (pues G_x consiste de todos los $g \in G$ tales que $x \in X^g$). Puesto que $|G_x| = |G_y|$ siempre que x e y están en la misma órbita, y que la órbita de x tiene $|G : G_x|$ elementos, en la suma de arriba los elementos de $\mathcal{O}X$ aportan en total el valor $|G| = |G : G_x||G_x|$. Recorriendo todas las órbitas de X obtenemos que $|\mathcal{O}X||G| = \sum_{g \in G} |X^g|$, como queremos. \square

EJEMPLO 3.55. *La cantidad de clases de conjugación de un grupo finito G es igual a*

$$\frac{1}{|G|} \sum_{g \in G} |C_G(g)|,$$

En efecto, para la acción de G sobre si mismo vía conjugación,

$$G^g = \{h \in G : ghg^{-1} = h\} = \{h \in G : hgh^{-1} = g\} = C_G(g).$$

COROLARIO 3.56. Si G es un grupo finito y X es un G -espacio transitivo con más de un elemento, entonces existe $g \in G$ tal que $X^g = \emptyset$.

DEMOSTRACIÓN. Como X es transitivo, tiene una sólo órbita. En consecuencia, por el Teorema 3.54,

$$|G| = \sum_{g \in G} |X^g|$$

y, como $|X^1| = |X| > 1$, debe existir $g \in G$ tal que $X^g = \emptyset$. \square

6. Teoremas de Sylow

Fijemos un número primo p . Un grupo finito es un p -grupo si su orden es una potencia de p . Supongamos que G es un grupo de orden $n = p^\alpha m$ con $\alpha > 0$ y m coprimo con p . Por definición un p -subgrupo de Sylow de G es un subgrupo de G de orden p^α . Cuando p esté claro o no nos interese hablaremos también de *subgrupos de Sylow*. En esta sección vamos a probar un teorema muy importante, que asegura, entre otras cosas, que el conjunto de los p -subgrupos de Sylow de G no es vacío. El teorema tiene tres ítems 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 3.57 (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 (23) 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 $g^p = 1$. \square

La noción de p -grupos se puede extender a grupos infinitos. La caracterización dada abajo indica la manera correcta de hacerlo.

COROLARIO 3.58. Un grupo finito G es un p -grupo si y sólo si el orden de cada uno de sus elementos es una potencia de p .

En la demostración del teorema de Sylow usaremos el teorema de Cauchy con G abeliano. Bajo esta hipótesis es posible dar una prueba alternativa del último por inducción en $|G|/p$, y obtener luego el caso general como un corolario inmediato del primero.

DEMOSTRACIÓN ALTERNATIVA DEL TEOREMA DE CAUCHY, PARA G ABELIANO. El resultado es obvio cuando $|G|/p = 1$. Para el paso inductivo tomemos $g \in G$ tal que $|g| > 1$. Si p divide a $|g|$, entonces $g^{|g|/p}$ tiene orden p . Si no, p divide a $|G/\langle g \rangle|$ y, por hipótesis inductiva, existe $h \in G$, tal que su clase en $G/\langle g \rangle$ tiene orden p . Pero entonces el orden de h es múltiplo de p y $h^{|h|/p}$ tiene orden p .

LEMA 3.59. 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 incluido en P .

DEMOSTRACIÓN. Por hipótesis HP es un subgrupo de $N_G(P)$ y P es un subgrupo normal de HP . Entonces por el tercer teorema del isomorfismo $H \cap P \triangleleft H$ y $HP/P \simeq H/H \cap P$, de lo cual se sigue que

$$|HP| = |HP : P||P| = |H : H \cap P||P|$$

es una potencia de p . En consecuencia, como $P \cup H \subseteq HP$, y P es un p -grupo maximal, $H \leq P$. \square

TEOREMA 3.60 (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 incluido en un p -subgrupo de Sylow de G . Además, la cantidad de p -subgrupos de Sylow de G que contienen a H es congruente a 1 módulo p .*

DEMOSTRACIÓN. Primero probemos que el conjunto de los p -subgrupos de Sylow de G no es vacío. Procedemos por inducción en $|G|/p$. Cuando $|G|/p = 1$, esto es trivial. Supongamos que el resultado 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 . De la ecuación de las clases

$$|G| = |ZG| + \sum_{g \in X' \setminus ZG} |G : C_G(g)|,$$

se sigue que p divide a $|ZG|$. En consecuencia, por el Lema 3.57, el centro de G tiene un elemento g de orden p . Como g es central, $\langle g \rangle \triangleleft G$. 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 $\pi: G \rightarrow G/\langle g \rangle$. La igualdad

$$|P| = |g||P'| = p|P'|$$

muestra que P es un p -subgrupo de Sylow de G . Fijemos un tal P y llamemos X a su clase de conjugación. Cada p -subgrupo H de G actúa por conjugación sobre X . Por el Lema 3.59,

$$X^H = \{gPg^{-1} : H \subseteq N_G(gPg^{-1})\} = \{gPg^{-1} : H \subseteq gPg^{-1}\}.$$

Por otra parte

$$|X^H| \equiv |X| \pmod{p},$$

puesto que $X \setminus X^H$ es una unión disjunta de órbitas no triviales y, por el Corolario 3.44, el cardinal de cada órbita no trivial de X es una potencia positiva de p . Así,

$$|\{gPg^{-1} : H \subseteq gPg^{-1}\}| \equiv |X| \pmod{p}.$$

Como $\{gPg^{-1} : P \subseteq gPg^{-1}\} = \{P\}$, tomando $H = P$ en esta igualdad, concluimos que $|X| \equiv 1 \pmod{p}$ y, en consecuencia, que

$$|\{gPg^{-1} : H \subseteq gPg^{-1}\}| \equiv 1 \pmod{p}.$$

Aplicando esta fórmula con H un p -subgrupo de Sylow se obtiene el ítem 2). Considerando ahora H arbitrario se verifica que vale el ítem 3). Finalmente, el ítem 1) se sigue del 3) tomando $H = 1$. \square

para cada grupo finito G , designamos con el símbolo $\text{Syl}_p G$ al conjunto de los p -subgrupos de Sylow de G .

COROLARIO 3.61. *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 $|G : N_G(P)|$, donde $P \in \text{Syl}_p G$ es arbitrario.*

DEMOSTRACIÓN. Dado que la acción de G sobre $\text{Syl}_p G$ por conjugación es transitiva, $|\text{Syl}_p G| = |G : G_P| = |G : N_G(P)|$. \square

COROLARIO 3.62. *Si G es un grupo de orden $p^r m$ con p primo y m coprimo con p , entonces $|\text{Syl}_p G|$ divide a m .*

DEMOSTRACIÓN. Es una consecuencia inmediata del Corolario 3.61. \square

COROLARIO 3.63. *Supongamos que P es un p -subgrupo de Sylow de un grupo finito G . Son equivalentes:*

1. P es un subgrupo completamente normal de G .
2. P es un subgrupo normal de G .
3. P es el único p -subgrupo de Sylow de G .

DEMOSTRACIÓN. 1) \Rightarrow 2) Es trivial.

2) \Rightarrow 3) Por el ítem 2) del Teorema 3.60.

3) \Rightarrow 1) Si G tiene sólo un p -subgrupo de Sylow P , entonces P es completamente normal en G , porque la imagen de P por un endomorfismo de G es un p -subgrupo de G que, por el ítem 3) del Teorema 3.60, está incluido en P . \square

PROPOSICIÓN 3.64. *Si $(P_i)_{i \in I}$ es una familia de subgrupos de Sylow de un grupo finito G , que contiene exactamente un p -subgrupo de Sylow para cada primo p que divide a $|G|$, entonces G está generado por $\bigcup_{i \in I} P_i$.*

DEMOSTRACIÓN. Consideremos el subgrupo G' de G generado por $\bigcup_{i \in I} P_i$. Como $P_i \leq G'$, el orden de P_i divide a G' y, como los $|P_i|$'s son coprimos dos a dos, $|G| = \prod_{i \in I} |P_i|$ también divide a G' . Por lo tanto $G' = G$. \square

OBSERVACIÓN 3.65. *Consideremos un subgrupo H de un grupo finito G y fijemos un divisor primo p de $|H|$. Por el ítem 3) del Teorema 3.60, todo p -subgrupo de Sylow P_H de H está incluido en un p -subgrupo de Sylow P de G y, además, $P_H = P \cap H$. En consecuencia,*

$$|\text{Syl}_p H| \leq |\text{Syl}_p G|.$$

Supongamos que P' es otro p -subgrupo de Sylow de G . Por el ítem 2) del mismo teorema, sabemos que existe $g \in G$ tal que $P' = gPg^{-1}$, de lo cual se sigue que

$$gP_H g^{-1} = P' \cap gHg^{-1}.$$

Por consiguiente, si H es normal, entonces $P \cap H \in \text{Syl}_p H$ para cada $P \in \text{Syl}_p G$ (en particular, cada p -subgrupo normal de G está incluido en todos los p -subgrupos de Sylow de G). Además $PH/H \in \text{Syl}_p(G/H)$, porque

$$|PH/H| = |P/(P \cap H)|$$

es una potencia de p y

$$|G/H : PH/H| = |G : PH|$$

es coprimo con p . Usando que

$$[g] \frac{PH}{H} [g]^{-1} = \frac{gPHg^{-1}}{H} = \frac{gPg^{-1}gHg^{-1}}{H} = \frac{gPg^{-1}H}{H} \quad \text{para todo } g \in G,$$

y que todos los elementos de $\text{Syl}_p(G/H)$ son conjugados, es fácil ver ahora que todos los subgrupos de Sylow de G/H son de esta forma.

PROPOSICIÓN 3.66. Si H es un subgrupo normal de un grupo finito G y p es un primo que divide a $|H|$, entonces $|\text{Syl}_p H|$ divide a $|\text{Syl}_p G|$. Además

$$\frac{|\text{Syl}_p G|}{|\text{Syl}_p H|} = \frac{|\text{N}_G(P_H)|}{|\text{N}_G(P)|} = \frac{|G : H| |\text{N}_H(P_H)|}{|\text{N}_G(P)|},$$

donde P_H y P son p -subgrupos de Sylow arbitrarios de H y G , respectivamente.

DEMOSTRACIÓN. G actúa sobre $\text{Syl}_p H$ por conjugación, porque

$$gP_Hg^{-1} \subseteq gHg^{-1} = H \quad \text{para todo } P_H \in \text{Syl}_p H \text{ y } g \in G.$$

Además, esta acción es transitiva debido a que lo es su restricción a H y, dado que $\text{N}_G(P_H)$ es el estabilizador de P_H para la acción de G ,

$$|\text{Syl}_p H| = |G : \text{N}_G(P_H)|.$$

Tomemos $P \in \text{Syl}_p G$ tal que $P \cap H = P_H$. Como para todo $g \in \text{N}_G(P)$,

$$gP_Hg^{-1} = g(P \cap H)g^{-1} = gPg^{-1} \cap gHg^{-1} = gPg^{-1} \cap H = P \cap H = P_H$$

el grupo $\text{N}_G(P)$ está incluido en $\text{N}_G(P_H)$. En consecuencia,

$$|H : \text{N}_H(P_H)| = |\text{Syl}_p H| = |G : \text{N}_G(P_H)| \quad \text{divide a} \quad |G : \text{N}_G(P)| = |\text{Syl}_p G|.$$

Finalmente

$$\frac{|\text{N}_G(P_H)|}{|\text{N}_G(P)|} = \frac{|G : \text{N}_G(P)|}{|G : \text{N}_G(P_H)|} = \frac{|\text{Syl}_p G|}{|\text{Syl}_p H|} = \frac{|G : \text{N}_G(P)|}{|H : \text{N}_H(P_H)|} = \frac{|G : H| |\text{N}_H(P_H)|}{|\text{N}_G(P)|},$$

como afirmamos. □

PROPOSICIÓN 3.67. Si H es un subgrupo normal de un grupo finito G y p es un primo que divide a $|G/H|$, entonces $|\text{Syl}_p(G/H)|$ divide a $|\text{Syl}_p G|$.

DEMOSTRACIÓN. Claramente G actúa sobre $\{PH/H : P \in \text{Syl}_p G\}$ por conjugación y esta acción es transitiva. Puesto que $\text{N}_G(P)$ está incluido en el estabilizador $G_{\frac{PH}{H}}$ de PH/H y que $|\text{Syl}_p(G/H)| = |G : G_{\frac{PH}{H}}|$, el cardinal de $\text{Syl}_p(G/H)$ divide a $|G : \text{N}_G(P)| = |\text{Syl}_p G|$. □

DEMOSTRACIÓN. Claramente G actúa sobre $\{PH/H : P \in \text{Syl}_p G\}$ por conjugación y esta acción es transitiva. Como $\text{N}_G(P) \subseteq G_{PH/H}$ y $|\text{Syl}_p(G/H)| = |G : G_{PH/H}|$, el cardinal de $\text{Syl}_p(G/H)$ divide a $|G : \text{N}_G(P)| = |\text{Syl}_p G|$. □

6.1. Algunos ejemplos

El objetivo de esta subsección es determinar los subgrupos de Sylow de algunos grupos finitos.

EJEMPLO 3.68. 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 3.69. Consideremos el grupo simétrico S_4 . Como se trata de un grupo de orden $4! = 2^3 \times 3$, sus 2-subgrupos de Sylow tienen orden 8 y sus 3-subgrupos de Sylow, orden 3. Dado que los únicos elementos de orden 3 de S_4 son sus ocho 3-ciclos, los últimos son los grupos cíclicos

$$\langle(1, 2, 3)\rangle, \quad \langle(1, 2, 4)\rangle, \quad \langle(1, 3, 4)\rangle \quad \text{y} \quad \langle(2, 3, 4)\rangle.$$

Por otra parte, como

$$H := \{\text{id}, (1, 2) \circ (3, 4), (1, 3) \circ (2, 4), (1, 4) \circ (2, 3)\}$$

es invariante, está incluido en todos los 2-subgrupos de Sylow de S_4 . Por lo tanto, estos son los subgrupos $P_\sigma := \langle\sigma, H\rangle$, con $\sigma \in S_4 \setminus H$ un elemento cuyo orden es una potencia de 2. Por ejemplo, podemos tomar como σ a un 4-ciclo. Más aún, por el Teorema 2.2 y el ítem 2) del teorema de Sylow, sabemos que todos los 2-subgrupos de Sylow de S_4 tienen esta forma. Puesto que $\langle\sigma\rangle = \langle\sigma^3\rangle$, los únicos candidatos son $P_{(1,2,3,4)}$, $P_{(1,2,4,3)}$ y $P_{(1,3,2,4)}$. Un cálculo directo muestra que

$$P_{(1,2,3,4)} := \{\text{id}, (1, 3), (2, 4), (1, 2) \circ (3, 4), (1, 3) \circ (2, 4), (1, 4) \circ (2, 3), (1, 2, 3, 4), (1, 4, 3, 2)\},$$

$$P_{(1,2,4,3)} := \{\text{id}, (1, 4), (2, 3), (1, 2) \circ (3, 4), (1, 3) \circ (2, 4), (1, 4) \circ (2, 3), (1, 2, 4, 3), (1, 3, 4, 2)\}$$

y

$$P_{(1,3,2,4)} := \{\text{id}, (1, 2), (3, 4), (1, 2) \circ (3, 4), (1, 3) \circ (2, 4), (1, 4) \circ (2, 3), (1, 3, 2, 4), (1, 4, 2, 3)\}.$$

Finalmente, como $P_{(1,2,3,4)}$ está generado por las permutaciones

$$\sigma := (1, 2, 3, 4) \quad \text{y} \quad \tau := (1, 4) \circ (2, 3),$$

y $\sigma^4 = \tau^2 = \tau \circ \sigma \circ \tau^{-1} \circ \sigma = \text{id}$, los grupos $P_{(1,2,3,4)}$, $P_{(1,2,4,3)}$ y $P_{(1,3,2,4)}$ son isomorfos a D_4 .

EJEMPLO 3.70. Parte de los argumentos usados en el ejemplo anterior muestran que

$$\langle(1, 2, 3)\rangle, \quad \langle(1, 2, 4)\rangle, \quad \langle(1, 3, 4)\rangle \quad \text{y} \quad \langle(2, 3, 4)\rangle$$

son los 3-subgrupos de Sylow de A_4 , y que $H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ es su único 2-subgrupo de Sylow.

EJEMPLO 3.71. Consideremos el grupo diedral D_n . Recordemos que D_n está generado por dos elementos x e y sujetos a las relaciones

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

y que

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

Recordemos también que

- Los elementos $x^i y$ tienen orden 2.
- Los elementos x^i tienen orden $n/(n : i)$.
- El subgrupo $\langle x^i \rangle$ de D_n es invariante para todo i .

Escribamos $n = 2^m t$ con t impar, de manera que $|D_n| = 2^{m+1}t$. Afirmamos que:

1. Todos los 2-subgrupos de Sylow de D_n son isomorfos a D_{2^m} , y hay t de ellos (aquí debemos interpretar a D_1 como el grupo cíclico de orden 2).
2. Si p es un primo impar que divide a t , entonces D_n tiene un único p -subgrupo de Sylow, el cual es cíclico.

El ítem 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 ítem 1). Como $\langle x^t \rangle \triangleleft D_n$ y $|x^t| = 2^m$, todos los 2-subgrupos de Sylow de D_n incluyen a $\langle x^t \rangle$. En consecuencia, dado que el orden de ningún $x^i \in D_n \setminus \langle x^t \rangle$ es una potencia de 2, los posibles 2-subgrupos de Sylow de D_n , son los subgrupos $K_i := \langle x^i y, x^t \rangle = \langle x^t \rangle \langle x^i y \rangle$, donde la última igualdad vale porque $\langle x^t \rangle$ es normal. De hecho, como

$$|\langle x^t \rangle \langle x^i y \rangle| = \frac{|\langle x^t \rangle| |\langle x^i y \rangle|}{|\langle x^t \rangle \cap \langle x^i y \rangle|} = \frac{2^m \times 2}{1} = 2^{m+1},$$

todos los K_i son, efectivamente, 2-subgrupos de Sylow de D_n . Puesto que

$$K_i = \langle x^i y, x^t \rangle = \{x^{tj+i} y, x^{tj} : 0 \leq j < 2^m\},$$

es claro que $K_i = K_{i'}$ si y sólo si $i' \equiv i \pmod{t}$. Así, los 2-subgrupos de Sylow de D_n son exactamente K_0, \dots, K_{t-1} . Para ver que K_i es isomorfo a D_n es suficiente notar que tiene orden 2^{m+1} y que los elementos $x^i y$ y x^t generan K_i y satisfacen

$$(x^t)^{2^m} = 1, \quad (x^i y)^2 = 1 \quad y \quad (x^i y) x^t (x^i y)^{-1} x^t = 1.$$

EJEMPLO 3.72. Recordemos que el grupo cuaterniónico generalizado H_n está generado por dos elementos x e y sujetos a las relaciones

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

y que

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

Recordemos también que

- Los elementos $x^i y$ tienen orden 4.
- Los elementos x^i tienen orden $2n/(2n : i)$.
- El subgrupo $\langle x^i \rangle$ de H_n es invariante para todo i .

Escribamos $n = 2^m t$ con t impar, de manera que $|H_n| = 2^{m+2} t$. Afirmamos que:

1. Todos los 2-subgrupos de Sylow de H_n son isomorfos a H_{2^m} , y hay t de ellos (aquí debemos interpretar a H_1 como el grupo cíclico de orden 4).
2. Si p es un primo impar que divide a t , entonces H_n tiene un único p -subgrupo de Sylow, el cual es cíclico.

El ítem 2) se sigue inmediatamente de que si $t = p^u v$ con v coprimo con p , entonces $\langle x^{2^{m+1} v} \rangle$ tiene orden p^u y es invariante. Consideremos ahora el ítem 1). El subgrupo $\langle x^t \rangle$ de H_n está incluido en todos los 2-subgrupos de Sylow de H_n , porque es invariante y tiene 2^{m+1} elementos. En consecuencia, como el orden de ningún $x^i \in H_n \setminus \langle x^t \rangle$ es una potencia de 2, los posibles 2-subgrupos de Sylow de H_n son algunos de los subgrupos $L_i := \langle x^i y, x^t \rangle = \langle x^t \rangle \langle x^i y \rangle$, donde la última igualdad vale porque $\langle x^t \rangle$ es invariante. Notemos ahora que

$$(x^i y)^2 = x^i y x^i y^{-1} y^2 = y^2 = x^n$$

y, por lo tanto, $\langle x^i y \rangle \cap \langle x^t \rangle = \{1, x^n\}$. Así,

$$|\langle x^t \rangle \langle x^i y \rangle| = \frac{|\langle x^t \rangle| |\langle x^i y \rangle|}{|\langle x^t \rangle \cap \langle x^i y \rangle|} = \frac{2^{m+1} \times 4}{2} = 2^{m+2},$$

lo que muestra que todos los L_i son 2-subgrupos de Sylow. Puesto que

$$L_i = \langle x^i y, x^t \rangle = \{x^{tj+i} y, x^{tj} : 0 \leq j < 2^{m+1}\},$$

es claro que $L_i = L_{i'}$ si y sólo si $i' \equiv i \pmod{t}$. Así, los 2-subgrupos de Sylow de H_n son exactamente L_0, \dots, L_{t-1} . Para ver que L_i es isomorfo a H_{2^m} es suficiente notar que tiene orden 2^{m+2} y que $x^i y$ y x^t generan L_i y satisfacen

$$(x^t)^{2^m} (x^i y)^{-2} = 1 \quad y \quad (x^i y) x^t (x^i y)^{-1} x^t = 1.$$

EJEMPLO 3.73. Consideremos un grupo simétrico S_p , con p primo. Como $|S_p| = p!$ y p es coprimo con $(p-1)!$, cada p -subgrupo de Sylow de S_p es cíclico de orden p y así está generado por un p -ciclo. Como la cantidad de los p -ciclos de S_p es $(p-1)!$ y cada subgrupo cíclico de orden p de S_p tiene $p-1$ de estos p -ciclos, la cantidad de p -subgrupos de Sylow de S_p es

$$(p-2)! = \frac{(p-1)!}{p-1}.$$

En consecuencia, por el ítem (1) del teorema de Sylow

$$(p-2)! \equiv 1 \pmod{p},$$

que es lo que dice el famoso teorema de Wilson.

EJEMPLO 3.74. 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 3.45 sabemos que, cualquiera sea n , el orden de $GL(n, k)$ 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 $UT(n, k)$ de $GL(n, k)$, formado por las matrices triangulares superiores que tienen 1 en la diagonal principal, $UT(n, k)$ es un p -subgrupo de Sylow de $GL(n, k)$.

TEOREMA 3.75 (Frattini). Si H es un subgrupo normal de un grupo finito G y P es un p -subgrupo de Sylow de H , entonces $G = H N_G(P)$. En particular, P es un subgrupo normal de H si y sólo si es un subgrupo normal de G .

DEMOSTRACIÓN. Tomemos $g \in G$. Como H es normal, $gPg^{-1} \subseteq gHg^{-1} = H$. En consecuencia, por el ítem 2) del teorema de Sylow, existe $h \in H$ tal que $hgPg^{-1}h^{-1} = P$. Así, $g = h^{-1}hg \in H N_G(P)$. \square

COROLARIO 3.76. Si un subgrupo H de un grupo finito G contiene al normalizador de un subgrupo de Sylow P de G , entonces $N_G(H) = H$.

DEMOSTRACIÓN. Debido al Teorema 3.75, como H es normal en $N_G(H)$,

$$N_G(H) = H N_{N_G(H)}(P) \subseteq H N_G(P) = H,$$

como queremos. \square

6.2. Algunas aplicaciones

En esta subsección establecemos algunos resultados que son consecuencia más o menos directa del teorema de Cauchy, los Teoremas de Sylow y sus corolarios. El primero es la clasificación de los grupos finitos cuyo orden es producto de dos primos distintos. La prueba que damos usa de manera esencial el teorema de Cauchy.

TEOREMA 3.77 (Caracterización de grupos de orden pq). *Supongamos que G es un grupo de orden pq con p y q primos y $q < p$.*

- Si G es abeliano, entonces $G \simeq \mathbb{Z}_{pq}$.
- Si G no es abeliano, entonces q divide a $p - 1$, el conjunto

$$R = \{r \in \mathbb{N} : 1 < r < p \text{ y } r^q \equiv 1 \pmod{p}\}$$

no es vacío y G está generado por elementos g y h , de órdenes p y q respectivamente, que satisfacen $hgh^{-1} = g^{r_0}$, donde r_0 es el mínimo elemento de R . En particular, G es producto semidirecto interno de los subgrupos $\langle g \rangle$ y $\langle h \rangle$.

DEMOSTRACIÓN. Por el teorema de Cauchy, existen $g, k \in G$ con $|\langle g \rangle| = p$ y $|\langle k \rangle| = q$. Además, por el Corolario 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 $G = \langle g \rangle \times \langle k \rangle \simeq \mathbb{Z}_{pq}$. Supongamos ahora que $\langle k \rangle$ no es normal. Como $\langle g \rangle$ si lo es, existe $0 \leq r < p$ tal que $kgk^{-1} = g^r$. Un argumento inductivo muestra ahora que $k^i g k^{-i} = g^{r^i}$ para todo $i > 1$, por lo que

$$g^{r^q} = k^q g k^{-q} = g,$$

lo cual implica que $r^q \equiv 1 \pmod{p}$. Por otra parte, dado que la igualdad $kgk^{-1} = 1$ es imposible y que G no es conmutativo, debe ser $r > 1$. Por lo tanto, como q es primo, q es el orden de r en \mathbb{Z}_p^* . En consecuencia, por el teorema de Lagrange, q divide a $|\mathbb{Z}_p^*| = p - 1$. Como la ecuación $X^q = 1$ no puede tener más de q raíces en \mathbb{Z}_p^* , y cada potencia de r es una raíz, existe $\alpha < q$ tal que $r^\alpha \equiv r_0 \pmod{p}$, donde r_0 es el mínimo de los enteros s tales que

$$1 < s < p \quad \text{y} \quad s^q \equiv 1 \pmod{p}.$$

Tomemos $h = k^\alpha \neq 1$. Puesto que $k = h^\beta$, donde $\beta \in \mathbb{Z}_q$ es el inverso multiplicativo de α , el grupo G está generado por g y h . Finalmente, como

$$h^q = (k^\alpha)^q = (k^q)^\alpha = 1 \quad \text{y} \quad hgh^{-1} = k^\alpha g k^{-\alpha} = g^{r^\alpha} = g^{r_0},$$

los elementos g y h satisfacen las relaciones requeridas en el enunciado. \square

Supongamos que p y q son primos y que q divide a $p - 1$. Por el teorema de Cauchy \mathbb{Z}_p^* tiene un elemento r de orden q . Por el Ejemplo 1.143, sabemos que para cada uno de estos r hay un grupo de orden pq generado por elementos g y h , de órdenes p y q respectivamente, que satisfacen $hgh^{-1} = g^r$.

En el resto de esta subsección denotaremos con n_p a la cantidad de p -subgrupos de Sylow de un grupo finito G .

PROPOSICIÓN 3.78. *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 3.62, forzosamente $n_q = 1$, $n_q = p$ o $n_q = p^2$. En el primer caso el único q -subgrupo de Sylow de G es normal debido al Corolario 3.63. Por el ítem 1) del teorema de Sylow, en el segundo $p \equiv 1 \pmod{q}$, por lo que $p > q$. Puesto que, nuevamente por el Corolario 3.62 y el ítem 1) del teorema de Sylow, $n_p \mid q$ y $n_p \equiv 1 \pmod{p}$, esto implica que $n_p = 1$, y así G tiene un único p -subgrupo de Sylow, el cual es normal, nuevamente por el Corolario 3.63. 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. \square

PROPOSICIÓN 3.79. *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 ítem 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 3.63 y, por lo tanto,

$$\begin{aligned} |(G \setminus S) \cup 1| &= 2pq - ((h_p p + 1)(p - 1) + (h_q q + 1)(q - 1)) \\ &\leq 2pq - ((p + 1)(p - 1) + (q + 1)(q - 1)) \\ &= 2pq - (p^2 - 1 + q^2 - 1) \\ &= -(q - p)^2 + 2 \leq -2, \end{aligned}$$

lo que es absurdo. \square

Aplicaciones a grupos de orden pequeño En este párrafo 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 $n_7 \equiv 1 \pmod{7}$ 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 $n_5 \equiv 1 \pmod{5}$ 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 $n_7 \equiv 1 \pmod{7}$ 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 A_5 : Por la Proposición 2.13 y el Teorema 3.10 para probar esto será suficiente ver que si G es un grupo simple de orden 60, entonces G tiene un subgrupo H de índice 5. Por el ítem 1) del teorema de Sylow y el Corolario 3.62 sabemos que $n_2 \in \{1, 3, 5, 15\}$ y $n_5 \in \{1, 6\}$. Por el Corolario 3.63, 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 3.61, 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 3.61, podemos tomar $H = N_G(P)$ donde 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 $H = \langle P_1, P_2 \rangle$.

7. p-Grupos finitos

En esta sección establecemos algunas propiedades básicas de los p -grupos finitos.

TEOREMA 3.80. *Si G es un p -grupo finito, $H \triangleleft G$ y $H \neq 1$, entonces $H \cap ZG \neq 1$. En particular, ZG no es trivial.*

DEMOSTRACIÓN. Consideremos la ecuación

$$|H| = |H \cap ZG| + \sum_{h \in X' \setminus (H \cap ZG)} |G : C_G(h)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de G que están incluidas en H (vease el segundo ejemplo debajo de la igualdad (25)). Dado que tanto $|H|$ como cada $|G : C_G(h)|$ son divisibles por p , también lo es $|H \cap ZG|$, de manera de que $H \cap ZG$ no es trivial. \square

COROLARIO 3.81. *Todo subgrupo normal de orden p de un p -grupo G está incluido en el centro de G .*

COROLARIO 3.82. *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 3.80 existe $g \in Z(G) \cap G_{i_1}$ tal que $G_1 := \langle g \rangle$ es un subgrupo normal de orden p de G incluido en G_{i_1} . Por lo tanto podemos suponer sin pérdida de generalidad que $i_1 = 1$. Consideremos la proyección canónica $\pi: G \rightarrow G/G_1$. 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

$$1 = \overline{G}_0 \subseteq \overline{G}_1 \subseteq \overline{G}_2 \subseteq \cdots \subseteq \overline{G}_{n-1} \subseteq \overline{G}_n,$$

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. \square

COROLARIO 3.83. *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 3.80 los grupos ZG y G/ZG tienen orden p y, por eso mismo son cíclicos, lo que contradice la Proposición 1.161.

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 1.119 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 $H_1 H_2 = G$. \square

COROLARIO 3.84. *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/ZG es abeliano y no es cíclico.*

DEMOSTRACIÓN. Por el Teorema 3.80 sabemos que $ZG \neq 1$ y, como G no es abeliano, $ZG \neq G$. Además, por la Proposición 1.161, el cociente G/ZG no es cíclico. Por lo tanto $|G/ZG| = p^2$ y $|ZG| = p$. Por otra parte, dado que por el corolario anterior G/ZG es abeliano,

$$[G, G] \subseteq ZG.$$

Pero la inclusión no puede ser propia, porque eso significaría que G es abeliano. Finalmente, por el Corolario 3.81, el único subgrupo normal de orden p de G es ZG . \square

TEOREMA 3.85. *Si H es un subgrupo propio de un p -grupo finito G , entonces $H \subsetneq N_G(H)$.*

DEMOSTRACIÓN. Si H es normal, entonces $H \subsetneq G = N_G(H)$. 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 $g^{-1}Hg \subseteq N_G(H)$. Esto termina la prueba porque $g^{-1}Hg \neq H$. \square

COROLARIO 3.86. Si H es un subgrupo propio maximal de un p -grupo finito G , entonces H es normal y su índice es p .

DEMOSTRACIÓN. Por el teorema anterior $H \triangleleft G$. Además, por el Corolario 1.94, el cociente G/H no tiene subgrupos no triviales y, en consecuencia, debido al Corolario 3.82, su cardinal es p . \square

OBSERVACIÓN 3.87. Supongamos que H es un subgrupo propio de un p -grupo finito G . Por el Teorema 3.85, en la cadena de subgrupos

$$H \triangleleft N_G^1(H) \triangleleft N_G^2(H) \triangleleft \dots \triangleleft N_G^{i-1}(H) \triangleleft N_G^i(H) = G,$$

donde $N_G^{j+1}(H) = N_G(N_G^j(H))$ 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

$$p^{\alpha_0} < p^{\alpha_1} < \dots < p^{\alpha_i},$$

de potencias de p . Por el Corolario 3.82, para cada $j < i$ hay una cadena

$$N_G^j(H) = G_{\alpha_j} \subseteq G_{\alpha_{j+1}} \subseteq \dots \subseteq G_{\alpha_{j+1}-1} \subseteq G_{\alpha_{j+1}} = N_G^{j+1}(H),$$

en la cual $G_{\alpha_{j+1}}$ es un subgrupo normal de orden $p^{\alpha_{j+1}}$ de $N_G^{j+1}(H)$. En particular H está incluido en un subgrupo de índice p de G .

TEOREMA 3.88. 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 ítem 3) del Teorema 3.60. Supongamos que $n > 0$ y que el teorema vale para subgrupos de G de orden p^{m+1} . Designemos con

$$P_1, \dots, P_u \quad \text{y} \quad Q_1, \dots, Q_v$$

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 Q_j fijo, es congruente a 1 módulo p . Para concluir la demostración será suficiente mostrar que la cantidad b_i de los Q_j 's que están contenidos en un P_i fijado, también es congruente a 1 módulo p , ya que entonces de la igualdad

$$\sum_{i=1}^u b_i = \sum_{j=1}^v a_j,$$

válida pues las dos sumas cuentan a cada P_i con multiplicidad igual a la cantidad de Q_j 's que contiene, se seguirá que $u \equiv v \pmod{p}$. Con esto en mente fijemos P_i y supongamos que

$$Q_{j_1}, \dots, Q_{j_{v'}}$$

son los Q_j 's contenidos en P_i . Debemos mostrar que $v' \equiv 1 \pmod{p}$. Por el Corolario 3.82 aplicado al grupo P_i y al la cadena trivial $1 \subseteq P_i$ sabemos que $v' \geq 1$. Si $v' = 1$, entonces es obvio que $v' \equiv 1 \pmod{p}$. Analizemos que ocurre cuando $v' > 1$. Por el Corolario 3.86, cada Q_{j_i} es un subgrupo normal de P_i . Por consiguiente $Q_{j_1}Q_{j_2} = P_i$. Por la Proposición 1.42, 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 3.83, 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 $Q_{j_{i_3}}$ tal que D_1 no esté incluido en $Q_{j_{i_3}}$. Escribamos $D_2 := Q_{j_1} \cap Q_{j_{i_3}}$. 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_i} , entonces $Q_{j_1} \cap Q_{j_i}$ contendría a D_1 y a D_2 , lo que es absurdo porque

$$|D_1| = |D_2| = |Q_{j_1} \cap Q_{j_i}| = p^{m-1}$$

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 $Q_{j_{i_4}}$ tal que ni D_1 ni D_2 estén incluidos en $Q_{j_{i_4}}$ y escribamos $D_3 := Q_{j_1} \cap Q_{j_{i_4}}$. 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 demostración, 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 3.89. *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. Tómesese $H := 1$ en el teorema anterior. \square

OBSERVACIÓN 3.90. *Supongamos que N es un subgrupo normal de un p -grupo finito G . Fijemos $m < n$ tales que $p^m \leq |N|$ y $p^n \leq |G|$ y designemos con X al conjunto de los subgrupos de orden p^n de G que intersecan a N en un subgrupo de orden p^m (X puede ser vacío). Como N es normal, G actúa sobre X por conjugación. Los puntos fijos de X bajo esta acción son los subgrupos normales de G que pertenecen a X . Además $|X^G| \equiv |X| \pmod{p}$, puesto que $X \setminus X^G$ es una unión disjunta de órbitas no triviales, y por el Corolario 3.44 el cardinal de cada una de esta órbitas es una potencia positiva de p . En consecuencia,*

$$|\{P \in X : P \text{ es un subgrupo normal de } G\}| \equiv |X| \pmod{p}.$$

Por ejemplo, por el Teorema 3.88, si N un subgrupo normal de un p -grupo finito G y

$$|N| \leq p^n \leq |G|,$$

entonces la cantidad de subgrupos normales de G de orden p^n que contienen a N es congruente a 1 módulo p y, por el Teorema 3.80, la cantidad de subgrupos de orden p^n de un p -grupo finito G cuya intersección con ZG es 1, es un múltiplo de p .

LEMA 3.91. *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, $|g| \leq p^2$ y $|G_1/\langle g \rangle| \leq p$. Por lo tanto, $|G_1| \leq p^3$. Para probar que vale la desigualdad opuesta será suficiente exhibir un morfismo sobreyectivo de G_1 en un grupo de orden p^3 . Tomemos grupos cíclicos $C_{p^2} = \langle x \rangle$ y $C_p = \langle y \rangle$ de orden p^2 y p , respectivamente. Como $(1+p)^p \equiv 1 \pmod{p^2}$ la aplicación

$$\begin{array}{ccc} C_{p^2} & \xrightarrow{\psi} & C_{p^2} \\ x^i & \longmapsto & x^{i(p+1)} \end{array},$$

es un automorfismo de orden p y, por consiguiente, la correspondencia

$$\begin{array}{ccc} C_p & \xrightarrow{\varsigma} & \text{Aut}(C_{p^2}) \\ y^j & \longmapsto & \psi^j \end{array}$$

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

$$\hat{x}^{p^2} = \hat{y}^p = 1 \quad \text{e} \quad \hat{y}\hat{x}\hat{y}^{-1} = \hat{x}^{p+1},$$

hay un morfismo $\xi: G_1 \rightarrow C_{p^2} \times_{\varsigma} C_p$ 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 3.92. *El grupo*

$$G_2 := \langle g, h, k|g^p, h^p, k^p, hgh^{-1}g^{-1}, k g k^{-1} g^{-1}, k h k^{-1} h^{-1} g \rangle$$

tiene p^3 elementos.

DEMOSTRACIÓN. Notemos que el subgrupo $\langle g \rangle$ de G_2 es normal, $|g| \leq p$ y $|G_2/\langle g \rangle| = p^2$. Por lo tanto, $|G_2| \leq p^3$. Tal como hicimos en el lema anterior, para probar que vale la desigualdad opuesta construiremos un morfismo sobreyectivo de G_2 en un grupo de orden p^3 . Un cálculo sencillo muestra que la aplicación

$$\begin{array}{ccc} C_p \times C_p & \xrightarrow{\psi} & C_p \times C_p \\ (y^i, y^j) & \longmapsto & (y^{i-j}, y^j) \end{array},$$

donde $C_p = \langle y \rangle$ es un grupo cíclico con p elementos, es un automorfismo de orden p , por lo que la correspondencia

$$\begin{array}{ccc} C_p & \xrightarrow{\varsigma} & \text{Aut}(C_p \times C_p) \\ y^k & \longmapsto & \psi^k \end{array}$$

es un morfismo. Tomemos el producto semidirecto $(C_p \times C_p) \times_{\varsigma} C_p$ y escribamos $\hat{y}_1 = (y, 0, 0)$, $\hat{y}_2 = (0, y, 0)$ y $\hat{y}_3 = (0, 0, y)$. Puesto que

$$\hat{y}_1^p = \hat{y}_2^p = \hat{y}_3^p = 1, \quad \hat{y}_2\hat{y}_1 = \hat{y}_1\hat{y}_2, \quad \hat{y}_3\hat{y}_1 = \hat{y}_1\hat{y}_3 \quad \text{y} \quad \hat{y}_3\hat{y}_2 = \hat{y}_1^{-1}\hat{y}_2\hat{y}_3,$$

hay un morfismo $\xi: G_2 \rightarrow (C_p \times C_p) \times_{\varsigma} C_p$ 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. \square

NOTA 3.93. En las demostraciones de los Lemas 3.91 y 3.92 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 3.94 (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 3.91 o al grupo G_2 introducido en el Lema 3.92.

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 $h^p \in \langle g \rangle$ y existe $1 \leq r < p^2$ 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 $0 \leq j < p^2$. Como

$$1 = h^{p^2} = g^{pj},$$

existe $0 \leq t < p$ 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

$$G \simeq \langle g \rangle \times \langle h \rangle \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_p$$

por el Teorema 1.117 y la Proposición 1.129.

r > 1: Un argumento inductivo prueba que $h^i gh^{-i} = g^{r^i}$ para todo $i \geq 1$. En particular $g = h^p gh^{-p} = g^{r^p}$, por lo que $r^p \equiv 1 \pmod{p^2}$. Puesto que

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

y $\mathbb{Z}_{p^2}^\times$ tiene un único subgrupo de orden p (pues es cíclico de orden $(p-1)p$), existe $0 < \alpha < p$ tal que $1+p \equiv r^\alpha \pmod{p^2}$. Notemos que $h^\alpha \in G \setminus \langle g \rangle$ porque p no divide a α . Cambiando h por h^α podemos suponer que $r = 1+p$, ya que

$$h^\alpha gh^{-\alpha} = g^{r^\alpha} = g^{1+p}.$$

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, $G \simeq D_4$, 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, $G \simeq H_2$.

p > 2: Haciendo inducción primero en j y luego en i se verifica que $h^i g^j = g^{j(1+p)^i} h^i$. Usando esto es fácil comprobar por inducción en l que

$$(g^{-t(1+p)}h)^l = g^{-t(1+p)(1+\dots+(1+p)^{l-1})}h^l = g^{-t(1+p)\frac{(1+p)^l-1}{p}}h^l.$$

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

$$(g^{-t(1+p)}h)g(g^{-t(1+p)}h)^{-1} = g^{-t(1+p)}hgh^{-1}g^{t(1+p)} = g^{-t(1+p)}g^{1+p}g^{t(1+p)} = g^{1+p},$$

reemplazando h por $g^{-t(1+p)}h$, vemos que G está generado por dos elementos g y h que satisfacen

$$g^{p^2} = h^p = 1 \quad \text{e} \quad hgh^{-1} = g^{1+p}$$

y, por lo tanto, $G \simeq G_1$.

Resta ver que sucede cuando todos los elementos no nulos de G tienen orden p . Nuevamente consideramos por separado los casos G conmutativo y G no conmutativo.

G es conmutativo: Tomemos $g \in G \setminus \{1\}$ arbitrario y $h, k \in G$ tales que sus clases en $G/\langle g \rangle$ generan $G/\langle g \rangle$. Por el Teorema 1.117, 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 $\langle k \rangle$, y, en consecuencia, 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 3.83 y 3.84 sabemos que $p > 2$, que $ZG = [G, G]$ es un subgrupo invariante de orden p de G y que $G/ZG \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Tomemos $h, k \in G$ tales que sus clases en G/ZG generen G/ZG . Entonces el conmutador

$$g = [h, k] = hkh^{-1}k^{-1} \in ZG$$

es distinto de 1, porque de lo contrario

$$G = \langle h, k, ZG \rangle$$

sería conmutativo. Por consiguiente G está generado por los elementos g, h y k , los cuales satisfacen las relaciones

$$g^p = h^p = k^p = hgh^{-1}g^{-1} = kgh^{-1}g^{-1} = khk^{-1}h^{-1}g = 1,$$

y en consecuencia es isomorfo a G_2 .

No habiendo más casos para considerar, la prueba está terminada. □

Parte 2

Anillos y módulos

Capítulo 4

Teoría elemental de anillos

1. Anillos

Un *anillo* A es un conjunto provisto de dos operaciones binarias, llamadas *suma* o *adición* y *producto* o *multiplicación*, tales que

1. A es un grupo abeliano vía la suma,
2. A es un monoide vía el producto,
3. El producto es distributivo a izquierda y a derecha con respecto a la suma.

Como es usual, denotaremos con $a+b$ a la suma de dos elementos $a, b \in A$, con ab al producto, con 0 al elemento neutro de A respecto de la suma, con $-a$ al opuesto aditivo de un elemento a y con 1 a la unidad o neutro respecto del producto. Con estas notaciones el último item de la definición anterior se escribe

$$a(b+c) = ab+ac \quad \text{y} \quad (b+c)a = ba+ca.$$

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 $M_n(A)$, de matrices cuadradas de $n \times n$ con coeficientes en un anillo A (cuando A es un 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 $\text{End}_k(V)$ de un k -espacio vectorial V , si $\dim_k(V) > 1$. Como el lector atento habrá notado, algunos de los ejemplos mencionados aquí, entre ellos el último, ya fueron considerados en la primera parte de estas notas.

PROPOSICIÓN 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) Basta observar que, por el ítem anterior,

$$ab + (-a)b = (a + (-a))b = 0b = 0.$$

La otra afirmación es similar. □

COROLARIO 4.2. Si $1 = 0$, entonces $A = 0$.

DEMOSTRACIÓN. Por la proposición anterior $a = a1 = a0 = 0$ para cada $a \in A$. □

El *anillo opuesto* de A es el anillo A^{op} , que tiene el mismo conjunto subyacente y suma que A , pero cuya multiplicación $\mu_{A^{\text{op}}}: A^{\text{op}} \times A^{\text{op}} \rightarrow A^{\text{op}}$ está definida por $\mu_{A^{\text{op}}}(a, b) := ba$. Es evidente que A es conmutativo si y sólo si $A = A^{\text{op}}$.

Un elemento a de A es un *divisor de cero a izquierda* si existe $b \in A \setminus \{0\}$ tal que $ab = 0$, un *divisor de cero a derecha* si existe $b \in A \setminus \{0\}$ tal que $ba = 0$. Finalmente a es un *divisor de cero* si lo es a izquierda o a derecha. Por ejemplo, el operador de derivación

$$\frac{d}{dX}: \mathbb{R}[X] \rightarrow \mathbb{R}[X]$$

es un divisor de cero a izquierda del anillo $\text{End}_{\mathbb{R}}(\mathbb{R}[X])$, porque componiéndolo a derecha con la evaluación en cero

$$\text{ev}_0: \mathbb{R}[X] \rightarrow \mathbb{R}[X],$$

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 $\text{ev}_0 \circ (\text{id} - \text{ev}_0) = 0$. Notemos que a es divisor de cero a un lado en A si y sólo si lo es al otro en A^{op} y que, salvo en el caso en que A es el anillo nulo, 0 es divisor de cero.

Tal como para magmas, monoides y grupos, muchas propiedades predicables sobre elementos y subconjuntos de A tienen una versión a izquierda y otra a derecha (que es la misma, pero predicada en A^{op}). También en esta parte del apunte a veces daremos sólo una de ellas, dejando como ejercicio la tarea de enunciar la otra.

Recordemos que un elemento $a \in A$ es cancelable a izquierda si $ab = ac \Rightarrow b = c$ y cancelable a derecha si $ba = ca \Rightarrow b = c$. Decimos que a es cancelable si lo es a izquierda y a derecha. Como vimos en la Sección 1 del Capítulo 1, los elementos cancelables a izquierda forman un submonoides 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 $b - c \neq 0$. □

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). \square

Un *dominio* o *anillo cancelativo* es un anillo no nulo 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

$$(aX^mY^n)(bX^{m'}Y^{n'}) := q^{m'n}abX^{m+m'}Y^{n+n'}$$

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 estándar, 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 *invertible a izquierda* si existe $b \in A$ tal que $ba = 1$ y es *invertible 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 *invertible*, 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 invertibles de A es un grupo vía el producto, llamado *grupo de unidades* de A . Por los comentarios que preceden a la Proposición 1.1 del Capítulo 1, todo elemento de A que es invertible a izquierda es cancelable a izquierda. Además, por dicha proposición también sabemos que si $a \in A$ es invertible a izquierda y cancelable a derecha o invertible a derecha y cancelable a izquierda, entonces es invertible. Por último, debido a la Proposición 1.2 del Capítulo 1, si A es finito, entonces cada $a \in A$ que es cancelable a izquierda o a derecha, es invertible.

EJERCICIO 4.7. Pruebe que si $a \in A$ es invertible a izquierda pero no a derecha, entonces tiene infinitas inversas a izquierda.

Sugerencia: Tome $b_0 \in I$, donde I es el conjunto de las inversas a izquierda de a , y pruebe que la aplicación $\theta: I \rightarrow I$, 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 invertibles a izquierda pero no a derecha.

EJERCICIO 4.8. Pruebe que si V es un k -espacio vectorial con base numerable, entonces $\text{End}_k(V)$ tiene elementos invertibles 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 $\varphi \in \text{End}_k(V)$ son equivalentes:

1. φ es inversible.
2. φ no es divisor de cero a izquierda.
3. φ no es divisor de cero a derecha.

Un *anillo de división* es un anillo no nulo en el cual todo elemento distinto de cero es inversible. Todo anillo de división es un dominio. Un *cuerpo* es un anillo de división conmutativo. Los anillos \mathbb{Q} , \mathbb{R} y \mathbb{C} , de los números racionales, reales y complejos, son cuerpos. También lo es $\mathbb{Z}/p\mathbb{Z}$, si p es primo. Después veremos ejemplos de anillos de división no conmutativos. Por el comentario que precede al Ejercicio 4.7, todo dominio finito es un anillo de división. Sin embargo, como veremos más adelante, estos son necesariamente conmutativos.

Un elemento a de un anillo es *nilpotente* si $a^n = 0$ para algún $n \in \mathbb{N}$.

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

Un subconjunto B de un anillo A es un *subanillo* de A si es cerrado para la resta y el producto y $1 \in B$. Entonces B es un anillo en forma natural. Dado que la intersección de una familia de subanillos de A es un subanillo de A , para cada subconjunto S de A existe un mínimo subanillo $\mathbb{Z}\{S\}$ de A que contiene a S , el cual es llamado *el subanillo de A generado por S* . Siguiendo la práctica usual, si $S = \{x_1, \dots, x_s\}$, 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 $M_n(\mathbb{Q})$ y $M_n(\mathbb{R})$ son subanillos de $M_n(\mathbb{C})$.

EJEMPLO 4.13. Una matriz cuadrada

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

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 $\text{Esc}_n(A)$ de

las matrices escalares, $D_n(A)$ de las matrices diagonales y $T_n(A)$ de las matrices triangulares superiores de $n \times n$ con coeficientes en A , son subanillos de $M_n(A)$.

EJEMPLO 4.14. El anillo de los enteros de Gauss es el subanillo $\mathbb{Z}[i]$ de \mathbb{C} . Es inmediato que $\mathbb{Z}[i]$ son los números complejos con parte real e imaginaria enteras.

EJEMPLO 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} . Es fácil ver que si $a + b\sqrt{3} = a' + b'\sqrt{3}$, entonces $a = a'$ y $b = b'$, de modo que esta escritura es única.

Por definición, el centro de un anillo A es el conjunto

$$Z A := \{a \in A : ab = ba \text{ para todo } b \in A\}.$$

Un elemento a de A es *central* si pertenece al centro de A . Es evidente que $Z A$ es un subanillo conmutativo de A . Además, no es difícil probar que si $a \in Z A$ es inversible, entonces $a^{-1} \in Z A$. 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 $Z A$ es un cuerpo.

PROPOSICIÓN 4.16. Para cada anillo A , el centro de $M_n(A)$, es el anillo $\text{Esc}_n(Z A)$, 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 $B = (a_{ij}) \in Z M_n(A)$. Como $E_{rs}B$ es la matriz cuya única fila no nula es la r -ésima, que coincide con la s -ésima fila de B y BE_{rs} es la matriz cuya única columna no nula es la s -ésima, que coincide con la r -ésima columna de B , la matriz B es diagonal y $a_{ss} = a_{rr}$ para todo r y s . Así, $Z M_n(A) \subseteq \text{Esc}_n(Z A)$. Como la inclusión recíproca es trivial, $Z M_n(A) = \text{Esc}_n(Z A)$. \square

Notemos que en la demostración anterior podríamos haber supuesto que $r \leq s$. Por lo tanto el mismo argumento muestra que $Z T_n(A) = \text{Esc}_n(Z A)$.

Consideremos ahora un subconjunto T de un anillo A . El *centralizador de T en A* es

$$Z_T A := \{a : ab = ba \text{ para todo } b \in T\}.$$

De la definición se sigue inmediatamente que $Z_A A$ es el centro de A . Argumentando del mismo modo que para $Z A$, se comprueba que $Z_T A$ es un subanillo de A cualquiera sea T , y, que si $a \in Z_T A$ es inversible, entonces $a^{-1} \in Z_T A$. En particular, si A anillo de división, entonces $Z_T A$ también lo es. Evidentemente un subanillo B de A es conmutativo si y sólo si $B \subseteq Z_B A$. Además, en este caso, $B\{a\}$ es conmutativo para cada $a \in Z_B A$. En consecuencia, si B es un subanillo conmutativo maximal de A , entonces $B = Z_B A$. También vale la recíproca, puesto que si $B = Z_B A$ y C es un subanillo conmutativo de A que incluye a B , entonces $C \subseteq Z_B A = B$.

Supongamos ahora que A es un anillo de división. Entonces es natural considerar el conjunto de los subanillos de división de A , el cual claramente es cerrado bajo intersecciones. En consecuencia, para cada subconjunto S de A existe un mínimo subanillo de división $Z(S)$ de A que contiene a S , el cual es llamado *el subanillo de división de A generado por S* . De la misma manera que para subanillos, cuando $Z(S) = A$ 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 $Z(1_A)$, llamado *el cuerpo primo de A* , el máximo es A , el ínfimo de una familia es la intersección de sus elementos

y el supremo, el subanillo de división de A generado por la unión de sus elementos. Para cada subanillo de división B de A y cada subconjunto S de A denotamos con $B(S)$ al mínimo subanillo de división de A que contiene a B y a S . Este sería el lugar apropiado para dar ejemplos de subanillos de división, y en particular de subcuerpos, pero de hecho sólo daremos ejemplos de estos últimos. Esto se debe simplemente a que en realidad todavía no hemos dado ningún ejemplo de anillo de división no conmutativo. Más adelante, cuando introduzcamos los cuaterniones, solucionaremos esta falencia.

EJEMPLO 4.17. *Dos de los subanillos del Ejemplo 4.11 son subcuerpos.*

EJEMPLO 4.18. *El subcuerpo $\mathbb{Q}(\sqrt{3})$ 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 $\frac{a-b\sqrt{3}}{a^2-3b^2}$.*

Terminamos esta subsección probando un famoso teorema de Wedderburn que dice que todo anillo de división finito es conmutativo. En la demostración, además de la ecuación de las clases usaremos propiedades básicas de los polinomios ciclotómicos. Por definición para cada $n \in \mathbb{N}$ el n -ésimo polinomio ciclotómico es

$$\phi_n(X) := \prod_{w \in \Omega_n} (X - w_i),$$

donde $\Omega_n \subseteq \mathbb{C}$ denota al conjunto de las raíces n -ésimas primitivas de la unidad. Es evidente que

$$X^n - 1 = \prod_{d|n} \phi_d(X).$$

Un argumento inductivo, usando este hecho, muestra que $\phi_n(X)$ es un polinomio mónico con coeficientes en \mathbb{Z} .

También usaremos implícitamente el siguiente resultado elemental.

LEMA 4.19. *Si $k \subseteq K$ son anillos de división y V es un K -espacio vectorial, entonces*

$$\dim_k(V) = \dim_k(K) \dim_K(V).$$

DEMOSTRACIÓN. Es suficiente ver que si $(u_i)_{i \in I}$ es una base de K como k -espacio vectorial a izquierda y $(w_j)_{j \in J}$ es una base de V como K -espacio vectorial a izquierda, entonces $(u_i w_j)_{i \in I, j \in J}$ es una base de V como k -espacio vectorial a izquierda. Veamos primero que esta última es una familia de generadores de V . Para ello tomemos $v \in V$ arbitrario. Por hipótesis existe una familia $(\lambda_j)_{j \in J}$, de elementos de K , con soporte finito, tal que

$$(26) \quad v = \sum_{j \in J} \lambda_j w_j.$$

Dado que, nuevamente por hipótesis, para cada $\lambda_j \neq 0$ existe una familia $(\alpha_{ij})_{i \in I}$, de elementos de K , con soporte finito, tal que

$$\lambda_j = \sum_{i \in I} \alpha_{ij} u_i,$$

reemplazando cada λ_j por la suma que aparece en el lado derecho de esta igualdad y poniendo $\alpha_{ij} = 0$ para todo i y todo j tal que $\lambda_j = 0$, obtenemos que

$$v = \sum_{j \in J} \left(\sum_{i \in I} \alpha_{ij} u_i \right) w_j = \sum_{i \in I, j \in J} \alpha_{ij} u_i w_j.$$

Veamos ahora que la familia $(u_i w_j)_{i \in I, j \in J}$ es linealmente independiente sobre k . Supongamos que $(\alpha_{ij})_{i \in I, j \in J}$ es una familia de elementos de k , con soporte finito, tal que

$$\sum_{j \in J} \left(\sum_{i \in I} \alpha_{ij} u_i \right) w_j = \sum_{i \in I, j \in J} \alpha_{ij} u_i w_j = 0.$$

Como $(w_j)_{j \in J}$ es linealmente independiente sobre K ,

$$\sum_{i \in I} \alpha_{ij} u_i = 0 \quad \text{para todo } j \in J,$$

y así, dado que $(u_i)_{i \in I}$ es linealmente independiente sobre k , cada α_{ij} es cero. \square

TEOREMA 4.20. *Todo anillo de división finito D es un cuerpo.*

DEMOSTRACIÓN. Denotemos con Z el centro de D y con Z_x al centralizador en D de cada elemento $x \in D$. Sabemos que Z es un cuerpo y que cada Z_x es un anillo de división. Además es evidente que si $q := \#(Z)$, $n_x := \dim_Z(Z_x)$, $m_x := \dim_{Z_x}(D)$ y $n := \dim_Z(D)$, entonces $n = m_x n_x$, $\#(Z_x) = q^{n_x}$ y $\#(D) = q^n = (q^{n_x})^{m_x}$. Es claro también que Z^\times es el centro de D^\times y que Z_x^\times es el centralizador en D^\times de cada elemento $x \in D^\times$. Tomemos un conjunto R de representantes de cada una de las clases de conjugación de D^\times que tienen más de un elemento. La ecuación de las clases de D^\times queda

$$(27) \quad q^n - 1 = \#(D^\times) = \#(Z^\times) + \sum_{x \in R} \frac{\#(D^\times)}{\#(Z_x^\times)} = q - 1 + \sum_{x \in R} \frac{q^n - 1}{q^{n_x} - 1}.$$

Dado que $x \notin Z$ para ningún $x \in R$, sabemos que n_x divide propiamente a n para todo $x \in R$. En consecuencia, tanto $X^n - 1$ como cada uno de los cocientes $\frac{X^n - 1}{X^{n_x} - 1}$ son polinomios divisibles por $\phi_n(X)$ en $\mathbb{Z}[X]$. De esto se sigue inmediatamente que $\phi_n(q)$ divide en \mathbb{Z} , tanto a $q^n - 1$ como a cada uno de los enteros $\frac{q^n - 1}{q^{n_x} - 1}$. Debido a la igualdad (27) tenemos entonces que $\phi_n(q) \mid q - 1$, lo que implica que

$$\prod_{w \in \Omega_n} |q - w| = |\phi_n(q)| \mid q - 1,$$

donde Ω_n es el conjunto de las raíces n -ésimas primitivas de la unidad. Dado que si $n > 1$, entonces $|q - w| > q - 1$ para cada $w \in \Omega_n$, se deduce de aquí que $n = 1$ y, así, $D = Z$. \square

3. Ideales

Un subconjunto $I \neq \emptyset$ de A es un *ideal a izquierda* si es cerrado para la suma y $ax \in I$ para todo $a \in A$ y $x \in I$, y es un *ideal a derecha* si es cerrado para la suma y $xa \in I$ para todo $a \in A$ y $x \in I$ o, equivalentemente, si es un ideal a izquierda de A^{op} . Si I es un ideal a izquierda y a derecha, entonces decimos que es un *ideal bilátero* de A . Frecuentemente nos referiremos a estos últimos simplemente como ideales. Evidentemente 0 y A son ideales de A . Estos son los llamados *ideales triviales*. Un ideal a izquierda, a derecha o bilátero de A es *propio* si es distinto de A . Es claro que la intersección de una familia arbitraria de ideales a izquierda, derecha o biláteros de A es un ideal del mismo tipo. Por ejemplo, para cada subconjunto S de A , la intersección de los ideales a izquierda de A que incluyen a S es el mínimo ideal a izquierda AS de A que contiene a S . Este es llamado el *ideal a izquierda de A generado por S* . Como es usual, para cada $x \in A$, escribimos Ax en lugar de $A\{x\}$. Los *ideales*

a derecha y *bilátero* de A generados por S (las definiciones son evidentes) serán denotados SA y ASA o $\langle S \rangle$, respectivamente. Por supuesto, escribimos xA en lugar de $\{x\}A$ y AxA en lugar de $A\{x\}A$. Es fácil ver que AS es el conjunto de todas las sumas finitas de elementos de la forma as , con $s \in S$ y $a \in A$. Similarmente, SA consiste de las sumas finitas de elementos de la forma sa , con $s \in S$ y $a \in A$, y ASA , de las sumas finitas de productos asb , con $a, b \in A$ y $s \in S$. En general $\{axb : a, b \in A\}$, donde x es un elemento fijo de A , no es un ideal bilátero de A . Por ejemplo, en $M_2(\mathbb{Q})$ el conjunto formado por los productos

$$(28) \quad \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} \\ a_{21}b_{11} & a_{21}b_{12} \end{pmatrix},$$

no es un ideal bilátero, porque $M_2(\mathbb{Q})$ no tiene ideales biláteros no triviales (vease la Proposición 4.26) y la expresión (28) 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.

PROPOSICIÓN 4.21. *Un ideal a izquierda, derecha o bilátero propio de un anillo A está incluido en un ideal maximal del mismo tipo de A .*

DEMOSTRACIÓN. Supongamos por ejemplo que $I \subsetneq A$ es un ideal a izquierda de A y consideremos el conjunto \mathcal{P} de los ideales a izquierda propios de A que contienen a I . Notemos que \mathcal{P} no es vacío pues $I \in \mathcal{P}$. Por el lema de Zermelo podemos tomar una cadena maximal $(I_i)_{i \in I}$ de elementos de \mathcal{P} . Dado que evidentemente no hay ningún ideal propio de A que contiene a todos los I_i , el teorema quedará probado si podemos ver que $\bigcup I_i$ es propio. Pero esto es claramente así, pues si 1 está en esta unión, entonces $1 \in I_i$ para algún $i \in I$, lo que se contradice con que I_i es propio. \square

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. $I_i \cap \sum_{j \in J \setminus \{i\}} I_j = 0$ para cada $i \in J$.

Decimos que un ideal a izquierda I de un anillo A es un *sumando directo* de otro ideal a izquierda J de A que lo contiene, si existe un ideal a izquierda I' de A tal que $J = I \oplus I'$. Usualmente I' no es único.

Para los ideales a derecha y biláteros se pueden dar definiciones similares y probar resultados análogos. Dejamos los detalles al lector.

Como ocurre con el conjunto de los subanillos, los conjuntos de los ideales a izquierda, a derecha y biláteros de un anillo A son reticulados completos vía el orden dado por la inclusión.

En los tres casos el mínimo es el ideal nulo, el máximo es A , el ínfimo de una familia es la intersección de sus elementos y el supremo es la suma. En general estos reticulados no son distributivos, pero siempre son modulares. En otras palabras,

$$I \cap (J + K) = J + I \cap K,$$

para cada terna de ideales a izquierda, derecha o biláteros (pero, por supuesto, todos del mismo tipo) I, J y K de A tales que $J \subseteq I$. En efecto, es inmediato que $I \cap (J + K) \supseteq J + I \cap K$. Para probar que vale la inclusión recíproca, basta observar que si una suma $a = b + c$, de elementos $b \in J$ y $c \in K$, está en I , entonces $c = a - b \in I \cap K$.

EJEMPLO 4.22. *Es evidente que cada ideal no nulo I de \mathbb{Z} tiene un mínimo número natural n_0 . Afirmamos que $I = \langle n_0 \rangle$. En efecto, por el algoritmo de división, para cada $a \in I$ existen $q, r \in \mathbb{Z}$ con $0 \leq r < n_0$ tales que $a = qn_0 + r$. Por la minimalidad de n_0 , como $r = a - qn_0 \in I$, debe ser $r = 0$. Esto muestra que todo ideal de \mathbb{Z} es cíclico. Un argumento similar muestra que el anillo $k[X]$, de polinomios con coeficientes en un cuerpo k , tiene la misma propiedad.*

EJERCICIO 4.23. *Pruebe que la suma e intersección de ideales en \mathbb{Z} están dadas por*

$$\langle m \rangle + \langle n \rangle = \langle (m; n) \rangle \quad \text{y} \quad \langle m \rangle \cap \langle n \rangle = \langle [m; n] \rangle,$$

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 4.22 mostramos que los anillos de enteros y de polinomios en una variable sobre un cuerpo 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 4.24. *Pruebe que si $A[X]$ es un dominio principal, entonces A es un cuerpo.*

PROPOSICIÓN 4.25. *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. \square

PROPOSICIÓN 4.26. *Si D es un anillo de división, entonces los únicos ideales biláteros de $M_n(D)$ son los triviales.*

DEMOSTRACIÓN. Para cada $1 \leq i, j \leq n$, llamemos E_{ij} a la matriz de $n \times n$ cuya único coeficiente no nulo es el (i, j) -ésimo, que vale 1. Basta observar que si un ideal I de $M_n(D)$ tiene un elemento no nulo

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix},$$

y $a_{ij} \neq 0$, entonces $\text{id} = \sum_{l=1}^n a_{ij}^{-1} E_{li} A E_{jl} \in I$. □

4. Morfismos de anillos

Un *morfismo de anillos* $f: A \rightarrow B$ 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 $f: A \rightarrow B$, y B es el *codominio*. Por ejemplo, la identidad $\text{id}_A: A \rightarrow A$ y, más generalmente, la inclusión canónica $i: B \rightarrow A$, de un subanillo B de A en A , es un morfismo de anillos. También lo es la composición $g \circ f: A \rightarrow A''$ de dos morfismos $f: A \rightarrow A'$ y $g: A' \rightarrow A''$.

Muchas de las propiedades básicas de los morfismos de anillos son análogas a las establecidas para los de monoides y grupos. Las definiciones de endomorfismo, isomorfismo, automorfismo, monomorfismo, epimorfismo, sección y retracción son las mismas. Un argumento sencillo prueba que un morfismo es un isomorfismo si y sólo si es biyectivo. Mantenemos la notación $A \simeq A'$ para señalar que los anillos A y A' son isomorfos. Es fácil ver que los monomorfismos, epimorfismos, secciones y retracciones son cerrados bajo la composición, que toda retracción es sobreyectiva, toda sección, inyectiva, todo morfismo inyectivo, un monomorfismo, y todo morfismo sobreyectivo, un epimorfismo. También que un morfismo $f: A \rightarrow A'$ 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 $f: A \rightarrow A'$ es inyectivo. En efecto, si $f(a) = f(a')$, entonces $f \circ g = f \circ g'$, donde $g, g': \mathbb{Z}[X] \rightarrow A$ son los morfismos definidos por

$$g(P) = P(a) \quad \text{y} \quad g'(P) = P(a') \quad \text{para todo polinomio } P.$$

Por lo tanto $g = g'$ y entonces $a = a'$. Pero, como lo muestra el primero de los ejemplos dados abajo, es falso que un epimorfismo deba ser sobreyectivo.

Fijemos morfismos $f: A \rightarrow A'$ y $g: A' \rightarrow A''$. De la misma manera que en la teoría de monoides y grupos, vale que:

1. Si $g \circ f$ es una sección, un monomorfismo, o un morfismo inyectivo, entonces también lo es f .
2. Si $g \circ f$ es una retracción, un epimorfismo, o un morfismo sobreyectivo, entonces también lo es g .

Los símbolos $\text{Hom}(A, A')$, $\text{Iso}(A, A')$, $\text{End}(A)$ y $\text{Aut}(A)$ denotan respectivamente a los conjuntos de morfismos de A en A' , isomorfismos de A en A' , endomorfismos de A y automorfismos de A . Es inmediato que $\text{End}(A)$ es un monoide (cuyo elemento neutro es la función identidad) vía la composición y que $\text{Aut}(A)$ es su grupo de unidades.

EJEMPLOS 4.27. Hay epimorfismos inyectivos que no son sobreyectivos y morfismos sobreyectivos que no son retracciones. En efecto:

1. La inclusión canónica $\iota: \mathbb{Z} \rightarrow \mathbb{Q}$ es un epimorfismo porque si $g, h: \mathbb{Q} \rightarrow C$ son morfismos de anillos tales que $g \circ \iota = h \circ \iota$, entonces

$$g(m/n) = g(m)g(n)^{-1} = h(m)h(n)^{-1} = h(m/n)$$

para todo $m/n \in \mathbb{Q}$. Por otra parte no existe ningún morfismo $\pi: \mathbb{Q} \rightarrow \mathbb{Z}$ pues $\pi(1/2)$ debería satisfacer $2\pi(1/2) = \pi(1) = 1$, lo cual es imposible. En particular ι no es una sección.

2. La aplicación $\pi: \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$, definida por $\pi(0) := \pi(2) := 0$ y $\pi(1) := \pi(3) := 1$, es sobreyectiva, pero no es una retracción.

EJEMPLO 4.28. Para cada anillo A hay un único morfismo $\iota: \mathbb{Z} \rightarrow A$. Es fácil ver que la imagen de ι es el anillo primo $\mathbb{Z}\{1_A\}$ de A . También es fácil ver que

$$\mathbb{Z}\{1_A\} \simeq \begin{cases} \mathbb{Z} & \text{si } n1_A \neq 0 \text{ para todo } n \in \mathbb{N}, \\ \mathbb{Z}/n\mathbb{Z} & \text{si no, donde } n \in \mathbb{N} \text{ es el mínimo natural tal que } n1_A = 0. \end{cases}$$

En el primer caso decimos que la característica de A es cero y en el segundo que es n . Es inmediato que un subanillo de un dominio es un dominio. En consecuencia, como $\mathbb{Z}/n\mathbb{Z}$ tiene divisores de cero si n no es primo, la característica de un dominio es necesariamente un número primo o cero.

EJEMPLO 4.29. Como $f(1) = 1$, un morfismo $f: \mathbb{Z}[i] \rightarrow A$, del anillo de enteros de Gauss en un anillo A , queda completamente determinado por la imagen de i . Puesto que $i^2 = -1$, debe ser $f(i)^2 = f(-1) = -1$. Además este es el único requisito que debe satisfacer $f(i)$. De modo que hay una correspondencia biunívoca entre $\text{Hom}(\mathbb{Z}[i], A)$ y $\{a \in A : a^2 = -1\}$. Cuando $A = \mathbb{Z}[i]$, este conjunto es $\{i, -i\}$. Como los endomorfismos obtenidos, son los automorfismos identidad y conjugación, $\text{Aut}(\mathbb{Z}[i]) = \text{End}(\mathbb{Z}[i])$ es un grupo cíclico de orden 2.

EJEMPLO 4.30. Para cada $n, m \in \mathbb{N}$ la aplicación

$$M_{n \times m}(A^{\text{op}}) \rightarrow M_{m \times n}(A),$$

que a cada matriz B le asigna su transpuesta tB , satisface

$${}^t(B + C) = {}^tB + {}^tC \quad \text{para todo } B, C \in M_{n \times m}(A^{\text{op}})$$

y

$${}^t(BC) = {}^tC{}^tB \quad \text{para todo } B \in M_{n \times m}(A^{\text{op}}) \text{ y } C \in M_{m \times l}(A^{\text{op}}).$$

En particular $M_n(A^{\text{op}}) \simeq M_n(A)^{\text{op}}$.

EJEMPLO 4.31. Para cada morfismo de anillos $f: A \rightarrow B$ y cada $n \in \mathbb{N}$, la aplicación

$$M_n(f): M_n(A) \rightarrow M_n(B),$$

definida por $M_n(f)((a_{ij})) := (f(a)_{ij})$, es un morfismo de anillos.

EJEMPLO 4.32. La aplicación $\theta: \mathbb{C} \rightarrow M_2(\mathbb{R})$, dada por

$$\theta(a + bi) := \begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

es un monomorfismo de anillos. Por lo tanto \mathbb{C} es isomorfo a un subanillo de $M_2(\mathbb{R})$. Notemos que $\det(\theta(z)) = |z|^2$ para todo $z \in \mathbb{C}$ y que si $S^1 := \{z \in \mathbb{C} : |z| = 1\}$, entonces $\theta(S^1) = \text{SO}(2)$, donde $\text{SO}(2) := \text{SO}(\mathbb{R}^2)$, es el grupo ortogonal del espacio euclideo usual \mathbb{R}^2 .

5. Núcleo e imagen

El núcleo $\ker f$ de un morfismo de anillos $f: A \rightarrow B$ es la preimagen de 0 por f . Es evidente que $\ker f$ es un ideal de A e $\text{Im } f$ 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

$$f^{-1}(f(I)) = I + \ker f \quad \text{y} \quad f(f^{-1}(J)) = J \cap \text{Im } f,$$

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 4.33. *Un morfismo de anillos $f: A \rightarrow B$, manda $a, a' \in A$ al mismo elemento de B si y sólo si $a - a' \in \ker f$. En particular, f es inyectiva si y sólo si $\ker f = 0$.*

6. Cociente de anillos por ideales

Fijados un anillo A y un subgrupo aditivo I de A , consideremos el grupo cociente A/I de A por I . Recordemos que para cada $a \in A$, el símbolo $[a]$ denota a la clase de a en A/I y que la proyección canónica $\pi: A \rightarrow A/I$ es un morfismo de grupos. Afirmamos que A/I tiene un producto tal que π es un morfismo de anillos si y sólo si I es un ideal de A . Para que π respete el producto, forzosamente la multiplicación de A/I deberá estar 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 $\pi: A \rightarrow A/I$ tiene la siguiente propiedad, llamada *propiedad universal del cociente*:

- Para cada morfismo de anillos $f: A \rightarrow B$ tal que $I \subseteq \ker f$ existe un único morfismo de anillos $\bar{f}: A/I \rightarrow B$ tal que el triángulo

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \pi & \nearrow \bar{f} & \\ A/I & & \end{array}$$

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 1.82 sabemos que $\ker \bar{f} = \pi(\ker f)$ e $\text{Im } \bar{f} = \text{Im } f$. En particular, $A/\ker f$ es isomorfo a $\text{Im } f$. Además, como grupo aditivo, $\pi(\ker f) = \ker f/I$.

OBSERVACIÓN 4.34. *Una manera equivalente de formular la propiedad universal del cociente es decir que la correspondencia*

$$\begin{array}{ccc} \text{Hom}(A/I, B) & \longrightarrow & \text{Hom}(A, B) \\ f & \longmapsto & f \circ \pi \end{array}$$

es inyectiva y su imagen es $\{f \in \text{Hom}(A, B) : f(I) = 0\}$.

OBSERVACIÓN 4.35. *Por la propiedad universal del cociente, si I y J son ideales de un anillo A tales que $I \subseteq J$, entonces existe un único morfismo $\bar{\pi}_J: A/I \rightarrow A/J$ tal que el triángulo*

$$\begin{array}{ccc} A & \xrightarrow{\pi_J} & A/J \\ \downarrow \pi_I & \nearrow \bar{\pi}_J & \\ A/I & & \end{array},$$

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 $(A/I)/(J/I) \simeq A/J$.

OBSERVACIÓN 4.36. *Supongamos que $f: A \rightarrow B$ es un morfismo de anillos y que J es un ideal de B . Denotemos con $\tilde{f}: A \rightarrow B/J$ a la composición de f con la proyección canónica $\pi: B \rightarrow B/J$. Es evidente que $\text{Im } \tilde{f} = (f(A) + J)/J$ y $\ker \tilde{f} = f^{-1}(J)$. En consecuencia, por la propiedad universal del cociente, \tilde{f} induce un isomorfismo $\bar{f}: A/f^{-1}(J) \rightarrow (f(A) + J)/J$. En particular, si A es un subanillo de B , entonces $A/(A \cap J) \simeq (A + J)/J$.*

EJERCICIO 4.37. *Pruebe que si $f: A \rightarrow B$ es un morfismo sobreyectivo de anillos e I es un ideal de A , entonces $A/(I + \ker f) \simeq B/f(I)$.*

OBSERVACIÓN 4.38. Consideremos un ideal I de un anillo A . Del isomorfismo que hay entre el reticulado de los ideales de A que contienen a I y el de los ideales de A/I se sigue que I es maximal si y sólo si $A/I \neq 0$ y no tiene ideales no triviales. En particular, debido a la Proposición 4.25, si A es conmutativo, entonces I es maximal si y sólo si A/I es un cuerpo.

COROLARIO 4.39. 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 4.25, es un cuerpo. Es evidente que podemos tomar como el morfismo en cuestión, la proyección canónica de A en A/I . \square

PROPOSICIÓN 4.40. Consideremos un morfismo de anillos $f: A \rightarrow B$. Si I y J son ideales de A y B tales que $f(I) \subseteq J$, entonces existe un único morfismo de anillos $\bar{f}: A/I \rightarrow B/J$ tal que el diagrama

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

donde $\pi_I: A \rightarrow A/I$ y $\pi_J: B \rightarrow B/J$ son las proyecciones canónicas, conmuta. Además, $\text{Im } \bar{f} = (J + \text{Im } f)/J$ y $\ker \bar{f} = f^{-1}(J)/I$.

DEMOSTRACIÓN. Es una consecuencia inmediata de la propiedad universal de π_I y de que $\text{Im}(\pi_J \circ f) = \pi_J(\text{Im } f)$ y $\ker(\pi_J \circ f) = f^{-1}(J)$. \square

OBSERVACIÓN 4.41. La correspondencia introducida en la proposición anterior tiene las siguientes propiedades:

1. $\text{id}_A: A/I \rightarrow A/I$ es la aplicación identidad de A/I .
2. Si $f: A \rightarrow B$ y $g: B \rightarrow C$ 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

$$g(f(I)) \subseteq K \quad \text{y} \quad \overline{g \circ f} = \bar{g} \circ \bar{f}.$$

EJERCICIO 4.42. Pruebe que si $f: A \rightarrow B$ es un morfismo de anillos y J es un ideal de B , entonces existe un único morfismo inyectivo $\bar{f}: A/I \rightarrow B/J$, donde $I = f^{-1}(J)$, tal que el diagrama

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

en el cual $\pi_I: A \rightarrow A/I$ y $\pi_J: B \rightarrow B/J$ son las proyecciones canónicas, conmuta. Pruebe además que $\text{Im } \bar{f} = (f(A) + J)/J$.

7. Ideales primos en anillos conmutativos

Un ideal propio I de un anillo conmutativo A es *primo* si $ab \in I$ implica $a \in I$ o $b \in I$.

OBSERVACIÓN 4.43. *Un ideal principal $\langle p \rangle$ de un anillo conmutativo A es primo si y sólo si p no es una unidad de A y $p \mid ab$ implica $p \mid a$ o $p \mid b$.*

PROPOSICIÓN 4.44. *Para cada ideal I de un anillo conmutativo A son equivalentes:*

1. I es primo,
2. A/I es un dominio.

DEMOSTRACIÓN. 1) \Rightarrow 2). Como I es propio, $A/I \neq 0$. Supongamos ahora que $[a][a'] = 0$, donde como venimos haciendo denotamos con $[a]$ y $[a']$ a la clase en A/I de dos elementos a y a' de A . Como $[aa'] = [a][a']$ se sigue de esto que $aa' \in I$ y, en consecuencia $a \in I$ o $a' \in I$. Pero entonces $[a] = 0$ o $[a'] = 0$, de donde I es primo.

2) \Rightarrow 1). Dado que $A/I \neq 0$ el ideal I es propio. Supongamos que $a, a' \in A$ satisfacen $aa' \in I$. Entonces $[a][a'] = [aa'] = 0$ en A/I y, en consecuencia, debido a la hipótesis $[a] = 0$ o $[a'] = 0$. Pero esto significa que $a \in I$ o $a' \in I$ y, por lo tanto, I es primo. \square

COROLARIO 4.45. *Todo ideal maximal de un anillo conmutativo es primo.*

DEMOSTRACIÓN. Como todo cuerpo es un dominio esto se sigue de la proposición anterior y de la Observación 4.38. \square

PROPOSICIÓN 4.46. *Si $f: A \rightarrow B$ es un morfismo de anillos y $J \subsetneq B$ es un ideal primo de B , entonces $f^{-1}(J)$ es un ideal primo de A .*

DEMOSTRACIÓN. Como un subanillo de un dominio es un dominio esto se sigue de la Proposición 4.44 y de que $A/f^{-1}(J)$ es un subanillo de B/J . \square

Notemos que la proposición anterior no se satisface para ideales maximales. Por ejemplo el ideal 0 de \mathbb{Q} es maximal, pero su preimagen por la inclusión canónica $\iota: \mathbb{Z} \rightarrow \mathbb{Q}$ sigue siendo 0 , que no es un ideal maximal de \mathbb{Z} .

PROPOSICIÓN 4.47. *Si $f: A \rightarrow B$ es un morfismo sobreyectivo de anillos e $I \subsetneq A$ es un ideal primo de A que contiene al núcleo de f , entonces $f(I)$ es un ideal primo de B .*

DEMOSTRACIÓN. Dado que, debido a las hipótesis A/I es isomorfo a $B/f(I)$, esto se sigue inmediatamente de la Proposición 4.44. \square

8. 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 coordinada a coordinada. Las proyecciones canónicas $\pi_j: \prod_{i \in I} A_i \rightarrow A_j$ son morfismos de anillos, y las definiciones de suma y producto están forzadas por este requisito. Tal como cuando trabajamos con grupos, si no hay posibilidad de confusión escribiremos $\prod A_i$ en lugar de $\prod_{i \in I} A_i$, y haremos otras simplificaciones similares siempre que, como consecuencia de las mismas, no se pierda claridad en la exposición. Además, escribiremos $A_1 \times \cdots \times A_n$ en lugar de $\prod_{i \in \mathbb{I}_n} A_i$, donde \mathbb{I}_n denota al conjunto de los primeros n números naturales.

El producto directo tiene la siguiente propiedad universal:

- Para cada familia $(f_i: A \rightarrow A_i)_{i \in I}$ de morfismos de anillos, existe un único morfismo de anillos $\mathbf{f}: A \rightarrow \prod A_i$ tal que, para cada $j \in I$, el diagrama

$$\begin{array}{ccc} A & & \\ \downarrow \mathbf{f} & \searrow f_j & \\ \prod A_i & \xrightarrow{\pi_j} & A_j \end{array}$$

conmuta. Claramente $\mathbf{f}(a) = (f_i(a))_{i \in I}$ y $\ker \mathbf{f} = \bigcap \ker(f_i)$.

EJERCICIO 4.48. Muestre que si $A = \prod A_j$, entonces $A^\times = \prod A_j^\times$.

PROPOSICIÓN 4.49. Para cada familia de morfismos de anillos $(f_j: A_j \rightarrow B_j)_{j \in J}$, existe un único morfismo de anillos

$$\prod f_j: \prod A_j \rightarrow \prod B_j,$$

tal que los diagramas

$$\begin{array}{ccc} \prod A_j & \xrightarrow{\prod f_j} & \prod B_j \\ \downarrow \pi_i & & \downarrow \pi_i \\ A_i & \xrightarrow{f_i} & B_i \end{array}$$

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 $(f_j(a_j))_{j \in J}$ y, usando esto, que

$$\ker\left(\prod f_j\right) = \prod \ker(f_j) \quad \text{y} \quad \text{Im}\left(\prod f_j\right) = \prod \text{Im}(f_j).$$

Por ejemplo para cada familia $(A_i)_{i \in I}$ de anillos y cada familia $(I_i)_{i \in I}$ con I_i un ideal bilátero de A_i para cada $i \in I$, las proyecciones canónicas $\pi_i: A_i \rightarrow A_i/I_i$ inducen un isomorfismo

$$\frac{\prod A_i}{\prod I_i} \longrightarrow \prod \frac{A_i}{I_i}.$$

OBSERVACIÓN 4.50. La correspondencia introducida en la Proposición 4.49 tiene las siguientes propiedades:

1. $\prod \text{id}_{A_j} = \text{id}_{\prod A_j}$.
2. Para cada par $(f_j: A_j \rightarrow B_j)_{j \in J}$ y $(g_j: B_j \rightarrow C_j)_{j \in J}$ 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 $A = A_1 \times \cdots \times A_n$. Para cada ideal a izquierda, a derecha o bilátero I de A y cada $1 \leq j \leq n$ escribamos

$$I_j := \{a_j \in A_j : (0, \dots, 0, a_j, 0, \dots, 0) \in I\}.$$

Es evidente que $I_1 \times \cdots \times I_n \subseteq I$. Afirmamos que

$$(29) \quad I = I_1 \times \cdots \times I_n.$$

En efecto, supongamos por ejemplo que I es un ideal a izquierda. Para cada $i \leq n$, 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 (29) se sigue inmediatamente. Notemos ahora que, debido a esta igualdad, sabemos que $I_j = \pi_j(I)$ para todo $j \in J$ y que 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 $j \neq i$.

8.1. 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 .

Para cada familia I_1, \dots, I_n de ideales de A , las proyecciones canónicas $\pi_i: A \rightarrow A/I_i$ inducen un morfismo

$$\pi: A \rightarrow \prod_{j=1}^n \frac{A}{I_j}.$$

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 4.51 (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 . □

9. El anillo de un monoide

Para cada anillo A y cada un monoide S , el conjunto $A^{(S)}$, de las funciones $\varphi: S \rightarrow A$ que tienen soporte finito, es un anillo, llamado *el anillo del monoide S con coeficientes en A* , y denotado $A[S]$, vía la suma coordenada a coordenada

$$(\varphi + \psi)(s) := \varphi(s) + \psi(s),$$

y el producto de convolución

$$(\varphi\psi)(s) := \sum_{\substack{u,v \in S \\ uv=s}} \varphi(u)\psi(v).$$

En efecto, ya sabemos que $A^{(S)}$ es un grupo abeliano vía la suma. Es el producto directo restringido de $|S|$ copias del grupo aditivo subyacente de A . El producto $\varphi\psi$ está bien definido porque la familia $(\varphi(u)\psi(v))_{u,v \in S}$ tiene soporte finito. Las igualdades

$$\begin{aligned} ((\varphi\psi)\vartheta)(s) &= \sum_{\substack{u,v \in S \\ uv=s}} \varphi\psi(u)\vartheta(v) \\ &= \sum_{\substack{u,v \in S \\ uv=s}} \left(\sum_{\substack{p,q \in S \\ pq=u}} \varphi(p)\psi(q) \right) \vartheta(v) \\ &= \sum_{\substack{x,y,z \in S \\ xyz=s}} \varphi(x)\psi(y)\vartheta(z) \\ &= \sum_{\substack{u,v \in S \\ uv=s}} \varphi(u) \left(\sum_{\substack{p,q \in S \\ pq=v}} \psi(p)\vartheta(q) \right) \\ &= \sum_{\substack{u,v \in S \\ uv=s}} \varphi(u)\psi\vartheta(v) \\ &= (\varphi(\psi\vartheta))(s) \end{aligned}$$

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 $1: S \rightarrow A$, 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 $as: S \rightarrow A$ 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

$$(30) \quad \sum_{s \in S} a_s s,$$

con soporte finito. Una expresión como (30) 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

$$\sum_{s \in S} a_s s + \sum_{s \in S} b_s s = \sum_{s \in S} (a_s + b_s) s \quad \text{y} \quad \left(\sum_{s \in S} a_s s \right) \left(\sum_{s \in S} b_s s \right) = \sum_{s \in S} \left(\sum_{\substack{u, v \in S \\ uv = s}} a_u b_v \right) s,$$

respectivamente.

La función $\iota_A: A \rightarrow A[S]$, definida por $\iota_A(a) := a1_S$ es un morfismo inyectivo de anillos, y la función $\iota_S: S \rightarrow A[S]$, 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 $f: A \rightarrow B$ es un morfismo de anillos y $\psi: S \rightarrow B$ 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 $f\psi: A[S] \rightarrow B$, tal que los triángulos

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \iota_A & \nearrow f\psi & \\ A[S] & & \end{array} \quad \text{y} \quad \begin{array}{ccc} S & \xrightarrow{\psi} & B \\ \downarrow \iota_S & \nearrow f\psi & \\ A[S] & & \end{array}$$

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 4.52. La aplicación trivial $\psi: S \rightarrow A$, definida por $\psi(s) := 1$ para todo $s \in S$, induce un morfismo $\varepsilon: A[S] \rightarrow A$, que es llamado el morfismo de aumentación de $A[S]$. Es evidente que

$$\varepsilon \left(\sum_{s \in S} a_s s \right) = \sum_{s \in S} a_s.$$

Al núcleo I_+ , de ε , se lo denomina el ideal de aumentación de $A[S]$. Es fácil ver que

$$I_+ = \sum_{s \in S} A(s - 1_S).$$

En efecto, es evidente que $\sum_{s \in S} A(s-1) \subseteq I_+$ y, como por otro lado,

$$\sum_{s \in S} a_s = 0 \implies \sum_{s \in S} a_s s = \sum_{s \in S} a_s s - \left(\sum_{s \in S} a_s \right) 1_S = \sum_{s \in S} a_s (s - 1_S),$$

también vale la inclusión inversa.

EJEMPLO 4.53. Para cada grupo G la aplicación $\psi: G \rightarrow A[G]^{\text{op}}$, definida por $\psi(g) := g^{-1}$, es un morfismo de G en el monoide multiplicativo de $A[G]^{\text{op}}$. Por lo tanto induce el morfismo de anillos

$$\begin{aligned} A^{\text{op}}[G] &\xrightarrow{f} A[G]^{\text{op}} \quad , \\ \sum_g \lambda_g g &\longmapsto \sum_g \lambda_g g^{-1} \end{aligned}$$

que es biyectivo porque la aplicación antipodal de G , introducida en el Ejemplo 1.61 del Capítulo 1, lo es. En particular, si A es conmutativo, entonces $A[G]^{\text{op}}$ es isomorfo a $A[G]$.

PROPOSICIÓN 4.54. Para cada par de anillos A_1 y A_2 y cada monoide S , hay un isomorfismo de anillos

$$\Theta: (A_1 \times A_2)[S] \rightarrow A_1[S] \times A_2[S],$$

que aplica $(a_1, a_2)s$ en (a_1s, a_2s) .

DEMOSTRACIÓN. Consideremos la inclusión canónica $\iota: A_1 \times A_2 \rightarrow A_1[S] \times A_2[S]$ y el morfismo de monoide $\psi: S \rightarrow (A_1[S] \times A_2[S])^\times$, dado por $\psi(s) := (s, s)$. Por la propiedad universal de $(A_1 \times A_2)[S]$ los morfismos ι y ψ se extienden a un morfismo

$$\Theta: (A_1 \times A_2)[S] \rightarrow A_1[S] \times A_2[S],$$

tal que $\Theta((a_1, a_2)s) = (a_1s, a_2s)$. Es evidente que Θ es inyectivo y, dado que $(a_1s, 0)$ y $(0, a_2s)$ están en la imagen de Θ , para todo $a_1 \in A_1, a_2 \in A_2$ y $s \in S$, que también es sobreyectivo. \square

PROPOSICIÓN 4.55. Para cada anillo A y cada par de monoide S y T , hay un isomorfismo de anillos

$$\Theta: A[S][T] \rightarrow A[S \times T],$$

que aplica $(as)t$ en $a(s, t)$.

DEMOSTRACIÓN. Por la propiedad universal de $A[S]$ hay un único morfismo

$$\Phi: A[S] \rightarrow A[S \times T],$$

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 se extiende al morfismo Θ buscado. Es fácil ver que Θ es biyectivo. \square

PROPOSICIÓN 4.56. Para cada morfismo de anillos $f: A \rightarrow B$ y cada morfismo de monoide $\psi: S \rightarrow T$, existe un único morfismo de anillos $f[\psi]: A[S] \rightarrow B[T]$, tal que los diagramas

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \iota_A & & \downarrow \iota_B \\ A[S] & \xrightarrow{f[\psi]} & B[T] \end{array} \quad y \quad \begin{array}{ccc} S & \xrightarrow{\psi} & T \\ \downarrow \iota_S & & \downarrow \iota_T \\ A[S] & \xrightarrow{f[\psi]} & B[T], \end{array}$$

donde

$$\iota_A: A \rightarrow A[S], \quad \iota_B: B \rightarrow B[T], \quad \iota_S: S \rightarrow A[S] \quad e \quad \iota_T: T \rightarrow B[T]$$

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 $A[S]$. \square

OBSERVACIÓN 4.57. Es evidente que $\text{Im}(f[\psi]) = f(A)[\psi(S)]$ y que el núcleo de $f[\psi]$ es la suma directa de la familia $(F_t)_{t \in \text{Im}(\psi)}$, de subgrupos aditivos de $A[S]$, definida por

$$F_t := \left\{ \sum_{s \in \psi^{-1}(t)} a_s s : \sum_{s \in \psi^{-1}(t)} f(a_s) = 0 \right\}.$$

Notemos ahora que para cada $s_t \in \psi^{-1}(t)$,

$$(31) \quad F_t = \ker(f)_{s_t} \oplus \bigoplus_{s \in \psi^{-1}(t) \setminus \{s_t\}} A(s - s_t).$$

En efecto es evidente que

$$\ker(f)_{s_t} \subseteq F_t \quad \text{y que} \quad A(s - s_t) \subseteq F_t \quad \text{para cada } s \in \psi^{-1}(t) \setminus \{s_t\}.$$

Por otro lado si

$$\sum_{s \in \psi^{-1}(t)} a_s s \in F_t,$$

entonces

$$\sum_{s \in \psi^{-1}(t)} a_s s = \left(\sum_{s \in \psi^{-1}(t)} a_s \right) s_t + \sum_{s \in \psi^{-1}(t) \setminus \{s_t\}} a_s (s - s_t)$$

está en el lado derecho de (31). Supongamos ahora que para $t \in \text{Im} \psi$ existe $s_t \in \psi^{-1}(t)$ tal que $\psi^{-1}(t) = s_t \ker \psi$ (si S es un grupo esta condición se satisface para todo $t \in \text{Im} \psi$ y todo $s_t \in \psi^{-1}(t)$). Entonces

$$\bigoplus_{s \in \psi^{-1}(t) \setminus \{s_t\}} A(s - s_t) = \bigoplus_{s \in \ker \psi \setminus \{e\}} A s_t (s - 1_S).$$

Supongamos además que $\ker \psi$ está generado como monoide por U y por inversos de elementos de U . Dado que $(u_i)_{i=1, \dots, n}$ formada por elementos de U o inversos de elementos de U ,

$$u_1 \cdots u_r - 1_S = \sum_{i=1}^r u_1 \cdots u_{i-1} (u_i - 1_S) \quad \text{y} \quad u^{-1} - 1_S = -u^{-1} (u - 1_S),$$

se sigue que

$$s - 1_S \in \sum_{u \in U} \ker(\psi)(u - 1_S) \quad \text{para todo } s \in \ker \psi \setminus \{1_S\},$$

y así,

$$\bigoplus_{s \in \psi^{-1}(t) \setminus \{s_t\}} A(s - s_t) = \bigoplus_{s \in \ker \psi \setminus \{1_S\}} A s_t (s - 1_S) = \sum_{u \in U} A s_t \ker(\psi)(u - 1_S).$$

Por lo tanto si $\ker \psi$ está generado como monoide por U y por inversos de elementos de U y para cada $t \in \text{Im } \psi$ existe $s_t \in \psi^{-1}(t)$ tal que $\psi^{-1}(t) = s_t \ker \psi$, entonces

$$\begin{aligned} \ker(f[\psi]) &= \bigoplus_{t \in \text{Im } \psi} \left[\ker(f)_{s_t} \oplus \left(\sum_{u \in U} A s_t \ker(\psi)(u - 1_S) \right) \right] \\ &= \bigoplus_{t \in \text{Im } \psi} \ker(f)_{s_t} \oplus \sum_{u \in U} A[S](u - 1_S). \end{aligned}$$

En particular si f es inyectivo, entonces

$$\ker(f[\psi]) = \sum_{u \in U} A[S](u - 1_S)$$

es el ideal de $A[S]$ generado por los elementos $u - 1_S$ con $u \in U$. Todo esto se aplica en particular al ideal de aumentación. En este caso $f - \text{id}_A$ y $\psi: S \rightarrow 1$ es el morfismo trivial, por lo que

$$I_+ = \sum_{u \in U} A[S](u - 1_S)$$

para cada conjunto U de elementos de S tal que S está generado por U y por inversas de elementos de U .

OBSERVACIÓN 4.58. La correspondencia introducida en la proposición anterior tiene las siguientes propiedades:

1. $\text{id}_A[\text{id}_S] = \text{id}_{A[S]}$.
2. Para cada par de morfismos de anillos $f: A \rightarrow B$ y $g: B \rightarrow C$ y cada par de morfismos de monoides $\psi: S \rightarrow T$ y $\vartheta: T \rightarrow L$,

$$g[\vartheta] \circ f[\psi] = (g \circ f)[\vartheta \circ \psi].$$

EJEMPLO 4.59. Para cada número natural r , denotemos con \mathbb{N}_0^r al monoide formado por todas las r -uplas de enteros mayores o iguales que cero, con la suma coordenada a coordenada. Introduciendo variables X_1, \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 $A[\mathbb{N}_0^r]$ y de polinomios $A[X_1, \dots, X_r]$ coinciden.

PROPOSICIÓN 4.60. 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 4.55. □

OBSERVACIÓN 4.61 (Propiedad universal del anillo de polinomios). Para cada n -upla de 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^n en el monoide multiplicativo de B , tal que $\gamma(X_i) = b_i$ para cada índice i . En consecuencia, por la propiedad universal del anillo de monoide, si además tenemos fijado un morfismo de anillos $f: A \rightarrow B$, 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 $f_\gamma: A[X_1, \dots, X_n] \rightarrow B$, 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_γ está dado por

$$f_\gamma\left(\sum a_{n_1, \dots, n_r} X_1^{n_1} \dots X_r^{n_r}\right) = \sum f(a_{n_1, \dots, n_r}) b_1^{n_1} \dots b_r^{n_r}.$$

Terminamos esta subsección con el cálculo del centro de un anillo de grupos $A[G]$.

PROPOSICIÓN 4.62. Para cada anillo de grupos $A[G]$,

$$Z(A[G]) = \left\{ \sum_h a_h h : a_h \in ZA \text{ para todo } h \in G \text{ y } a_{ghg^{-1}} = a_h \text{ para todo } h, g \in G \right\}.$$

DEMOSTRACIÓN. Por definición $Z_G(A[G])$ es el conjunto de los elementos de $A[G]$ que conmutan con todos los elementos de G . Es evidente que $\sum_h a_h h \in Z_G(A[G])$ si y sólo si

$$\sum_h a_h ghg^{-1} = \sum_h a_h h \quad \text{para todo } g \in G.$$

Así,

$$Z_G(A[G]) = \left\{ \sum_h a_h h : a_{ghg^{-1}} = a_h \text{ para todo } h, g \in G \right\}.$$

En consecuencia, como $Z(A[G]) = Z_G(A[G]) \cap Z_A(A[G])$,

$$Z(A[G]) = \left\{ \sum_h a_h h : a_h \in ZA \text{ para todo } h \in G \text{ y } a_{ghg^{-1}} = a_h \text{ para todo } h, g \in G \right\}.$$

como queremos. \square

10. Los cuaterniones

En esta subsección F es un cuerpo arbitrario de característica distinta de 2. Presentaremos aquí los anillos de cuaterniones. En particular definiremos los cuaterniones de Hamilton que fueron descubiertos por él en 1843.

Fijemos elementos $a, b \in F^\times$ que pueden coincidir o no y consideremos el F -espacio vectorial A de dimensión 4 con base $\{1, i, j, k\}$. Supongamos que A tiene un producto F -bilineal que lo convierte en un anillo asociativo con neutro 1, tal que

$$(32) \quad i^2 := a, \quad j^2 := b, \quad ij := k \quad \text{y} \quad ji := -k.$$

Entonces necesariamente

$$(33) \quad k^2 = -ab, \quad ik = -ki = aj \quad \text{y} \quad jk = -kj = -bi.$$

PROPOSICIÓN 4.63. El F -espacio vectorial A provisto del producto definido sobre $\{1, i, j, k\}$ por la condición de que 1 sea su neutro más las condiciones (32) y (33), y extendido A por F -bilinealidad, es un anillo asociativo

DEMOSTRACIÓN. Sólo debemos verificar que el producto es asociativo y distributivo. Debido a que el producto es definido sobre $\{1, i, j, k\}$ y extendido a A por F -bilinealidad, sólo debemos comprobar que $(xy)z = x(yz)$ para todo $x, y, z \in \{1, i, j, k\}$. Dejamos al lector la realización de esta tarea directa y sencilla. \square

DEMOSTRACIÓN. Sólo debemos verificar que el producto es asociativo. Como este es F -bilineal es suficiente comprobar que $(xy)z = x(yz)$ para todo $x, y, z \in \{1, i, j, k\}$. Dejamos al lector la realización de esta tarea directa y sencilla. \square

Denotemos con $(\frac{a,b}{F})$ y llamamos *anillo de cuaterniones (generalizado)* al F -espacio vectorial A dotado de la estructura de anillo obtenido en la proposición anterior. Cuando $F = \mathbb{R}$ y $a = b = -1$ obtenemos el anillo de *cuaterniones de Hamilton* \mathbb{H} .

En lo que sigue de esta sección escribiremos A en lugar de $(\frac{a,b}{F})$ e identificaremos a F con $F \cdot 1$.

PROPOSICIÓN 4.64. *El anillo A no tiene ideales biláteros no triviales y su centro es F .*

DEMOSTRACIÓN. Para cada $x, y \in A$ denotamos con $[x, y]$ a $xy - yx$. Un cálculo directo muestra que si $x = c_1 \cdot 1 + c_i \cdot i + c_j \cdot j + c_k \cdot k$, entonces

$$[i, x] = 2ac_k \cdot j + 2c_j \cdot k, \quad [j, x] = -2bc_k \cdot i - 2c_i \cdot k \quad \text{y} \quad [k, x] = 2bc_j \cdot i - 2ac_i \cdot j.$$

En consecuencia el centro de A es F . Supongamos ahora que $x \neq 0$ y que $x \in I$, donde I es un ideal bilátero de A . Un cálculo directo muestra que

$$-4bc_j \cdot i = [j, [i, x]] \in I, \quad 4abc_k \cdot j = [k, [j, x]] \in I \quad \text{y} \quad -4ac_i \cdot k = [i, [k, x]] \in I.$$

Por lo tanto si $c_i \neq 0$, $c_j \neq 0$ o $c_k \neq 0$, entonces I contiene a un elemento inversible. Por otro lado es evidente que si $c_i = c_j = c_k = 0$, entonces $c_1 = x \neq 0$ es también un elemento inversible de I . \square

Denotemos con A_+ a $F \cdot i \oplus F \cdot j \oplus F \cdot k$. Los elementos de A_+ se denominan *cuaterniones puros*. Cada elemento $x \in A$ se escribe de manera única como

$$x = x_1 + x_+ \quad \text{con } x_1 \in F \cdot 1 \text{ y } x_+ \in A_+.$$

Definimos el *conjugado* de este x por $\bar{x} := x_1 - x_+$. Es evidente que

$$\overline{x+y} = \bar{x} + \bar{y}, \quad \overline{\bar{x}} = x, \quad \bar{x} = x \Leftrightarrow x \in F \quad \text{y} \quad \bar{x} = -x \Leftrightarrow x \in A_+.$$

Además es fácil ver que

$$\overline{xy} = \bar{y}\bar{x} \quad \text{para todo } x, y \in A.$$

En efecto, por la F -bilinealidad es suficiente comprobar esto para $x, y \in \{1, i, j, k\}$, lo que dejamos como ejercicio para el lector.

Definimos la *norma* $N(x)$ de $x \in A$ por $N(x) := x\bar{x}$. Un cálculo directo muestra que si $x = x_1 + x_+$ con $x_1 = c_1 \cdot 1 \in F \cdot 1$ y $x_+ = c_i \cdot i + c_j \cdot j + c_k \cdot k \in A_+$ entonces

$$N(x) = (x_1 + x_+)(x_1 - x_+) = x_1^2 - x_+^2 = c_1^2 - ac_i^2 - bc_j^2 + abc_k^2 \in F.$$

Notemos que

$$N(xy) = xy\bar{xy} = xy\bar{y}\bar{x} = xN(y)\bar{x} = x\bar{x}N(y) = N(x)N(y) \quad \text{para todo } x, y \in A.$$

TEOREMA 4.65. *Son equivalentes:*

1. A es un anillo de división.
2. Si $x \in A \setminus \{0\}$, entonces $N(x) \neq 0$.
3. Si $c_1, c_i, c_j \in F$ satisfacen $c_1^2 = ac_i^2 + bc_j^2$, entonces $c_1 = c_i = c_j = 0$.

DEMOSTRACIÓN. 1) \Rightarrow 2) Porque

$$N(x)N(x^{-1}) = N(xx^{-1}) = N(1) = 1.$$

2) \Rightarrow 1) Porque si $N(x) \neq 0$, entonces

$$x \frac{1}{N(x)} \bar{x} = \frac{1}{N(x)} x \bar{x} = \frac{1}{N(x)} N(x) = 1.$$

2) \Rightarrow 3) Porque si $c_1^2 = ac_i^2 + bc_j^2$, entonces

$$N(c_1 \cdot 1 + c_i \cdot i + c_j \cdot j) = c_1^2 - ac_i^2 - bc_j^2 = 0.$$

3) \Rightarrow 2) Supongamos que $x = c_1 \cdot 1 + c_i \cdot i + c_j \cdot j + c_k \cdot k$ y que $N(x) = 0$. Entonces

$$(34) \quad 0 = c_1^2 - ac_i^2 - bc_j^2 + abc_k^2,$$

lo que implica que

$$c_1^2 - bc_k^2 = a(c_i^2 - bc_k^2).$$

Por lo tanto

$$a(c_i^2 - bc_k^2)^2 = (c_1^2 - bc_k^2)(c_i^2 - bc_k^2) = (c_1c_i + c_jc_kb)^2 - b(c_1c_k + c_ic_j)^2.$$

En consecuencia, por hipótesis,

$$c_i^2 - bc_k^2 = 0,$$

lo que, nuevamente por hipótesis, implica que $c_i = c_k = 0$. Pero entonces, debido a la igualdad (34) y, por tercera vez a la hipótesis, $c_1 = c_j = 0$. \square

COROLARIO 4.66. *El anillo \mathbb{H} es de división y no conmutativo.*

OBSERVACIÓN 4.67. *El conjunto de los cuaterniones de Hamilton que tienen coordenadas racionales forman un subanillo de división de \mathbb{H} .*

OBSERVACIÓN 4.68. *Cada elemento de \mathbb{H} se puede escribir de manera única como $z_1 + z_2j$ con $z_1, z_2 \in \mathbb{C}$, donde identificamos \mathbb{C} con el subanillo de \mathbb{H} generado por i . La aplicación*

$$\theta: \mathbb{H} \rightarrow M_2(\mathbb{C}),$$

dada por

$$\theta(z_1 + z_2j) := \begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix},$$

es un monomorfismo de anillos. Por lo tanto \mathbb{H} es isomorfo a un subanillo de $M_2(\mathbb{C})$. Notemos que $\det(\theta(z)) = N(z)$ para todo $z \in \mathbb{H}$.

OBSERVACIÓN 4.69. *Debido a la Observación 1.108 El subgrupo de \mathbb{H}^\times , generado por $e^{i\pi/n}$ y j , es isomorfo al grupo cuaterniónico generalizado H_n . En particular H_2 es isomorfo al subgrupo $\{\pm 1, \pm i, \pm j, \pm k\}$. Notemos también que $S^3 := \{z \in \mathbb{H} : N(z) = 1\}$ es un subgrupo de \mathbb{H}^\times que contiene a las copias de los H_n mencionadas arriba.*

OBSERVACIÓN 4.70. *Dado que para cada cuaternión puro $x := c_1 \cdot i + c_2 \cdot j + c_3 \cdot k \in \mathbb{H}$ de norma 1,*

$$x^2 = -N(x) = -1,$$

en \mathbb{H} hay infinitas copias de \mathbb{C} .

11. El cuerpo de cocientes de un dominio conmutativo

En esta sección construimos 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

$$\frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs} \quad \text{y} \quad \frac{p}{q} \frac{r}{s} = \frac{pr}{qs},$$

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 4.71. *El cuerpo de cocientes de A es, efectivamente, un cuerpo. Además, la aplicación*

$$\begin{array}{ccc} A & \xrightarrow{\iota} & \mathbb{Q}_A \\ a & \longmapsto & \frac{a}{1} \end{array}$$

es un morfismo inyectivo de anillos, que tiene la siguiente propiedad universal: dados un cuerpo k y un morfismo inyectivo $f: A \rightarrow k$, existe un único morfismo de cuerpos $\tilde{f}: \mathbb{Q}_A \rightarrow k$ tal que el triángulo

$$\begin{array}{ccc} A & \xrightarrow{f} & k \\ \downarrow \iota & \nearrow \tilde{f} & \\ \mathbb{Q}_A & & \end{array}$$

conmuta.

DEMOSTRACIÓN. Las igualdades

$$\begin{aligned} \left(\frac{p}{q} + \frac{r}{s}\right) + \frac{t}{u} &= \frac{ps + qr}{qs} + \frac{t}{u} = \frac{psu + qru + qst}{qsu} = \frac{p}{q} + \frac{ru + st}{su} = \frac{p}{q} + \left(\frac{r}{s} + \frac{t}{u}\right), \\ \frac{p}{q} + \frac{r}{s} &= \frac{ps + qr}{qs} = \frac{rq + sp}{sq} = \frac{r}{s} + \frac{p}{q}, \\ \frac{p}{q} + \frac{0}{1} &= \frac{p1 + q0}{q1} = \frac{p}{q}, \\ \frac{p}{q} + \frac{-p}{q} &= \frac{pq - qp}{q^2} = \frac{0}{q^2} = \frac{0}{1}, \\ \left(\frac{p}{q} \frac{r}{s}\right) \frac{t}{u} &= \frac{pr}{qs} \frac{t}{u} = \frac{prt}{qsu} = \frac{p}{q} \frac{rt}{su} = \frac{p}{q} \left(\frac{r}{s} \frac{t}{u}\right), \\ \frac{p}{q} \frac{r}{s} &= \frac{pr}{qs} = \frac{rp}{sq} = \frac{r}{s} \frac{p}{q}, \\ \frac{p}{q} \frac{1}{1} &= \frac{p1}{q1} = \frac{p}{q} \end{aligned}$$

y

$$\frac{p}{q} \left(\frac{r}{s} + \frac{t}{u} \right) = \frac{p ru + st}{q su} = \frac{pru + pst}{qsu} = \frac{prqu + qspt}{qsqu} = \frac{pr}{qs} + \frac{pt}{qu} = \frac{pr}{qs} + \frac{p}{q} \frac{t}{u},$$

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 $\iota: A \rightarrow \mathbb{Q}_A$ 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 $f: A \rightarrow k$ es un morfismo inyectivo de A en un cuerpo. Si $\tilde{f}: \mathbb{Q}_A \rightarrow k$ 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. \square

NOTA 4.72. Es usual identificar $a \in A$ con $\iota(a) = \frac{a}{1}$.

Capítulo 5

Dominios de factorización única

El Teorema fundamental de la aritmética dice que todo número entero n se escribe de manera única como un producto

$$n = up_1^{l_1} \cdots p_m^{l_m},$$

donde los $p_1 < \cdots < p_m$ son números primos positivos, llamados los factores primos o irreducibles de n , el exponente $l_i > 0$ es la multiplicidad de p_i en la factorización y $u = \pm 1$. En este capítulo estudiaremos una clase de anillos, llamados dominios de factorización única o factoriales, en los cuales vale una generalización directa de esta propiedad. Nuestro objetivo principal será probar que los anillos de polinomios sobre dominios factoriales son factoriales, el cual es un célebre teorema de Gauss. Las definiciones y propiedades básicas tienen sentido para monoides conmutativos y cancelativos, y las establecemos en ese contexto.

1. Monoides factoriales

Fijemos un monoide conmutativo S . Recordemos que un elemento s de S es una unidad si es inversible, y que el conjunto S^\times de las unidades de S es un grupo. Dados elementos s y t de S , decimos que s *divide* a t o que es un *divisor* de t y que t *es divisible por* s , y escribimos $s \mid t$, si existe $c \in S$ tal que $sc = t$. La relación de divisibilidad es reflexiva y transitiva y, por lo tanto, define una estructura de preorden parcial en S . Decimos también que dos elementos s y t de S son *asociados*, y escribimos $s \sim t$, si

$$s \mid t \quad \text{y} \quad t \mid s.$$

Es evidente que \sim es un relación de equivalencia y que el cociente S/\sim es un conjunto parcialmente ordenado vía el orden inducido por la relación de divisibilidad en S .

Un *máximo divisor común* de dos elementos s y t de S es cualquier elemento $c \in S$ que satisfice:

- $c \mid s$ y $c \mid t$,
- si $d \mid s$ y $d \mid t$, entonces $d \mid c$,

y un *mínimo múltiplo común* de s y t es cualquier elemento $e \in S$ que satisfice:

- $s \mid e$ y $t \mid e$,
- si $s \mid f$ y $t \mid f$, entonces $e \mid f$.

En principio no hay ningún motivo por el cual dos elementos s y t de S deban tener un máximo divisor común, pero si tienen uno c , entonces por la misma definición es evidente que un elemento $d \in S$ es un máximo divisor común de s y t si y sólo si es asociado a c . Lo mismo es cierto para los mínimos múltiplos comunes de s y t .

Un elemento $p \in S \setminus S^\times$ es *irreducible* si todos sus divisores son unidades o asociados, y es *primo* si cada vez que divide a un producto, divide a uno de los factores. Dicho de otro modo, p es irreducible si y sólo si

$$s \mid p \Rightarrow s \in S^\times \text{ o } s \sim t,$$

y es primo si y sólo si

$$p \mid st \Rightarrow p \mid s \text{ o } p \mid t.$$

OBSERVACIÓN 5.1. *Supongamos que S es cancelativo. En este caso si $s, t \in S$ y $s \mid t$, entonces el elemento $c \in S$ tal que $sc = t$ es único, y es llamado el cociente de t por s . Afirmamos que s y t son asociados si y sólo existe una unidad u de S tal que $t = su$. En efecto, es claro que si u existe, entonces $s \mid t$ y $t \mid s$. Recíprocamente, si s y t son asociados, entonces hay elementos $u, v \in S$ tales que $t = su$ y $s = tv$. Por consiguiente*

$$t = su = tv,$$

de lo cual se sigue que $uv = 1$, debido a que S es cancelativo.

PROPOSICIÓN 5.2. *Si S es cancelativo, entonces todo elemento primo $p \in S$, es irreducible.*

DEMOSTRACIÓN. Supongamos que $s \mid p$ y escribamos $p = st$. Como p es primo, $p \mid s$ o $p \mid t$. Es claro que el primer caso $p \sim s$. Supongamos entonces que $p \mid t$ y escribamos $t = vp$. Como S es cancelativo, la igualdad

$$p = st = svp,$$

implica que $sv = 1$ y así, s es una unidad de S . □

Un monoide conmutativo y cancelativo S es *semifactorial* si para todo $s \in S$ existen una unidad u e irreducibles p_1, \dots, p_m tales que

$$(35) \quad s = up_1 \cdots p_m$$

Una escritura de s como (35) es llamada una *factorización de s* como producto de irreducibles. Notemos que $m = 0$ si y sólo s es inversible, y que si $m > 0$, entonces se puede tomar $u = 1$. Decimos que S es *factorial* si es semifactorial y la escritura de cada $s \in S$ como producto de irreducibles es única en el siguiente sentido: Si

$$s = up_1 \cdots p_m = vq_1 \cdots q_n,$$

con $u, v \in S^\times$ y $p_1, \dots, p_m, q_1, \dots, q_n$ irreducibles, entonces $m = n$ y existe $\sigma \in S_m$ tal que $p_i \sim q_{\sigma_i}$ para todo i .

Por la Proposición 5.2 sabemos que en un monoide cancelativo los elementos primos son irreducibles. El siguiente teorema muestra, en particular, que en los monoides factoriales vale la recíproca.

TEOREMA 5.3. Para cada monoide conmutativo y cancelativo S son equivalentes:

1. S es factorial.
2. S es semifactorial y todo elemento irreducible $p \in S$ es primo.
3. Cada $s \in S$ se factoriza como un producto

$$s = up_1 \cdots p_n,$$

donde u es una unidad y p_1, \dots, p_n son primos.

DEMOSTRACIÓN. 1) \Rightarrow 2) Es claro que S es semifactorial. Veamos que cada elemento irreducible $p \in S$ es primo. Supongamos que $p \mid st$ y $st = px$. Entonces combinando p con una factorización de x se obtiene una de st , y combinando una de s con una de t , se obtiene otra. Como la factorización de st es única salvo asociados, esto implica que $p \mid s$ o $p \mid t$

2) \Rightarrow 3) Es trivial.

3) \Rightarrow 1) Consideremos una factorización

$$s = vq_1 \cdots q_m$$

de s en producto de una unidad v e irreducibles q_1, \dots, q_m . Si $n = 0$, entonces s es inversible. Por lo tanto $m = 0$ y $v = u$. Supongamos que la factorización es única salvo asociados siempre que $n \leq n_0$ y que $n = n_0 + 1$. Como p_n es primo, debe dividir a v o a unos de los q_i 's. Pero es imposible que p_n divida a v , porque sería una unidad. Así, $p \mid q_i$. Podemos asumir sin pérdida de generalidad que $i = m$. Puesto que q_m es irreducible y p_n no es una unidad, $q_m \sim p_n$. En consecuencia existe $w \in S^\times$ tal que

$$wq_1 \cdots q_{m-1} = p_1 \cdots p_{n-1}.$$

Ahora la demostración se termina inmediatamente usando la hipótesis inductiva. \square

Una sucesión

$$s_1, s_2, s_3, \dots$$

de elementos de S es *estacionaria* si existe $n_0 \in \mathbb{N}$ tal que $s_i \sim s_{n_0}$ para todo $i \geq n_0$. Una *cadena de divisores sucesivos* de S es una sucesión

$$s_1, s_2, s_3, \dots$$

de elementos de S tal que $s_{i+1} \mid s_i$ para todo i . Es evidente que si S es factorial, entonces toda cadena de divisores sucesivos de S es estacionaria. Nuestro próximo objetivo es verificar que esta condición implica que S es semifactorial. Esto es, que es intermedia entre la de ser semifactorial y factorial. Para ello comenzamos estableciendo un lema.

LEMA 5.4. Si toda cadena de divisores sucesivos de S es estacionaria, entonces cada $s \in S$ que no es una unidad es divisible por un elemento irreducible de S .

DEMOSTRACIÓN. Supongamos que la tesis es falsa para un s . Entonces se obtiene una sucesión no estacionaria

$$s_1, s_2, s_3, \dots$$

de divisores sucesivos de S , tomando $s_1 = s$ y s_{i+1} como un divisor de s_i no inversible ni asociado a s_i . \square

PROPOSICIÓN 5.5. Si toda cadena de divisores sucesivos de S es estacionaria, entonces S es semifactorial.

DEMOSTRACIÓN. Supongamos que $s_0 \in S \setminus S^\times$ no es producto de irreducibles. Afirmamos que existen $s_1, \dots, s_n, \dots, p_1, \dots, p_n, \dots \in S$, con los p_i 's irreducibles, tales que $s_i = p_i s_{i+1}$ para todo $i \geq 0$. En efecto supongamos hemos obtenido $s_1, \dots, s_n, p_1, \dots, p_n \in S$ como queremos. Entonces $s_0 = p_1 p_2 \cdots p_n s_n$, por lo que, debido a la hipótesis, $s_n \notin S^\times$. En consecuencia, por el Lema 5.4, existen $p_{n+1}, s_{n+1} \in S$ con p_{n+1} irreducible, tales que $s_n = p_{n+1} s_{n+1}$. Se comprueba fácilmente ahora que la cadena de divisores sucesivos

$$s_1, s_2, s_3, s_4 \dots$$

no es estacionaria. \square

Una familia de representantes de las clases de equivalencia de los irreducibles de S (módulo asociados), es cualquier subconjunto \mathcal{P} de S , tal que para cada irreducible q de S hay un único $p \in \mathcal{P}$ asociado a q . Por ejemplo, los primos positivos son una familia de representantes de las clases de equivalencia de los irreducibles de $\mathbb{Z} \setminus \{0\}$ y los polinomios mónicos de grado 1 son una familia de representantes de las clases de equivalencia de los irreducibles de $\mathbb{C}[X] \setminus \{0\}$. Tales familias existen siempre, aunque es raro que se pueda elegir una en forma canónica, como en los ejemplos anteriores. De todo modos, en el resto de la sección consideramos fijada una, que además supondremos totalmente ordenada. Es evidente que S es factorial si cada elemento $s \in S$ se escribe de manera única como un producto

$$(36) \quad s = u p_1^{m_1} \cdots p_m^{m_m},$$

con $u \in S^\times$, $p_1 < \cdots < p_m$ en \mathcal{P} y $m_1, \dots, m_m \in \mathbb{N}$. Los elementos p_1, \dots, p_m son los factores irreducibles de s , y para cada i entre 1 y m , el número m_i es la multiplicidad o el exponente de p_i en s , o en la factorización de s . Decimos que $p \in \mathcal{P}$ tiene multiplicidad 0 en s si no es un factor irreducible de s . Adoptada esta convención, podemos reescribir (36) en la forma

$$s = u(s) \prod_{p \in \mathcal{P}} p^{m_p(s)},$$

donde $m_p(s)$ es la multiplicidad de p en s .

En un monoide factorial S , cada par de elementos tiene máximo divisor común y mínimo múltiplo común. En efecto, para cada $s, t \in S$, los elementos

$$(s : t) := \prod_{p \in \mathcal{P}} p^{\min(m_p(s), m_p(t))} \quad \text{and} \quad [s : t] := \prod_{p \in \mathcal{P}} p^{\max(m_p(s), m_p(t))},$$

donde $\min(m_p(s), m_p(t))$ denota al mínimo de $m_p(s)$ y $m_p(t)$ y $\max(m_p(s), m_p(t))$ al máximo, son un máximo divisor común y mínimo múltiplo común de s y t , respectivamente. Este resultado es una generalización directa del método para encontrar el máximo divisor común y el mínimo múltiplo común de dos números factorizados en primos, enseñado en la escuela primaria. Notemos que

$$st \sim (s : t)[s : t].$$

2. Dominios de factorización única

Consideremos el monoide multiplicativo de un anillo conmutativo A . Es evidente que $a \mid 0$ para todo $a \in A$ y que $0 \mid a$ implica que $a = 0$. En particular 0 irreducible si y sólo si A es un cuerpo. Además vale lo siguiente:

1. si $a \mid b$ y $a \mid c$ entonces $a \mid rb + sc$ para todo $r, s \in A$,

2. si $a = bq + c$ entonces los divisores comunes de a y b coinciden con los de b y c ,
3. Si $a \sim 0$, entonces $a = 0$,
4. Un elemento $p \in A$ es primo si y sólo si el ideal $\langle p \rangle$ lo es (ver la Observación 4.43),
5. 0 es primo si y sólo si A es un dominio (ver la Proposición 4.44).

Es evidente que A es un dominio si y sólo si $A \setminus \{0\}$ es un submonioide del monoide multiplicativo de A y que en este caso un elemento p no nulo de A es irreducible o primo en $A \setminus \{0\}$ si y sólo si lo es en A .

Un anillo A es un *dominio semifactorial* si es un dominio y $A \setminus \{0\}$ es un monoide semifactorial, y es un *dominio factorial* o de *factorización única*, si el monoide multiplicativo $A \setminus \{0\}$ es factorial. Ya sabemos que si este es el caso, entonces cada par de elementos no nulos $a, b \in A$ tiene máximo divisor común y mínimo múltiplo común. En realidad, estos operadores están definidos para todo a y b . Por ejemplo, cuando $b=0$ el primero da a y el segundo 0.

PROPOSICIÓN 5.6. *Para cada elemento $p \neq 0$ de un dominio principal A son equivalentes:*

1. $\langle p \rangle$ es maximal,
2. p es primo,
3. p es irreducible.

DEMOSTRACIÓN. 1) \Rightarrow 2). Por el Corelario 4.45.

2) \Rightarrow 3). Por la Proposición 5.2.

3) \Rightarrow 1). Si $\langle p \rangle$ no fuera maximal, entonces existiría $q \in A$ tal que $\langle p \rangle \subsetneq \langle q \rangle \subsetneq A$, lo que claramente implica que $q \mid p$ pero q no es unidad ni asociado a p . \square

TEOREMA 5.7. *Todo dominio principal es factorial.*

DEMOSTRACIÓN. Por las la Proposiciones 5.5 y 5.6 y el Teorema 5.3 será suficiente probar que toda cadena

$$s_1, s_2, s_3, \dots,$$

de divisores sucesivos de $A \setminus \{0\}$ es estacionaria. Veamos que esto es así. Dado que

$$\langle s_1 \rangle \subseteq \langle s_2 \rangle \subseteq \langle s_3 \rangle \subseteq \dots$$

la unión $\bigcup_{i \in \mathbb{N}} \langle s_i \rangle$ es un ideal. Como A es un dominio principal existe $s \in A \setminus \{0\}$ tal que

$$\bigcup_{i \in \mathbb{N}} \langle s_i \rangle = \langle s \rangle.$$

Por lo tanto si $s \in \langle s_n \rangle$,

$$\langle s \rangle = \langle s_n \rangle = \langle s_{n+1} \rangle = \langle s_{n+2} \rangle = \dots$$

y, en consecuencia, $s_n \mid s_{n+i}$ para todo $i \in \mathbb{N}$. \square

Capítulo 6

Teoría elemental de módulos

1. Módulos

Una *acción a izquierda* de un anillo A sobre un grupo abeliano M es una aplicación $(a, m) \mapsto a \cdot m$, de $A \times M$ en M , que satisface:

1. $1 \cdot m = m$ para todo $m \in M$,
2. $a \cdot (m + n) = a \cdot m + a \cdot n$ para todo $a \in A$ y $m, n \in M$,
3. $(a + b) \cdot m = a \cdot m + b \cdot m$ para todo $a, b \in A$ y $m \in M$,
4. $a \cdot (b \cdot m) = (ab) \cdot m$ para todo $a, b \in A$ y $m \in M$.

La primera igualdad dice que la acción es unitaria, las dos siguientes que es distributiva y la última que es asociativa. De ahora en más escribiremos $ab \cdot m$ en lugar de $(ab) \cdot m$.

Un *A-módulo a izquierda* o *módulo a izquierda sobre A* es un grupo abeliano M provisto de una acción a izquierda de A sobre M .

La terminología “acción a izquierda” y “A-módulo a izquierda” utilizada, sugiere que hay versiones a derecha de estos conceptos, y sólo tiene sentido si estas verdaderamente existen. Como es de esperarse, este es el caso.

Dados un anillo A y un grupo abeliano M , una *acción a derecha* de A sobre M es una aplicación $(m, a) \mapsto m \cdot a$, de $M \times A$ en M , que satisface:

1. $m \cdot 1 = m$ para todo $m \in M$,
2. $(m + n) \cdot a = m \cdot a + n \cdot a$ para todo $a \in A$ y $m, n \in M$,
3. $m \cdot (a + b) = m \cdot a + m \cdot b$ para todo $a, b \in A$ y $m \in M$,
4. $(m \cdot a) \cdot b = m \cdot (ab)$ para todo $a, b \in A$ y $m \in M$.

Un *A-módulo a derecha* o *módulo a derecha sobre A* es un grupo abeliano M provisto de una acción a derecha de A sobre M . Es evidente que una acción a derecha de A sobre un grupo abeliano es simplemente una acción a izquierda de A^{op} sobre el mismo grupo, y que un A-módulo a derecha no es otra cosa que un A^{op} -módulo a izquierda, de modo que las dos teorías son equivalentes. Debido a esto sólo consideraremos módulos a izquierda, dejando al lector

la tarea de trasladar los resultados al contexto de módulos a derecha. Consecuentemente, a partir de ahora cuando hablemos de un A -módulo o módulo sobre A nos estaremos refiriendo a un módulo a izquierda, y llamaremos *acciones* a las acciones a izquierda.

EJERCICIO 6.1. *Pruebe que*

$$a \cdot 0 = 0 \cdot m = 0 \quad \text{y} \quad (-a) \cdot m = a \cdot (-m) = -a \cdot m,$$

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

$$\begin{array}{ccc} M & \xrightarrow{\rho(a)} & M \\ m & \longmapsto & a \cdot m \end{array}$$

es un endomorfismo de M para cada $a \in A$, y la aplicación

$$\begin{array}{ccc} A & \xrightarrow{\rho} & \text{End}(M) \\ a & \longmapsto & \rho(a) \end{array}$$

es un morfismo de anillos. Recíprocamente, si $\rho: A \rightarrow \text{End}(M)$ 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 $\text{End}(M)$.

EJEMPLO 6.2. *El A -módulo nulo es el grupo 0 provisto de la única acción a izquierda de A sobre él.*

EJEMPLO 6.3. *Cada anillo A es un A -módulo bajo la acción regular a izquierda, dada por la multiplicación. Cuando consideremos a A como módulo vía esta acción lo denotaremos ${}_A A$.*

EJEMPLO 6.4. *Un módulo sobre un cuerpo k es un k -espacio vectorial.*

EJEMPLO 6.5. *Por el Ejemplo 4.28, para cada grupo abeliano M , hay un único morfismo de anillos $\iota: \mathbb{Z} \rightarrow \text{End}(M)$. 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 6.6. *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*

$$\begin{array}{ccc} M & \xrightarrow{f} & M \\ m & \longmapsto & X \cdot m \end{array}$$

es un endomorfismo de k -espacios vectoriales porque

$$X \cdot (m + n) = X \cdot m + X \cdot n \quad \text{y} \quad X \cdot (\lambda \cdot m) = (X\lambda) \cdot m = (\lambda X) \cdot m = \lambda \cdot (X \cdot m),$$

para todo $m, n \in M$ y $\lambda \in k$. Recíprocamente, dados un k -espacio vectorial M y una aplicación k -lineal $f: M \rightarrow M$, 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 $\text{End}(M)$, y utilizar la propiedad universal del anillo de polinomios (Observación 4.61).

EJEMPLO 6.7. 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 $f: M \rightarrow M$ que satisface $f^2 = -\text{id}$.

EJEMPLO 6.8. 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

$$\begin{array}{ccc} M & \xrightarrow{\rho(s)} & M \\ m & \longmapsto & s \cdot m \end{array}$$

es un morfismo de k -espacios vectoriales,

- La función

$$\begin{array}{ccc} S & \xrightarrow{\rho} & \text{End}_k(M) \\ s & \longmapsto & \rho(s) \end{array}$$

es un morfismo de monoides.

Recíprocamente, dados un k -módulo M y un morfismo de monoides $\rho: S \rightarrow \text{End}_k(M)$, 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 6.9. Una representación de un grupo G sobre un k -espacio vectorial M es un morfismo de grupos $\rho: G \rightarrow \text{Aut}_k(M)$. 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 $\rho: A \rightarrow \text{End}(M)$ 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 $\rho: \mathbb{Z} \rightarrow \text{End}(\mathbb{Z}_6 \times \mathbb{Z}_9)$ asociado es $18\mathbb{Z}$. La acción inducida de \mathbb{Z}_{18} sobre $\mathbb{Z}_6 \times \mathbb{Z}_9$ es fiel.

2. Submódulos

Un subconjunto N de un A -módulo M es un *submódulo* de M si es cerrado para la suma y $a \cdot m \in N$ para todo $a \in A$ y $m \in N$. Por ejemplo 0 y M son submódulos de M . Estos son los llamados *submódulos triviales*. Un submódulo de M es *propio* si es distinto de M . Como el conjunto de los submódulos de M es cerrado bajo intersecciones, para cada $S \subseteq M$ existe un

mínimo submódulo AS de M que contiene a S , llamado *el submódulo de M generado por S* , el cual es precisamente la intersección de todos los submódulos de M que contienen a S . Una notación alternativa bastante usual para AS es $\langle S \rangle$. Es evidente que AS es el conjunto de las sumas finitas de elementos de la forma $a \cdot m$, con $a \in A$ y $m \in S$. Dado $m \in M$ escribiremos Am en lugar de $A\{m\}$. Además, cuando $S = \{s_1, \dots, s_n\}$ 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 6.10. *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 subfamilia 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 $1 \leq j \leq n$ existe un subconjunto finito I_j de I tal que $x_j \in \sum_{i \in I_j} M_i$ y así $M = \sum_{i \in I'} M_i$, donde $I' = I_1 \cup \dots \cup I_n$.

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 6.11. *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 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 minimal, 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 ${}_A A$.

Para terminar, consideremos algunos de los ejemplos mencionados en la sección anterior, y veamos cuales son los submódulos. Los de un k -espacio vectorial son los subespacios vectoriales; los de un \mathbb{Z} -módulo, los subgrupos; los de un $k[X]$ -módulo, los subespacios vectoriales estables bajo la acción de X ; los de un $k[S]$ -módulo, los subespacios vectoriales cerrados bajo la acción de S ; y los de ${}_A A$, los ideales a izquierda.

3. Morfismos de módulos

Un *morfismo* de A -módulos $f: M \rightarrow N$ es una terna (M, f, N) , donde f es un morfismo del grupo abeliano subyacente de M en el de N , que satisface

$$f(a \cdot m) = a \cdot f(m) \quad \text{para todo } a \in A \text{ y } m \in M.$$

El A -módulo M es el dominio de $f: M \rightarrow N$ y N es el codominio.

Por ejemplo, la identidad $\text{id}_M: M \rightarrow M$ y, más generalmente, la inclusión canónica $i: N \rightarrow M$ de un submódulo N de M en M , es un morfismo. También lo es la composición $g \circ f: M \rightarrow L$, definida en forma evidente, de dos morfismos $f: M \rightarrow N$ y $g: N \rightarrow L$. Los morfismos de A -módulos son llamados también *aplicaciones A -lineales*.

Muchas de las propiedades básicas de los morfismos de A -módulos son análogas a las establecidas para los de monoides, grupos y anillos. Las definiciones de endomorfismo, isomorfismo, automorfismo, monomorfismo, epimorfismo, sección y retracción son las mismas. Sigue siendo cierto que un morfismo es un isomorfismo si y sólo si es biyectivo. Mantenemos la notación $M \simeq M'$ para señalar que los A -módulos M y M' son isomorfos. Es fácil ver que los monomorfismos, epimorfismos, secciones y retracciones son cerrados bajo composición, que toda retracción es sobreyectiva, toda sección inyectiva, todo morfismo inyectivo un monomorfismo, y todo morfismo sobreyectivo un epimorfismo. También que un morfismo $f: M \rightarrow M'$ 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 $f: M \rightarrow M'$ es inyectivo. En efecto, si $f(m) = f(m')$, entonces $f \circ g = f \circ g'$, donde $g, g': {}_A A \rightarrow M$ son los morfismos definidos por

$$g(a) = a \cdot m \quad \text{y} \quad g'(a) = a \cdot m' \quad \text{para todo } a \in A.$$

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 10 del Capítulo 1 muestran que cuando $A = \mathbb{Z}$ hay monomorfismos que no son secciones y epimorfismos que no son retracciones.

Tal como para monoides, grupos y anillos, dados morfismos $f: M \rightarrow N$ y $g: N \rightarrow L$,

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 $\text{Hom}_A(M, M')$, $\text{Iso}_A(M, M')$, $\text{End}_A(M)$ y $\text{Aut}_A(M)$ denotan respectivamente a los conjuntos de morfismos de A -módulos de M en M' , isomorfismos de M en M' ,

endomorfismos de M y automorfismos de M . Es inmediato que $\text{End}_A(M)$ es un monoide (cuyo elemento neutro es la función identidad) vía la composición y que $\text{Aut}_A(M)$ es su grupo de unidades.

Como veremos enseguida, los morfismos de A -módulos tienen una estructura mucho más rica que los de monoides, grupos y anillos. En particular, $\text{End}_A(M)$ tiene una estructura natural de anillo.

3.1. Estructuras en el conjunto de los morfismos de un módulo en otro

Para cada par de A -módulos a izquierda M y N , el conjunto $\text{Hom}_A(M, N)$ es un grupo abeliano vía $(f + g)(m) := f(m) + g(m)$. El neutro es el *morfismo nulo* $0_{MN}: M \rightarrow N$, que envía cada elemento de M en 0 , y el opuesto de un morfismo $f: M \rightarrow N$, es la función $-f: M \rightarrow N$ que envía cada $m \in M$ en $-f(m)$. La composición es distributiva con respecto a la suma y en particular $\text{End}_A(M)$ es un anillo cuyo neutro es id_M . Notemos que de la distributividad de la composición con respecto a la suma se sigue también que las aplicaciones

$$v_*: \text{Hom}_A(M, N) \rightarrow \text{Hom}_A(M, N') \quad \text{y} \quad u^*: \text{Hom}_A(M, N) \rightarrow \text{Hom}_A(M', N),$$

definidas para cada par de morfismos de A -módulos, $v: N \rightarrow N'$ y $u: M' \rightarrow M$, por

$$v_*(f) := v \circ f \quad \text{y} \quad u^*(f) := f \circ u$$

respectivamente, son morfismos de grupos abelianos.

Las correspondencias $v \mapsto v_*$ y $u \mapsto u^*$ tienen las siguientes propiedades:

1. $\text{id}_* = \text{id}$.
2. $(v' \circ v)_* = v'_* \circ v_*$ para cada par de morfismos $v: N \rightarrow N'$ y $v': N' \rightarrow N''$.
3. $(v' + v)_* = v'_* + v_*$ para cada par de morfismos $v, v': N \rightarrow N'$.
4. $\text{id}^* = \text{id}$.
5. $(u \circ u')^* = u'^* \circ u^*$ para cada par de morfismos $u: M' \rightarrow M$ y $u': M'' \rightarrow M'$.
6. $(u' + u)^* = u'^* + u^*$, para cada par de morfismos $u, u': M' \rightarrow M$.

OBSERVACIÓN 6.12. Para cada A -módulo M , la función

$$(37) \quad \begin{array}{ccc} M & \longrightarrow & \text{Hom}_A(A, M), \\ m & \longmapsto & f_m \end{array}$$

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 a cada morfismo $f: A \rightarrow M$ le asigna su valor en 1 . Cuando $M = A$ tiene sentido preguntarse si (37) 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 $\text{End}_A(A)$.

4. Núcleo e imagen

El *núcleo* $\ker f$ de un morfismo de A -módulos $f: M \rightarrow M'$ es la preimagen de 0 por f . Es evidente que $\ker f$ es un submódulo de M e $\text{Im } f$ un submódulo de M' . Más aún, no es difícil comprobar que la imagen de un submódulo N de M es un submódulo de M' , y que la preimagen de un submódulo N' de M' es un submódulo de M .

Es obvio que la inclusión canónica $\iota: \ker f \rightarrow M$ tiene las siguientes propiedades, la segunda de las cuales es llamada la *propiedad universal del núcleo*:

- $f \circ \iota = 0_{\ker f, M}$,
- Para cada morfismo de A -módulos $g: N \rightarrow M$ que satisface $f \circ g = 0_{NM'}$, existe un único morfismo de A -módulos $g': N \rightarrow \ker f$ tal que el diagrama

$$\begin{array}{ccccc}
 N & \xrightarrow{g} & M & \xrightarrow{f} & M' \\
 \downarrow g' & \nearrow \iota & & & \\
 \ker f & & & &
 \end{array}$$

conmuta.

PROPOSICIÓN 6.13. Si $f: M \rightarrow M'$ 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 1.76. □

COROLARIO 6.14. Un morfismo f de A -módulos es inyectivo si y sólo si $\ker f = 0$.

5. Cociente 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 $\pi: M \rightarrow M/N$ 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 satisface

$$a \cdot [m] = [a \cdot m].$$

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 $\pi: M \rightarrow M/N$ tiene la siguiente propiedad, llamada *propiedad universal del cociente*:

- Si $f: M \rightarrow M'$ es un morfismo de A -módulos cuyo núcleo incluye a N , entonces existe un único morfismo de A -módulos $\bar{f}: M/N \rightarrow M'$ tal que el triángulo

$$\begin{array}{ccc}
 M & \xrightarrow{f} & M' \\
 \downarrow \pi & \nearrow \bar{f} & \\
 M/N & &
 \end{array}$$

conmuta.

Para comprobarlo basta observar que, por la propiedad universal del cociente de grupos, dado un morfismo de grupos abelianos $f: M \rightarrow M'$ con $N \subseteq \ker f$, existe un único morfismo de grupos abelianos $\bar{f}: M/N \rightarrow M'$ 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 $\text{Im } \bar{f} = \text{Im } f$ (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 6.15 (Primer teorema de isomorfismo). *Toda función A -lineal $f: M \rightarrow M'$ induce un isomorfismo $\bar{f}: M/\ker f \rightarrow \text{Im } f$.*

DEMOSTRACIÓN. Es claro. \square

EJEMPLO 6.16. *Supongamos que $M = Am$ es cíclico. Entonces el morfismo*

$$\begin{array}{ccc} A & \longrightarrow & M \\ a & \longmapsto & a \cdot m \end{array},$$

es sobreyectivo y su núcleo es un ideal a izquierda I . Así, por el teorema anterior, $M \simeq A/I$.

TEOREMA 6.17 (Segundo teorema de isomorfismo). *Si $L \subseteq N$ son submódulos de un A -módulo M , entonces N/L es un submódulo de M/L y $M/N \simeq (M/L)/(N/L)$.*

DEMOSTRACIÓN. Copie la prueba del Teorema 1.84. \square

TEOREMA 6.18 (Tercer teorema de isomorfismo). *Si L y N son dos submódulos de un A -módulo M , entonces $L/L \cap N \simeq (N + L)/N$.*

DEMOSTRACIÓN. Copie la prueba del Teorema 1.85. \square

El conjunto $\text{Sub}_N(M)$, 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 $\text{Sub}(M)$ en lugar de $\text{Sub}_0(M)$. 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 6.19 (Teorema de la correspondencia). *Si $f: M \rightarrow M'$ es un morfismo sobreyectivo de A -módulos, entonces las funciones*

$$\begin{array}{ccc} \text{Sub}_{\ker f}(M) & \longrightarrow & \text{Sub}(M') \\ N & \longmapsto & f(N) \end{array} \quad y \quad \begin{array}{ccc} \text{Sub}(M') & \longrightarrow & \text{Sub}_{\ker f}(M) \\ N' & \longmapsto & f^{-1}(N') \end{array}$$

son isomorfismos de reticulados, inversos uno del otro. Además $L/N \simeq f(L)/f(N)$ para cada $L, N \in \text{Sub}_{\ker f}(M)$ con $N \subseteq L$.

DEMOSTRACIÓN. Es una consecuencia fácil del Teorema 1.90. Alternativamente, se lo puede probar copiando la demostración de una parte de ese resultado. \square

DEFINICIÓN 6.20. *Un A -módulo M es simple si $M \neq 0$ y sus únicos submódulos son los triviales.*

DEFINICIÓN 6.21. *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 6.22. *Un submódulo N de un A -módulo M es maximal si y sólo si M/N es simple.*

OBSERVACIÓN 6.23. *Un A -módulo no nulo M es simple si y sólo si $M = Am$ para todo $m \in M \setminus \{0\}$. En particular todo A -módulo simple es cíclico y, por lo tanto isomorfo a un cociente de A por un ideal a izquierda que, por el corolario anterior, es maximal.*

PROPOSICIÓN 6.24. *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 ítem 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

$$[m] = a_1 \cdot [m_1] + \dots + a_s \cdot [m_s] \quad \text{con } a_1, \dots, a_s \in A.$$

Como $m - a_1 \cdot m_1 - \dots - a_s \cdot m_s \in N$, existen $b_1, \dots, b_r \in A$ tales que

$$m - a_1 \cdot m_1 - \dots - a_s \cdot m_s = b_1 \cdot n_1 + \dots + b_r \cdot n_r,$$

lo cual termina la prueba. \square

PROPOSICIÓN 6.25. *Si N es un submódulo propio de un A -módulo M y M/N es finitamente generado, entonces M tiene un submódulo maximal que incluye a N . En particular, todo A -módulo finitamente generado tiene submódulos maximales.*

DEMOSTRACIÓN. Supongamos que las clases de $m_1, \dots, m_r \in M$ en M/N generan M/N y consideremos el conjunto \mathcal{P} de los submódulos propios de M que contienen a N . Notemos que \mathcal{P} no es vacío pues $N \in \mathcal{P}$. Por el lema de Zermelo podemos tomar una cadena maximal $(N_i)_{i \in I}$ de elementos de \mathcal{P} . Dado que evidentemente no hay ningún submódulo propio de M que contenga a todos los N_i , el teorema quedará probado si podemos ver que $\bigcup N_i$ es propio. Pero esto es claramente así, pues si m_1, \dots, m_r están en esta unión, entonces $m_1, \dots, m_r \in N_i$ para algún $i \in I$, lo que se contradice con que N_i es propio, pues $N + \langle m_1, \dots, m_r \rangle = M$. \square

EJERCICIO 6.26. *Pruebe que el \mathbb{Z} -módulo \mathbb{Q} no tiene submódulos maximales.*

Consideremos un morfismo de A -módulos $f: M \rightarrow M'$ 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 $\bar{f}: M/N \rightarrow M'/N'$ tal que el cuadrado

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ \downarrow \pi & & \downarrow \pi' \\ M/N & \xrightarrow{\bar{f}} & M'/N' \end{array},$$

donde π y π' son las proyecciones canónicas, conmuta. De las fórmulas para el núcleo y la imagen obtenidas al establecer la misma, se sigue de inmediato que

$$\text{Im } \bar{f} = \pi'(\text{Im } f) \quad \text{y} \quad \ker \bar{f} = f^{-1}(N')/N.$$

PROPOSICIÓN 6.27. *La correspondencia establecida arriba tiene las siguientes propiedades:*

1. *Para todo submódulo N de M , el morfismo $\bar{\text{id}}: M/N \rightarrow M/N$ es la identidad de M/N .*
2. *Consideremos morfismos de A -módulos $f: M \rightarrow M'$ y $g: M' \rightarrow M''$ 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 $\overline{g \circ f} = \bar{g} \circ \bar{f}$.*

DEMOSTRACIÓN. Por la unicidad de los morfismos $\overline{\text{id}}$ y $\overline{g \circ f}$, basta observar que el cuadrado

$$\begin{array}{ccc} M & \xrightarrow{\text{id}} & M \\ \downarrow \pi & & \downarrow \pi \\ M/N & \xrightarrow{\text{id}} & M/N \end{array}$$

y el rectángulo exterior del diagrama

$$\begin{array}{ccccc} M & \xrightarrow{f} & M' & \xrightarrow{g} & M'' \\ \downarrow \pi & & \downarrow \pi' & & \downarrow \pi'' \\ M/N & \xrightarrow{\overline{f}} & M'/N' & \xrightarrow{\overline{g}} & M''/N'' \end{array}$$

conmutan. □

6. Producto y coproducto directo

Ahora vamos a estudiar dos construcciones, el producto y el coproducto directo de módulos, las cuales son las maneras más simples de obtener nuevos módulos a partir de otros (aunque su importancia se debe más a las propiedades universales que tienen que a este hecho). Comenzamos considerando la suma directa interna, que nos da la forma más sencilla en que un módulo puede recuperarse a partir de algunos de sus submódulos. Luego introducimos las nociones de producto directo y de coproducto directo o suma directa externa, y estudiamos algunas de sus propiedades y la relación que hay entre estas construcciones y la suma directa interna.

6.1. Suma directa interna

Consideremos un A -módulo M y una familia $(M_j)_{j \in J}$ de submódulos de M . En general la escritura de un elemento $m \in \sum_{j \in J} M_j$ como una suma con soporte finito

$$(38) \quad m = \sum_{j \in J} m_j,$$

de elementos $m_j \in M_j$, no es única. En particular, 0 puede tener escrituras no triviales (es decir, con algún m_j no nulo). Decimos que $(M_j)_{j \in J}$ está en suma directa, o que la suma de los M_j es directa, y escribimos $\bigoplus_{j \in J} M_j$ en lugar de $\sum_{j \in J} M_j$, si la escritura (38), de cada elemento $m \in \sum_{j \in J} M_j$, es única. Si $M = \bigoplus_{j \in J} M_j$ decimos también que M es la suma directa interna de la familia de sus submódulos $(M_j)_{j \in J}$. En este caso las aplicaciones

$$\begin{array}{ccc} M_i \xrightarrow{\iota_i} M & & M \xrightarrow{\pi_i} M_i \\ m \longmapsto m & \text{y} & \sum_{j \in J} m_j \longmapsto m_i \end{array}$$

son morfismos bien definidos de A -módulos para cada $i \in J$, que satisfacen

$$\pi_i \circ \iota_j = \delta_{ij} \quad \text{y} \quad \sum_{j \in J} \iota_j \circ \pi_j = \text{id}.$$

TEOREMA 6.28. 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 $M_{\hat{i}}$ a $\sum_{j \in J \setminus \{i\}} M_j$. Son equivalentes:

1. M es suma directa interna de $(M_j)_{j \in J}$.
2. $\bigcap_{i \in J} M_{\hat{i}} = 0$.
3. $M_i \cap M_{\hat{i}} = 0$ para cada $i \in J$.
4. $M_i \cap \sum_{j < i} M_j = 0$ para todo orden total de J y cada $i \in J$.
5. Existe un orden total de J tal que $M_i \cap \sum_{j < i} M_j = 0$ 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 $M_i \subseteq \bigcap_{j \neq i} M_{\hat{j}}$.

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 $M_i \cap \sum_{j < i} M_j \neq 0$, lo que contradice al ítem 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 6.29. 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 6.24, cada uno de los sumandos es finitamente generado.

6.2. Producto directo

El producto cartesiano de una familia de A -módulos $(M_j)_{j \in J}$ es un A -módulo, llamado *producto directo* de la familia $(M_j)_{j \in J}$ y denotado $\prod_{j \in J} M_j$, vía la suma coordinada a coordinada y la *acción diagonal*

$$a \cdot (m_j)_{j \in J} = (a \cdot m_j)_{j \in J}.$$

Las proyecciones canónicas $\pi_j: \prod_{i \in I} M_i \rightarrow M_j$ 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 14.2 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:

- Para cada familia $(f_i: M \rightarrow M_i)_{i \in I}$ de morfismos de A -módulos, existe un único morfismo $\mathbf{f}: M \rightarrow \prod M_i$ tal que para cada $j \in I$ el diagrama

$$\begin{array}{ccc} M & & \\ \downarrow \mathbf{f} & \searrow f_j & \\ \prod M_i & \xrightarrow{\pi_j} & M_j \end{array}$$

conmuta.

Claramente $\mathbf{f}(m) = (f_i(m))_{i \in I}$ y $\ker \mathbf{f} = \bigcap \ker(f_i)$. Una manera equivalente de establecer la propiedad universal de $\prod M_i$ es diciendo que, para cada A -módulo M , la correspondencia

$$\begin{array}{ccc} \text{Hom}(M, \prod M_i) & \xrightarrow{\Psi} & \prod \text{Hom}(M, M_i) \\ f \mapsto & & (\pi_i \circ f)_{i \in I} \end{array}$$

es biyectiva. Es fácil ver que Ψ es un isomorfismo de grupos abelianos.

OBSERVACIÓN 6.30. Consideremos submódulos M_1, \dots, M_n de un A -módulo M . Como en el Teorema 6.28, escribamos $M_{\widehat{i}} := M_1 + \cdots + \widehat{M_i} + \cdots + M_n$. Por la propiedad universal del producto, las proyecciones canónicas $\pi_{\widehat{i}}: M \rightarrow M/M_{\widehat{i}}$ inducen un morfismo

$$M \xrightarrow{\pi} \frac{M}{M_{\widehat{1}}} \times \cdots \times \frac{M}{M_{\widehat{n}}},$$

cuyo núcleo es $\bigcap_{i=1}^n M_{\widehat{i}}$. Por la Observación 1.119, sabemos que π es sobreyectivo si y sólo si $M = M_1 + \cdots + M_n$.

COROLARIO 6.31. El morfismo π es biyectivo si y sólo si M es suma directa interna de los submódulos M_1, \dots, M_n .

DEMOSTRACIÓN. Es consecuencia inmediata del Teorema 6.28 y la Observación 6.30. \square

PROPOSICIÓN 6.32. Para cada familia $(f_i: M_i \rightarrow N_i)_{i \in I}$ de morfismos de A -módulos, existe un único morfismo

$$\prod f_i: \prod M_i \rightarrow \prod N_i$$

tal que los diagramas

$$\begin{array}{ccc} \prod M_i & \xrightarrow{\prod f_i} & \prod N_i \\ \downarrow \pi_i & & \downarrow \pi_j \\ M_j & \xrightarrow{f_j} & N_j \end{array}$$

conmutan.

DEMOSTRACIÓN. Se sigue de la propiedad universal de $\prod N_i$. \square

Es fácil ver que

$$\prod f_i((m_i)_{i \in I}) = (f_i(m_i))_{i \in I}, \quad \ker\left(\prod f_i\right) = \prod \ker(f_i) \quad \text{e} \quad \text{Im}\left(\prod f_i\right) = \prod \text{Im}(f_i).$$

OBSERVACIÓN 6.33. La correspondencia introducida en la Proposición 6.32 tiene las siguientes propiedades:

1. $\prod \text{id}_{M_i} = \text{id}_{\prod M_i}$.
2. Para cada par $(f_i: L_i \rightarrow M_i)_{i \in I}$ y $(g_i: M_i \rightarrow N_i)_{i \in I}$, de morfismos de A -módulos,

$$\left(\prod g_i\right) \circ \left(\prod f_i\right) = \prod (g_i \circ f_i).$$

OBSERVACIÓN 6.34. Si N_i es un submódulo de M_i para cada $i \in I$, entonces las proyecciones canónicas $\pi_i: M_i \rightarrow M_i/N_i$ inducen un morfismo sobreyectivo

$$\prod M_i \xrightarrow{\prod \pi_i} \prod \frac{M_i}{N_i},$$

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

$$\frac{\prod M_i}{\prod N_i} \simeq \prod \frac{M_i}{N_i}.$$

6.3. Coproducto directo

El *coproducto directo* o *suma directa* de una familia de A -módulos $(M_i)_{i \in I}$, es el submódulo $\bigoplus_{i \in I} M_i$ 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 y es fácil comprobar que las inclusiones canónicas $\iota_j: M_j \rightarrow \bigoplus_{i \in I} M_i$ son morfismos de A -módulos. Además, por los resultados de la subsección 14.3 del Capítulo 1, sabemos que

$$\pi_i(\iota_i(m)) = m \quad \text{para todo } i \in I \text{ y } m \in M_i,$$

que

$$\sum_{i \in I} \iota_i(\pi_i(m)) = m \quad \text{para todo } m \in \bigoplus M_i,$$

y que, para cada familia $(f_i: M_i \rightarrow M)_{i \in I}$, de morfismos de grupos abelianos, existe un único morfismo de grupos abelianos $\mathbf{f}: \bigoplus M_i \rightarrow M$ tal que para cada $j \in I$ el diagrama

$$\begin{array}{ccc} & & M \\ & \nearrow f_j & \uparrow \mathbf{f} \\ M_j & \xrightarrow{\iota_j} & \bigoplus M_i \end{array}$$

conmuta. Recordemos que $\mathbf{f}(m) = \sum f_j(\pi_j(m))$, donde $\pi_j: \bigoplus_{i \in I} M_i \rightarrow M_j$ es la proyección canónica. Un cálculo directo muestra que si M es un A -módulo y los f_i 's son A -lineales,

entonces \mathbf{f} es un morfismo de A -módulos. Esto establece la propiedad universal de la suma directa, la cual puede formularse también diciendo que para cada A -módulo M , la aplicación

$$\Psi: \text{Hom}_A \left(\bigoplus M_i, M \right) \rightarrow \prod \text{Hom}_A(M_i, M),$$

definida por $\Psi(\varphi) := (\varphi \circ \iota_i)_{i \in I}$, es biyectiva. En realidad vale algo más fuerte, que Ψ es un isomorfismo de grupos abelianos. Es obvio que

$$\ker \mathbf{f} = \left\{ (m_i)_{i \in I} \in \bigoplus M_i : \sum_{i \in I} f_i(m_i) = 0 \right\} \quad \text{e} \quad \text{Im } \mathbf{f} = \sum \text{Im } f_i.$$

OBSERVACIÓN 6.35. Para cada familia $(M_i)_{i \in I}$ de submódulos de un A -módulo M , la función

$$\begin{array}{ccc} \bigoplus M_i & \xrightarrow{\quad \varsigma \quad} & M \\ (m_i)_{i \in I} & \longmapsto & \sum_{i \in I} m_i \end{array}$$

es un morfismo de A -módulos. Como caso particular de lo que vimos arriba obtenemos que

$$\ker \varsigma = \left\{ (m_i)_{i \in I} \in \bigoplus M_i : \sum_{i \in I} m_i = 0 \right\} \quad \text{e} \quad \text{Im } \varsigma = \sum M_i.$$

PROPOSICIÓN 6.36. Para cada familia $(M_i)_{i \in I}$, de submódulos de un A -módulo M , son equivalentes:

1. $\sum M_i$ es suma directa interna de $(M_i)_{i \in I}$.
2. El morfismo $\varsigma: \bigoplus M_i \rightarrow M$, definido por $\varsigma((m_i)_{i \in I}) := \sum_{i \in I} m_i$, es inyectivo.

DEMOSTRACIÓN. Se lo comprueba inmediatamente. □

Notemos que esto dice que los M_i 's están en suma directa interna si y sólo si el morfismo ς es inyectivo.

PROPOSICIÓN 6.37. Para cada familia $(f_i: M_i \rightarrow N_i)_{i \in I}$, de morfismos de A -módulos, existe un único morfismo

$$\bigoplus f_i: \bigoplus M_i \rightarrow \bigoplus N_i$$

tal que los diagramas

$$\begin{array}{ccc} M_j & \xrightarrow{f_j} & N_j \\ \downarrow \iota_j & & \downarrow \iota_j \\ \bigoplus M_i & \xrightarrow{\bigoplus f_i} & \bigoplus N_i \end{array}$$

conmutan.

DEMOSTRACIÓN. Se sigue de la propiedad universal de $\bigoplus M_i$. □

Es fácil ver que

$$\left(\bigoplus f_i \right) ((m_i)_{i \in I}) = (f_i(m_i))_{i \in I}, \quad \ker \left(\bigoplus f_i \right) = \bigoplus \ker(f_i) \quad \text{e} \quad \text{Im} \left(\bigoplus f_i \right) = \bigoplus \text{Im}(f_i).$$

OBSERVACIÓN 6.38. La correspondencia introducida en la Proposición 1.124 tiene las siguientes propiedades:

1. $\bigoplus \text{id}_{M_i} = \text{id}_{\bigoplus M_i}$.
2. Para cada par $(f_i: L_i \rightarrow M_i)_{i \in I}$ y $(g_i: M_i \rightarrow N_i)_{i \in I}$, de familias de morfismos de A -módulos,

$$\left(\bigoplus g_i\right) \circ \left(\bigoplus f_i\right) = \bigoplus (g_i \circ f_i).$$

OBSERVACIÓN 6.39. Si N_i es un submódulo de M_i para cada $i \in I$, entonces las proyecciones canónicas $\pi_i: M_i \rightarrow M_i/N_i$ inducen un morfismo sobreyectivo

$$\bigoplus M_i \xrightarrow{\bigoplus \pi_i} \bigoplus \frac{M_i}{N_i},$$

cuyo núcleo es $\bigoplus N_i$. Por consiguiente,

$$\frac{\bigoplus M_i}{\bigoplus N_i} \simeq \bigoplus \frac{M_i}{N_i}.$$

6.4. Morfismos entre sumas directas finitas de A -módulos

Los resultados que daremos ahora son similares a los establecidos para grupos en la subsección (6.4) del Capítulo 1. En realidad son algo mejores, y esto se debe a que en cada A -módulo la suma es conmutativa.

Para cada par $\mathbf{M} = (M_1, \dots, M_r)$ y $\mathbf{M}' = (M'_1, \dots, M'_s)$, de familias finitas de A -módulos, el conjunto $M_{s \times r}(\text{Hom}_A(\mathbf{M}, \mathbf{M}'))$ formado por todas las matrices

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

con $f_{ij} \in \text{Hom}_A(M_j, M'_i)$, es un grupo abeliano vía la suma coordenada a coordenada. Cuando $\mathbf{M} = \mathbf{M}'$ escribiremos $M_r(\text{End}_A(\mathbf{M}))$ en lugar de $M_{r \times r}(\text{Hom}_A(\mathbf{M}, \mathbf{M}))$. Notemos que $M_r(\text{End}_A(\mathbf{M}))$ es un anillo vía el producto de matrices. De hecho, cuando $M_1 = \dots = M_r = M$, es el anillo de matrices $M_r(\text{End}_A(M))$.

OBSERVACIÓN 6.40. La aplicación

$$\theta: M_{s \times r}(\text{Hom}_A(\mathbf{M}, \mathbf{M}')) \rightarrow \text{Hom}_A(M_1 \oplus \cdots \oplus M_r, M'_1 \oplus \cdots \oplus M'_s),$$

definida por

$$\theta(f_{ij})(m_1, \dots, m_r) := \left(\sum_j f_{1j}(m_j), \dots, \sum_j f_{sj}(m_j) \right),$$

es un isomorfismo de grupos abelianos. Su inversa es la función que envía cada morfismo $f: M_1 \oplus \cdots \oplus M_r \rightarrow M'_1 \oplus \cdots \oplus M'_s$ en la matriz $(\pi_i \circ f \circ \iota_j)$, donde $\pi_i: M'_1 \oplus \cdots \oplus M'_s \rightarrow M'_i$ es la proyección canónica a la i -ésima coordenada y $\iota_j: M_j \rightarrow M_1 \oplus \cdots \oplus M_r$ 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

$$\theta(f_{ij})(m_1, \dots, m_r) = \begin{pmatrix} f_{11} & \cdots & f_{1r} \\ \vdots & \ddots & \vdots \\ f_{s1} & \cdots & f_{sr} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}.$$

Supongamos ahora que $\mathbf{M}'' = (M''_1, \dots, M''_t)$ es otra familia de A -módulos. Es fácil ver que para cada $(f_{ij}) \in M_{s \times r}(\text{Hom}(\mathbf{M}, \mathbf{M}'))$ y $(g_{kl}) \in M_{t \times s}(\text{Hom}(\mathbf{M}', \mathbf{M}''))$,

$$\theta((g_{kl})(f_{ij})) = \theta(g_{kl}) \circ \theta(f_{ij}),$$

donde $(g_{kl})(f_{ij})$ es el producto de matrices. En particular

$$\theta: M_r(\text{End}_A(\mathbf{M})) \rightarrow \text{End}_A(M_1 \oplus \cdots \oplus M_r)$$

es un isomorfismo de anillos.

OBSERVACIÓN 6.41. Para cada $B := (b_{ij}) \in M_{s \times r}(A^{\text{op}})$, denotemos con $l_B: A^r \rightarrow A^s$ al morfismo de A -módulos 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:

$$l_B(a_1, \dots, a_r) = \begin{pmatrix} b_{11} & \cdots & b_{1r} \\ \vdots & \ddots & \vdots \\ b_{s1} & \cdots & b_{sr} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix},$$

para todo $(a_1, \dots, a_r) \in A^r$. Usando los resultados de la presente subsección y la Observación 6.12, se comprueba fácilmente que la correspondencia

$$\begin{array}{ccc} M_{s \times r}(A^{\text{op}}) & \longrightarrow & \text{Hom}_A(A^r, A^s) \\ B & \longmapsto & l_B \end{array}$$

es un isomorfismo de grupos abelianos. Más aún, evidentemente $l_{I_r} = \text{id}_{A^r}$ y $l_{CB} = l_C l_B$ para cada par de matrices $B \in M_{s \times r}(A^{\text{op}})$ y $C \in M_{t \times s}(A^{\text{op}})$.

7. Sucesiones exactas cortas

Una sucesión de A -módulos y morfismos

$$\cdots \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} M_4 \longrightarrow \cdots$$

es una *sucesión exacta* si la imagen de cada morfismo es el núcleo del siguiente. Esto es, si la sucesión subyacente de morfismos de grupos abelianos es exacta. Una *sucesión exacta corta* es una sucesión exacta de la forma

$$(39) \quad 0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0.$$

Como vimos en la Sección 16 del Capítulo 1, esto ocurre si y sólo si f es inyectiva, g es sobreyectiva y $\ker g = \text{Im } f$.

Decimos que la sucesión exacta corta (39) es equivalente a la sucesión exacta corta

$$0 \longrightarrow M' \xrightarrow{i} N \xrightarrow{p} M'' \longrightarrow 0,$$

si existe un morfismo de A -módulos $h: M \rightarrow N$ tal que el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow \text{id}_{M'} & & \downarrow h & & \downarrow \text{id}_{M''} & & \\ 0 & \longrightarrow & M' & \xrightarrow{i} & N & \xrightarrow{p} & M' & \longrightarrow & 0 \end{array}$$

conmuta. Como vimos en la Sección 16 del Capítulo 1, en ese caso h es un isomorfismo. Una consecuencia inmediata de la definición es que la relación de equivalencia de sucesiones exactas cortas es reflexiva y transitiva. Ahora es claro que también es simétrica.

PROPOSICIÓN 6.42. *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 $s: M'' \rightarrow M$ y $r: M \rightarrow M'$ tales que $f \circ r + s \circ g = \text{id}_M$.

Además, si $s: M'' \rightarrow M$ y $r: M \rightarrow M'$ satisfacen la propiedad del ítem 3), entonces la sucesión

$$0 \longrightarrow M'' \xrightarrow{s} M \xrightarrow{r} M' \longrightarrow 0$$

es exacta, s es una sección de g y r una retracción de f . Por último, cada sección s de g puede completarse de manera única a un par (s, r) que satisface las condiciones requeridas en el ítem 3), y lo mismo vale para cada retracción r de f .

DEMOSTRACIÓN. Asumamos que s y r satisfacen las condiciones requeridas en el ítem 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 $\text{Im } s \subseteq \ker r$. En realidad $\text{Im } s = \ker r$ 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 ítems 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

$$g \circ (\text{id}_M - s \circ g) = 0,$$

existe un único morfismo de A -módulos $r: M \rightarrow M'$ tal que $f \circ r = \text{id}_M - s \circ g$.

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 $s: M'' \rightarrow M$ tal que $f \circ r + s \circ g = \text{id}_M$. \square

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

$$(40) \quad 0 \longrightarrow M' \xrightarrow{\iota_{M'}} M' \oplus M'' \xrightarrow{\pi_{M''}} M'' \longrightarrow 0,$$

donde $\iota_{M'}$ y $\pi_{M''}$ son la inclusión y proyección canónicas, es escindida. El siguiente resultado muestra que este ejemplo es arquetípico.

PROPOSICIÓN 6.43. *Una sucesión exacta corta de A -módulos*

$$(41) \quad 0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

es escindida si y sólo si es equivalente a la sucesión exacta corta (40).

DEMOSTRACIÓN. Basta observar que un morfismo $(r, h): M \rightarrow M' \oplus M''$ realiza una equivalencia entre las sucesiones exactas cortas (40) y (41) si y sólo si $h = g$ y r es una retracción de f . \square

Capítulo 7

Algunos tipos de módulos

1. Módulos libres

Consideremos un A -módulo M y un subconjunto S de M . Una *combinación lineal* de elementos de S es una suma

$$\sum_{s \in S} a_s \cdot s,$$

donde cada $a_s \in A$ y $(a_s)_{s \in S}$ es una familia con soporte finito. Al escalar a_s se lo llama el *coeficiente* de s en la combinación lineal. Es evidente que el conjunto de las combinaciones lineales de elementos de S coincide con el submódulo de M generado por S . Decimos que S es *linealmente independiente* si

$$\sum_{s \in S} a_s \cdot s = 0 \Rightarrow a_s = 0 \quad \text{para todo } s.$$

Es decir, si la única combinación lineal de elementos de S que da cero es la trivial. En este caso cada elemento de AS se escribe de manera única como combinación lineal de elementos de S , porque

$$\sum_{s \in S} a_s \cdot s = \sum_{s \in S} b_s \cdot s \Rightarrow \sum_{s \in S} (a_s - b_s) \cdot s = 0 \Rightarrow a_s - b_s = 0 \quad \text{para todo } s.$$

Por último, decimos que S es una *base* de M , si es un conjunto linealmente independiente de generadores de M . Un A -módulo M es *libre* si tiene una base. No todo A -módulo es libre. Por ejemplo el \mathbb{Z} -módulo $\mathbb{Z}/2\mathbb{Z}$ no lo es. Por otra parte, para cada conjunto I , el A -módulo $A^{(I)}$ es libre. Una base, que siguiendo una tradición firmemente establecida, llamaremos *base canónica* de $A^{(I)}$, es el conjunto $\{e_i : i \in I\}$, donde $e_i : I \rightarrow A$ es la función que vale 1 en i y 0 en todos los otros puntos de su dominio.

OBSERVACIÓN 7.1. Si M es un A -módulo libre con base S y $f : M \rightarrow N$ 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 $f: S \rightarrow N$ 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 $\bar{f}: M \rightarrow N$, tal que el triángulo

$$\begin{array}{ccc} S & \xrightarrow{f} & N \\ \downarrow \iota & \nearrow \bar{f} & \\ M & & \end{array},$$

donde $\iota: S \rightarrow M$ es la inclusión canónica, conmuta.

En efecto, debido a que cada elemento $m \in M$ es una combinación lineal

$$(42) \quad m = \sum_{s \in S} a_s \cdot s,$$

necesariamente $\bar{f}(m) = \sum_{s \in S} a_s \cdot f(s)$. Como la escritura (42) es única, esta definición no es ambigua. Finalmente, es fácil comprobar que la función \bar{f} que acabamos de determinar, es A -lineal.

PROPOSICIÓN 7.2. *Si M es un A -módulo libre con una base S , entonces M es canónicamente isomorfo a $A^{(S)}$.*

DEMOSTRACIÓN. Por las propiedades universales de (M, S) y $(A^{(S)}, \{e_s : s \in S\})$, existen morfismos únicos de A -módulos

$$f: A^{(S)} \rightarrow M \quad \text{y} \quad g: M \rightarrow A^{(S)}$$

tales que $f(e_s) = s$ y $g(s) = e_s$ para todo $s \in S$. Como los triángulos

$$\begin{array}{ccc} S & \xrightarrow{\iota} & M \\ \downarrow \iota & \nearrow f \circ g & \\ M & & \end{array} \quad \text{y} \quad \begin{array}{ccc} S & \xrightarrow{\iota} & M \\ \downarrow \iota & \nearrow \text{id} & \\ M & & \end{array}$$

conmutan, se sigue de la unicidad en la propiedad universal de (M, S) que $f \circ g = \text{id}_M$. Similarmente, $g \circ f = \text{id}_{A^{(S)}}$. \square

NOTA 7.3. *La palabra canónicamente en el enunciado de la proposición anterior hace referencia al hecho de que el isomorfismo $f: A^{(S)} \rightarrow M$ es el único que extiende a la biyección $e_s \mapsto s$, de la base canónica de $A^{(S)}$ en S .*

TEOREMA 7.4. *Supongamos que A es un anillo no nulo. Son equivalentes:*

1. *Todos los A -módulos son libres.*
2. *A tiene un A -módulo simple libre.*
3. *A es un anillo de división.*

DEMOSTRACIÓN. 1) \Rightarrow 2) Es suficiente verificar que hay un A -módulo simple. Para ello basta notar que por la Proposición 6.25 el anillo A tiene un ideal a izquierda maximal I y, que por la Proposición 6.22, 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

$$\begin{array}{ccc} A & \xrightarrow{\rho(a)} & M \\ a & \longmapsto & a \cdot m \end{array}$$

es un isomorfismo. Así, A es un A -módulo simple y entonces, por la Proposición 4.25, 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 S . Si $m \in M \setminus S$, entonces $S \cup \{m\}$ es linealmente dependiente y, por lo tanto, hay una combinación lineal no trivial

$$\lambda_m \cdot m + \sum_{s \in S} \lambda_s \cdot s = 0.$$

Por la independencia lineal de S , necesariamente $\lambda_m \neq 0$. Despejando obtenemos que

$$m = - \sum_{s \in S} \lambda_m^{-1} \lambda_s \cdot s,$$

lo cual prueba que $\langle S \rangle \supseteq (M \setminus S) \cup S = M$ y muestra que S es una base de M . □

OBSERVACIÓN 7.5. Todo A -módulo M es isomorfo a un cociente de un módulo libre. Más precisamente, si S es un conjunto de generadores de M , entonces la función $\pi: A^{(S)} \rightarrow M$, definida por $\pi(e_s) := s$, para todo $s \in S$, es un epimorfismo. Por lo tanto $M \simeq A^{(S)} / \ker \pi$.

Ampliando un poco la definición dada arriba, diremos que un *A -módulo libre sobre un conjunto X* es cualquier par (M, j) , formado por un A -módulo M y una función $j: X \rightarrow M$, que tiene la siguiente propiedad universal:

- Para cada función $f: X \rightarrow N$, de X en un A -módulo N , existe un único morfismo de A -módulos $\bar{f}: M \rightarrow N$, tal que el triángulo

$$\begin{array}{ccc} X & \xrightarrow{f} & N \\ \downarrow j & \nearrow \bar{f} & \\ M & & \end{array},$$

conmuta.

OBSERVACIÓN 7.6. Si (M, j) es un A -módulo libre sobre X , $l: Y \rightarrow X$ es una función biyectiva y $\varphi: M \rightarrow N$ es un isomorfismo de A -módulos, entonces $(N, \varphi \circ j \circ l)$ es un A -módulo libre sobre Y .

PROPOSICIÓN 7.7. Un par (M, j) , formado por un A -módulo M y una función $j: X \rightarrow M$, es un A -módulo libre sobre X si y sólo si la aplicación A -lineal $\varphi: A^{(X)} \rightarrow M$, definida por $\varphi(e_x) := j(x)$, es un isomorfismo. En consecuencia, j es inyectiva y $j(X)$ es una base de M .

DEMOSTRACIÓN. Por la observación anterior si φ es un isomorfismo, entonces (M, j) tiene la propiedad universal requerida. Recíprocamente, si (M, j) tiene esta propiedad, entonces hay

un único morfismo $\psi: M \rightarrow A^{(X)}$ tal que el triángulo

$$\begin{array}{ccc} X & \xrightarrow{j} & M \\ \downarrow \iota & & \swarrow \psi \\ A^{(X)} & & \end{array},$$

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 $\psi \circ \varphi = \text{id}_{A^{(X)}}$ y $\varphi \circ \psi = \text{id}_M$. \square

PROPOSICIÓN 7.8. *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 6.11. \square

Decimos que un anillo A satisface la propiedad de *invariancia del cardinal de las bases*, o, por brevedad, que tiene o satisface la ICB, si en cada A -módulo libre todas las bases tienen el mismo cardinal. Como un módulo libre finitamente generado es isomorfo a uno de la forma A^n y, por la proposición anterior, todas las bases de un módulo libre no finitamente generado, son coordinables, A tiene la ICB si y sólo si $A^n \simeq A^m \Leftrightarrow n = m$. Finalmente, puesto que tener un isomorfismo $A^n \simeq A^m$ es lo mismo que tener matrices $A \in M_{m \times n}(A)$ y $B \in M_{n \times m}(A)$ tales que $AB = I_m$ y $BA = I_n$, donde $I_m \in M_m(A)$ e $I_n \in M_n(A)$ son las matrices identidad, es inmediato que A tiene la ICB si y sólo si la existencia de tales matrices es imposible cuando $m \neq n$.

EJEMPLO 7.9. *Para cada anillo no nulo A , el anillo $B := \text{End}_A(A^{(\mathbb{N})})$ no tiene la ICB. Para verificarlo basta observar que la aplicación $\psi = (\psi_1, \psi_2)$ de B en $B \oplus B$, definida por*

$$\psi_1(f)(e_i) := f(e_{2i-1}) \quad \text{y} \quad \psi_2(f)(e_i) := f(e_{2i}),$$

donde $\{e_n : n \in \mathbb{N}\}$ es la base canónica de $A^{(\mathbb{N})}$, es un isomorfismo de B -módulos.

PROPOSICIÓN 7.10. *Se satisfacen las siguientes propiedades:*

1. *Un anillo A tiene la ICB si y sólo si A^{op} la tiene.*
2. *Si A tiene la ICB, entonces $M_r(A)$ tiene la ICB para todo $r \in \mathbb{N}$.*
3. *Si $f: A \rightarrow B$ 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 $M_{m \times n}(M_r(A))$ puede verse de manera evidente como una matriz en $M_{mr \times nr}(A)$ y porque esta correspondencia respeta productos e identidades. Para probar que vale la tercera es suficiente mostrar que si dos matrices $A \in M_{m \times n}(A)$ y $B \in M_{n \times m}(A)$ satisfacen $AB = I_m$ y $BA = I_n$, entonces $m = n$. Para ello basta observar que aplicando f en cada coordenada de A y de B se obtienen matrices $A' \in M_{m \times n}(B)$ y $B' \in M_{n \times m}(B)$ tales que $A'B' = I_m$ y $B'A' = I_n$, y que (como por hipótesis B tiene la ICB) esto implica que $m = n$. \square

Un A -módulo a izquierda M es *hopfiano* si todo endomorfismo sobreyectivo $f: M \rightarrow M$ es un isomorfismo.

PROPOSICIÓN 7.11. *Si todo A -módulo libre finitamente generado es hopfiano, entonces A satisface la ICB.*

DEMOSTRACIÓN. Supongamos que existe un isomorfismo $f: A^m \rightarrow A^n$, con $m, n \in \mathbb{N}$, y $m < n$. Entonces la función

$$\begin{aligned} A^n &\xrightarrow{g} A^n, \\ (x_1, \dots, x_n) &\longmapsto f(x_1, \dots, x_m) \end{aligned},$$

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.

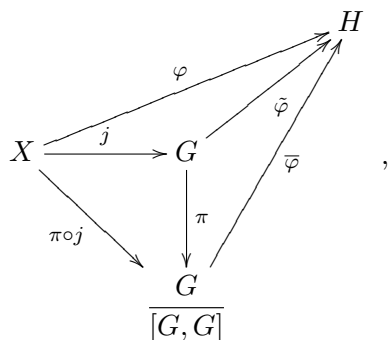
TEOREMA 7.12. *Todos los anillos conmutativos satisfacen la ICB.*

DEMOSTRACIÓN. Por el Corolario 4.39, hay un morfismo de A en un cuerpo. Así el teorema se sigue del ítem 3) de la Proposición 7.10 y de que todos los anillos de división satisfacen la ICB. □

Ahora estamos en posición de probar el Teorema 1.101. Para ello será conveniente establecer primero un resultado auxiliar, que es importante en si mismo.

PROPOSICIÓN 7.13. *Si (G, j) es un grupo libre, entonces el par $(G/[G, G], \pi \circ j)$, donde $\pi: G \rightarrow G/[G, G]$ es la proyección canónica, es un \mathbb{Z} -módulo libre.*

DEMOSTRACIÓN. Denotemos con X al dominio de j y tomemos una función $\varphi: X \rightarrow H$, de X en un grupo abeliano H . Por las propiedades universales de (G, j) y del abelianizado de G , existen morfismos únicos $\tilde{\varphi}: G \rightarrow H$ y $\bar{\varphi}: G/[G, G] \rightarrow H$ tales que el diagrama



donde π es la proyección canónica, conmuta. En particular, $\bar{\varphi} \circ \pi \circ j = \varphi$. Además $\bar{\varphi}$ es el único morfismo con esta propiedad, porque si $\hat{\varphi}: G/[G, G] \rightarrow H$ también satisface $\hat{\varphi} \circ \pi \circ j = \varphi$, entonces, por la propiedad universal de (G, j) , forzosamente $\hat{\varphi} \circ \pi = \bar{\varphi} \circ \pi$ y, por lo tanto, dado que π es sobreyectivo, $\hat{\varphi} = \bar{\varphi}$. □

DEMOSTRACIÓN DEL TEOREMA 1.101. Supongamos que (G, j) y (H, l) son grupos libres sobre X e Y respectivamente. Por los comentarios hechos al comienzo de la subsección 17.1 del Capítulo 1, sabemos que si G y H son isomorfos, entonces $G/[G, G]$ y $H/[H, H]$ también lo son. Debido la Proposición 7.13 y al Teorema 7.12, esto implica que $|X| = |Y|$. Recíprocamente,

por la propiedad universal de (G, j) , dada una biyección $\varphi: X \rightarrow Y$, existen morfismos únicos $\overline{\varphi}: G \rightarrow H$ y $\overline{\varphi}^{-1}: H \rightarrow G$ tales que los diagramas

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & Y \\ \downarrow j & & \downarrow l \\ G & \xrightarrow{\overline{\varphi}} & H \end{array} \quad y \quad \begin{array}{ccc} Y & \xrightarrow{\varphi^{-1}} & X \\ \downarrow l & & \downarrow j \\ H & \xrightarrow{\overline{\varphi}^{-1}} & G \end{array}$$

conmutan. Como

$$\overline{\varphi}^{-1} \circ \overline{\varphi} \circ j = j \circ \varphi^{-1} \circ \varphi = j,$$

debe ser $\overline{\varphi}^{-1} \circ \overline{\varphi} = \text{id}_G$. Un argumento similar muestra que $\overline{\varphi} \circ \overline{\varphi}^{-1} = \text{id}_H$. □

2. Módulos de torsión y divisibles

En esta sección asumimos que A es un dominio conmutativo y estudiamos las nociones de torsión y divisibilidad de A -módulos.

2.1. Torsión

Un elemento m de un A -módulo M es *de torsión* si existe $a \in A \setminus \{0\}$ tal que $a \cdot m = 0$. Por ejemplo $([1], 0)$ es un elemento de torsión del \mathbb{Z} -módulo $\mathbb{Z}_3 \oplus \mathbb{Z}$, mientras que $(0, 1)$ no lo es. La *torsión* de M es el conjunto

$$T(M) := \{m \in M : m \text{ es de torsión}\}.$$

Un A -módulo M es *de torsión* si $T(M) = M$ y es *sin torsión* si $T(M) = 0$.

EJEMPLO 7.14. *Cada A -módulo libre es sin torsión.*

EJEMPLO 7.15. *El \mathbb{Z} -módulo \mathbb{Q} no tiene torsión pero no es libre.*

PROPOSICIÓN 7.16. *Para cada A -módulo M , el conjunto $T(M)$ es un submódulo de M .*

DEMOSTRACIÓN. Basta observar que para todo $b \in A$ y $m, m' \in M$, si $a \cdot m = a' \cdot m' = 0$ con $a, a' \in A \setminus \{0\}$, entonces

$$aa' \cdot (m + m') = aa' \cdot m + aa' \cdot m' = a'a \cdot m + aa' \cdot m' = 0 \quad y \quad a \cdot (b \cdot m) = b \cdot (a \cdot m) = 0$$

porque A es conmutativo, y que $aa' \neq 0$ porque A es un dominio. □

PROPOSICIÓN 7.17. *Para cada A -módulo M , el submódulo $T(M)$ es de torsión y el módulo cociente $M/T(M)$ es sin torsión.*

DEMOSTRACIÓN. Es evidente que la primera afirmación es verdadera. Veamos que también lo es la segunda. Tomemos $m \in M$. Si $[m] \in T(M/T(M))$, entonces $a \cdot m \in T(M)$ para algún $a \in A \setminus \{0\}$ y, por lo tanto, existe $b \in A \setminus \{0\}$ tal que $ba \cdot m = b \cdot (a \cdot m) = 0$. Como $ba \neq 0$, esto implica que $m \in T(M)$. □

PROPOSICIÓN 7.18. *Para cada morfismo de A -módulos $f: M \rightarrow N$,*

$$f(T(M)) \subseteq T(N).$$

Además si f es inyectivo, entonces $f(T(M)) = f(M) \cap T(N)$.

DEMOSTRACIÓN. Tomemos $a \in A \setminus \{0\}$ y $m \in M$. La inclusión se sigue inmediatamente de que si $a \cdot m = 0$, entonces $a \cdot f(m) = f(a \cdot m) = 0$. Supongamos ahora que f es inyectiva y que $a \cdot f(m) = 0$. Entonces $f(a \cdot m) = a \cdot f(m) = 0$ y así $a \cdot m = 0$. esto muestra que en este caso $f(T(M)) = f(M) \cap T(N)$. \square

OBSERVACIÓN 7.19. Por la proposición anterior cada morfismo de A -módulos $f: M \rightarrow N$ induce por restricción y por paso al cociente, morfismos

$$f_T: T(M) \rightarrow T(N) \quad y \quad \bar{f}_T: \frac{M}{T(M)} \rightarrow \frac{N}{T(N)}.$$

Se comprueba facilmente que

$$(\text{id}_M)_T = \text{id}_{T(M)} \quad y \quad (\overline{\text{id}_M})_T = \text{id}_{M/T(M)}$$

para cada A -módulo M , y que

$$(g \circ f)_T = g_T \circ f_T \quad y \quad \overline{(g \circ f)}_T = \bar{g}_T \circ \bar{f}_T,$$

para cada par de morfismos de A -módulos $f: M \rightarrow N$ y $g: N \rightarrow L$.

2.2. Divisibilidad

Decimos que un A -módulo M es *divisible* si para cada $m \in M$ y cada $a \in A \setminus \{0\}$, existe $m' \in M$ tal que $a \cdot m' = m$.

EJEMPLO 7.20. 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 7.21. Los módulos divisibles tienen las siguientes propiedades:

1. El producto directo de una familia de módulos divisibles es divisible.
2. La suma directa de una familia de módulos divisibles es divisible.
3. Todo sumando directo de un módulo divisible es divisible.

DEMOSTRACIÓN. Dejada al lector. \square

PROPOSICIÓN 7.22. Si un A -módulo M es divisible, entonces también lo es cada uno de sus cocientes M/N .

DEMOSTRACIÓN. Porque $a \cdot m' = m \Rightarrow a \cdot [m'] = [m]$. \square

LEMA 7.23. Si M es un A -módulo divisible y sin torsión, entonces para cada $m \in M$ y cada $a \in A \setminus \{0\}$ existe un único $m' \in M$ tal que $a \cdot m' = m$.

DEMOSTRACIÓN. Como M es divisible, existe m' tal que $a \cdot m' = m$. Si también $a \cdot m'' = m$, entonces

$$a \cdot (m' - m'') = 0,$$

por lo que $m' = m''$, debido a que M es sin torsión. \square

TEOREMA 7.24. 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

$$q \cdot \left(\frac{p}{q} \cdot m \right) = \frac{qp}{1q} \cdot m = p \cdot m$$

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 obliga a definir

$$(43) \quad \frac{p}{q} \cdot m := m'.$$

Para ver que esta definición es buena, basta observar que si $\frac{p}{q} = \frac{r}{s}$ y $s \cdot m'' = r \cdot m$, entonces $m' = m''$. Pero esto es así pues M no tiene torsión, $qs \neq 0$ y

$$qs \cdot m'' = qr \cdot m = sp \cdot m = qs \cdot m'.$$

Notemos que

$$q \cdot \left(\frac{p}{q} \cdot m \right) = q \cdot m' = p \cdot m \quad \text{para todo } \frac{p}{q} \in \mathbb{Q}_A \text{ y } m \in M.$$

Para concluir la demostración debemos probar que M es un \mathbb{Q}_A -módulo via (43). 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. \square

PROPOSICIÓN 7.25. *Para todo A -módulo N existen un A -módulo divisible M y un monomorfismo $\iota: N \rightarrow M$. Si N no tiene torsión, entonces se puede tomar M sin torsión.*

DEMOSTRACIÓN. Tomemos un conjunto I de generadores de N arbitrario. Es claro que podemos suponer sin pérdida de generalidad que $N = A^{(I)}/S$ para un submódulo S de $A^{(I)}$. Pero por la Proposición 7.22 sabemos que $M = \mathbb{Q}_A^{(I)}/S$ es divisible, y es evidente que la inclusión canónica de $A^{(I)}$ en $\mathbb{Q}_A^{(I)}$ induce un monomorfismo ι de N en M . Además, debido a la Proposición 7.18,

$$\iota(N) \cap T(M) = \iota(T(N)).$$

En consecuencia si $T(N) = 0$, entonces la composición

$$N \xrightarrow{\iota} M \xrightarrow{\pi} \frac{M}{T(M)},$$

donde π es la proyección canónica, es inyectiva y así, en este caso, podemos reemplazar M por el módulo sin torsión $M/T(M)$. \square

Notemos que si N es sin torsión, entonces la dimensión del \mathbb{Q}_A -espacio vectorial M , construido en la demostración, es menor o igual al cardinal del conjunto de generadores de N elegido.

TEOREMA 7.26. Si N es un A -módulo finitamente generado y sin torsión, entonces existe un A -módulo libre finitamente generado y un monomorfismo $\iota: N \rightarrow M$.

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 $n_j \in S \setminus B$ 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

$$\begin{array}{ccc} N & \xrightarrow{\iota} & M \\ n & \longmapsto & \lambda \cdot n \end{array} .$$

Dado que A es conmutativo y N es sin torsión, ι es un morfismo inyectivo de A -módulos. Como M es libre con base B , esto termina la prueba. \square

3. Módulos proyectivos y módulos inyectivos

En la Subsección 3.1 vimos que los conjuntos $\text{Hom}_A(M, N)$ tienen estructuras naturales de grupos abelianos tales que dados morfismos de A -módulos $v: N \rightarrow N'$ y $u: M' \rightarrow M$, las funciones

$$v_*: \text{Hom}_A(M, N) \rightarrow \text{Hom}_A(M, N') \quad \text{y} \quad u^*: \text{Hom}_A(M', N) \rightarrow \text{Hom}_A(M, N),$$

definidas por $v_*(f) = v \circ f$ y $u^*(f) = f \circ u$, son morfismos de grupos. En esta sección estudiamos el comportamiento de estas funciones respecto de la exactitud.

TEOREMA 7.27. Una sucesión

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'',$$

de morfismos de A -módulos, es exacta si y sólo si la sucesión inducida

$$0 \longrightarrow \text{Hom}_A(M, N') \xrightarrow{f_*} \text{Hom}_A(M, N) \xrightarrow{g_*} \text{Hom}_A(M, N'')$$

lo es, para cada módulo M .

DEMOSTRACIÓN. Por definición, f es un monomorfismo si y sólo si f_* es inyectivo para todo M . Además es claro que

$$g \circ f = 0 \Rightarrow g_* \circ f_* = 0$$

para todo A -módulo M . Recíprocamente, si $g_* \circ f_* = 0$ para $M := N'$, entonces

$$g \circ f = g_* \circ f_*(\text{id}_{N'}) = 0.$$

Supongamos ahora que f es un monomorfismo e $\text{Im } f = \ker g$, y tomemos $v: M \rightarrow N$ tal que $g_*(v) = 0$. Debido a la propiedad universal de la inclusión canónica $\iota: \ker g \rightarrow N$ y a que f define un isomorfismo de N' en $\ker g$, existe un único morfismo $v': M \rightarrow N'$ tal que

$$f_*(v') = f \circ v' = v.$$

Así, en este caso, $\ker(g_*) = \text{Im}(f_*)$ para todo A -módulo M . Para terminar la demostración será suficiente ver que si $\ker(g_*) = \text{Im}(f_*)$ para $M := \ker g$, entonces $\ker g \subseteq \text{Im } f$. Pero como $g_*(\iota) = 0$ para la inclusión canónica $\iota: \ker g \rightarrow N$, existe $\iota': \ker g \rightarrow N'$ tal que $f \circ \iota' = f_*(\iota') = \iota$ y, así, $\ker g = \text{Im } \iota \subseteq \text{Im } f$. \square

TEOREMA 7.28. *Una sucesión*

$$N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$

de morfismos de A -módulos, es exacta si y sólo si la sucesión inducida

$$0 \longrightarrow \text{Hom}_A(N'', M) \xrightarrow{g^*} \text{Hom}_A(N, M) \xrightarrow{f^*} \text{Hom}_A(N', M)$$

lo es, para cada módulo M .

DEMOSTRACIÓN. Dejada al lector. □

PROPOSICIÓN 7.29. *Consideremos morfismos de A -módulos $f: N' \rightarrow N$ y $g: N \rightarrow N''$. Son equivalentes:*

1. *La sucesión*

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$

es escindida.

2. *Para cada módulo M , la sucesión inducida*

$$0 \longrightarrow \text{Hom}_A(M, N') \xrightarrow{f_*} \text{Hom}_A(M, N) \xrightarrow{g_*} \text{Hom}_A(M, N'') \longrightarrow 0$$

es exacta.

3. *Para cada módulo M , la sucesión inducida*

$$0 \longrightarrow \text{Hom}_A(N'', M) \xrightarrow{g^*} \text{Hom}_A(N, M) \xrightarrow{f^*} \text{Hom}_A(N', M) \longrightarrow 0$$

es exacta.

DEMOSTRACIÓN. Si s es una sección de g , entonces claramente s_* es una sección de g_* , cualquiera sea M . En particular g_* es sobreyectiva. Recíprocamente, si g_* es sobreyectiva para $M := N''$, entonces existe $s: N'' \rightarrow N$ tal que $g \circ s = g_*(s) = \text{id}_{N''}$. Por el Teorema 7.27, esto prueba que 1) \Leftrightarrow 2). La demostración de la equivalencia entre 1) y 3) es similar. □

Decimos que un A -módulo P es *proyectivo* si dados un morfismo $\varphi': P \rightarrow N'$ y un morfismo sobreyectivo $g: N \twoheadrightarrow N'$, existe un morfismo $\varphi: P \rightarrow N$ tal que el diagrama

$$\begin{array}{ccc} & P & \\ \varphi \swarrow & \downarrow \varphi' & \\ N & \xrightarrow{g} & N' \end{array}$$

conmuta.

PROPOSICIÓN 7.30. *La suma de una familia de módulos proyectivos es un módulo proyectivo y todo sumando directo de un módulo proyectivo es proyectivo.*

DEMOSTRACIÓN. Supongamos que $(P_i)_{i \in I}$ es una familia de módulos proyectivos, que $g: N \twoheadrightarrow N'$ es un morfismo sobreyectivo y que

$$\varphi': \bigoplus_{i \in I} P_i \rightarrow N'$$

es un morfismo. Como los P_j 's son módulos proyectivos, existen morfismos $\varphi_j: P_j \rightarrow N$ tales que $g \circ \varphi_j = \varphi' \circ \iota_j$, donde ι_j es la inclusión canónica de P_j en $\bigoplus_{i \in I} P_i$. Por la propiedad universal de la suma directa hay un único morfismo

$$\varphi: \bigoplus_{i \in I} P_i \rightarrow N$$

tal que $\varphi \circ \iota_j = \varphi_j$ para todo $j \in J$. Para concluir que la primera afirmación es verdadera resta probar que $g \circ \varphi = \varphi'$, pero esto es consecuencia inmediata de que $g \circ \varphi \circ \iota_j = g \circ \varphi_j = \varphi' \circ \iota_j$ para todo $j \in I$.

Consideremos ahora la segunda afirmación. Supongamos que $g: N \rightarrow N'$ es un epimorfismo, que $\varphi': P \rightarrow N'$ es un morfismo y que existe un módulo Q tal que $P \oplus Q$ es proyectivo. Entonces hay un morfismo $\varphi: P \oplus Q \rightarrow N$ tal que $g \circ \varphi = \varphi' \circ \pi_P$, donde $\pi_P: P \oplus Q \rightarrow P$ es la proyección canónica. Componiendo con la inclusión canónica $\iota_P: P \rightarrow P \oplus Q$ obtenemos la igualdad

$$g \circ \varphi \circ \iota_P = \varphi' \circ \pi_P \circ \iota_P = \varphi',$$

la cual muestra que P es proyectivo. □

En la siguiente proposición damos varias caracterizaciones de los módulos proyectivos

PROPOSICIÓN 7.31. *Para cada A -módulo P son equivalentes:*

1. P es proyectivo.
2. Si $g: N \rightarrow N'$ es un epimorfismo, entonces $g_*: \text{Hom}_A(P, N) \rightarrow \text{Hom}_A(P, N')$ es un epimorfismo.
3. Si

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$

es una sucesión exacta, entonces

$$0 \longrightarrow \text{Hom}_A(P, N') \xrightarrow{f_*} \text{Hom}_A(P, N) \xrightarrow{g_*} \text{Hom}_A(P, N'') \longrightarrow 0$$

también lo es.

4. Todo epimorfismo $g: N \rightarrow P$ es una retracción.
5. P es isomorfo a un sumando directo de un módulo libre.

DEMOSTRACIÓN. Es claro que 1) \Leftrightarrow 2). Además, por el Teorema 7.27, los items 2) y 3) también son equivalentes. El cuarto item se sigue del primero tomando $f' = \text{id}_P$. Como todo módulo es cociente de un módulo libre, 4) \Rightarrow 5). Finalmente, debido a la proposición anterior, para probar que 5) \Rightarrow 1) es suficiente ver que A es proyectivo, lo cual es evidente. □

Un A -módulo I es *inyectivo* si dados un morfismo $\varphi': N' \rightarrow I$ y un morfismo inyectivo $f: N' \hookrightarrow N$, existe un morfismo $\varphi: N \rightarrow I$ tal que el diagrama

$$\begin{array}{ccc} & I & \\ & \uparrow \varphi' & \swarrow \varphi \\ N' & \xrightarrow{f} & N \end{array}$$

conmuta.

PROPOSICIÓN 7.32. *El producto de una familia de módulos inyectivos es un módulo inyectivo y todo sumando directo de un módulo inyectivo es inyectivo.*

DEMOSTRACIÓN. Dejada al lector. □

PROPOSICIÓN 7.33. *Para cada A -módulo I son equivalentes:*

1. I es inyectivo.
2. Si $f: N' \rightarrow N$ es un monomorfismo, entonces $f^*: \text{Hom}_A(N, I) \rightarrow \text{Hom}_A(N', I)$ es sobreyectiva.
3. Si

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$

es una sucesión exacta, entonces

$$0 \longrightarrow \text{Hom}_A(N'', I) \xrightarrow{g^*} \text{Hom}_A(N, I) \xrightarrow{f^*} \text{Hom}_A(N', I) \longrightarrow 0$$

también lo es.

4. Todo monomorfismo $f: I \rightarrow N$ es una sección.

DEMOSTRACIÓN. Es claro que 1) \Leftrightarrow 2). Además, por el Teorema 7.28, los items 2) y 3) también son equivalentes. El cuarto item se sigue del primero tomando $\varphi' = \text{id}_I$. Solamente resta probar que 4) \Rightarrow 1). Para ello, dados un morfismo $\varphi': N' \rightarrow I$ y un morfismo inyectivo $f: N' \hookrightarrow N$, consideremos el diagrama conmutativo

$$\begin{array}{ccc} I & \xrightarrow{\iota_I} & I \oplus_{\varphi', f} N \\ \varphi' \uparrow & & \uparrow \iota_N \\ N' & \xrightarrow{f} & N \end{array}$$

donde $I \oplus_{\varphi', f} N$ es el cociente de $I \oplus N$ por el submódulo $J := \{(\varphi'(n), -f(n)) : n \in N'\}$ e ι_I, ι_N son los morfismos inducidos por las inclusiones canónicas a la suma directa. Afirmamos que ι_I es inyectivo. En efecto si $(m, 0) = (\varphi'(n), -f(n))$, entonces $n = 0$ porque f es un monomorfismo y, por lo tanto, $m = \varphi'(0) = 0$. Así, por hipótesis, ι_I tiene una retracción r , y es evidente que $r \circ \iota_N \circ f = r \circ \iota_I \circ \varphi' = \varphi'$. □

TEOREMA 7.34 (Baer). *Si todo morfismo de un ideal a izquierda de A en A -módulo I , se extiende a A , entonces I es inyectivo.*

DEMOSTRACIÓN. Supongamos que $f: N' \rightarrow N$ es un monomorfismo y que $\varphi': N' \rightarrow I$ es un morfismo. Una extensión parcial de φ' es un par (L, l) , formado por un submódulo L de N que contiene a $f(N')$ y un morfismo $l: L \rightarrow I$ tal que $l \circ f = \varphi'$. El conjunto de las extensiones parciales de φ' está ordenado por

$$(L, l) \leq (H, h) \quad \text{si} \quad L \subseteq H \quad \text{y} \quad h|_L = l.$$

Por el lema de Zorn hay una extensión parcial maximal $\varphi: M \rightarrow I$ de φ' . Para terminar la prueba será suficiente verificar que $M = N$. Tomemos $n \in N$ arbitrario y consideremos la aplicación A -lineal $\phi: (M : n) \rightarrow I$, dada por $\phi(a) := \varphi(a \cdot n)$. Por hipótesis ϕ se extiende a un morfismo $\psi: A \rightarrow I$. Definimos $\bar{\varphi}: M + An \rightarrow I$ por $\bar{\varphi}(m + a \cdot n) := \varphi(m) + \psi(a)$ para $m \in M$ y $a \in A$. Esta definición es correcta porque si $m + a \cdot n = m' + a' \cdot n$ con $a, a' \in A$ y $m, m' \in M$, entonces $a' - a \in (M : n)$ y así,

$$\varphi(m) - \varphi(m') = \varphi((a' - a) \cdot n) = \phi(a' - a) = \psi(a') - \psi(a).$$

Debido a la maximalidad de (M, φ) , de la existencia de la extensión $(M + An, \bar{\varphi})$, se sigue que $n \in M$. □

PROPOSICIÓN 7.35. *Supongamos que A es un dominio. Entonces todo módulo inyectivo es divisible. Si además A es principal, entonces vale la recíproca.*

DEMOSTRACIÓN. Supongamos primero que I es inyectivo, tomemos $m \in I$ y $a \in A$ y consideremos la aplicación A -lineal $f: Aa \rightarrow I$, dada por $f(ba) := b \cdot m$. Por hipótesis, existe una extensión $\bar{f}: A \rightarrow I$ de f . Es evidente que $a\bar{f}(1) = f(a) = m$. Supongamos ahora que I es divisible y que todo ideal de A es monogenerado. Por el teorema de Baer, para probar que I es inyectivo será suficiente mostrar que, para cada $a \in A$, todo morfismo $f: Aa \rightarrow I$ se extiende a A . Como I es divisible, existe $m \in I$ tal que $a \cdot m = f(a)$. Es claro que la función $\bar{f}: A \rightarrow I$, definida por $\bar{f}(b) := b \cdot m$, es un morfismo de A -módulos que extiende a f . \square

Capítulo 8

Condiciones de cadena

Nuestro objetivo en esta sección es introducir las nociones de anillos noetherianos y artinianos y estudiar sus propiedades básicas. En esta exposición M designa a un A -módulo arbitrario.

1. Módulos noetherianos

Un A -módulo es *noetheriano* si todos sus submódulos son finitamente generados. En el siguiente resultado establecemos otras caracterizaciones muy útiles de estos módulos. Una sucesión $M_1, M_2, M_3, M_4, \dots$ 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 8.1. *Son equivalentes:*

1. M es noetheriano.
2. Toda sucesión creciente $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$ de submódulos de M es estacionaria.
3. Toda familia no vacía de submódulos de M tiene un elemento maximal.

DEMOSTRACIÓN. 1) \Rightarrow 2) Consideremos una cadena creciente

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$

de submódulos de M . Como $N = \bigcup_i M_i$ es finitamente generado, existe $n \in \mathbb{N}$ tal que $M_n = N$. En consecuencia $M_n = M_{n+i}$ para todo $i \in \mathbb{N}$.

2) \Rightarrow 3) Supongamos, por el contrario, que existe una familia $(M_i)_{i \in I}$ no vacía de submódulos de M que no tiene elemento maximal. Afirmamos que hay una sucesión i_1, i_2, i_3, \dots de elementos de I tal que

$$M_{i_1} \subsetneq M_{i_2} \subsetneq M_{i_3} \subsetneq \dots$$

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 $N' = N$. \square

TEOREMA 8.2. *Para cada submódulo N de M son equivalentes:*

1. M es noetheriano.
2. N y M/N son noetherianos.

DEMOSTRACIÓN. Es claro que si M es noetheriano, entonces todos los submódulos de N son finitamente generados. También lo es cada submódulo L de M/N , porque $L = \pi(\pi^{-1}(L))$, donde $\pi: M \rightarrow M/N$ 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

$$M' \cap N \quad \text{y} \quad \frac{M'}{M' \cap N} \simeq \frac{M' + N}{N}$$

son finitamente generados. Pero entonces, por el ítem 2) de la Proposición 6.24, también lo es M' . \square

COROLARIO 8.3. *Una suma directa de A -módulos $M_1 \oplus \cdots \oplus M_n$ es noetheriana si y sólo si cada M_i lo es.*

DEMOSTRACIÓN. Por inducción en n usando el teorema anterior. \square

PROPOSICIÓN 8.4. *Todo A -módulo noetheriano M es hopfiano.*

DEMOSTRACIÓN. Si $f: M \rightarrow M$ 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. \square

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 8.5. *Todo cociente de un anillo noetheriano a izquierda es noetheriano a izquierda.*

TEOREMA 8.6 (de la base de Hilbert). *Si un anillo A es noetheriano a izquierda, entonces también lo es el anillo de polinomios $A[X]$.*

DEMOSTRACIÓN. Supongamos que en $A[X]$ hay un ideal a izquierda I que no es finitamente generado. Definimos una sucesión de polinomios P_1, P_2, \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 $J := \sum_{j \geq 1} Aa_j$ de A , es finitamente

generado. Así, existe $m \in \mathbb{N}$ tal que $J = \sum_{j=1}^m Aa_j$. Escribamos $a_{m+1} = u_1a_1 + \dots + u_ma_m$. Como el grado de P_{m+1} no es menor que el de ninguno de los polinomios P_1, \dots, P_m ,

$$P := u_1X^{\text{gr}(P_{m+1})-\text{gr}(P_1)}P_1 + \dots + u_mX^{\text{gr}(P_{m+1})-\text{gr}(P_m)}P_m \in \sum_{j=1}^m A[X]P_j.$$

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 $\text{gr}(P_{m+1} - P) < \text{gr}(P_{m+1})$, esto contradice la elección de P_{m+1} . \square

COROLARIO 8.7. *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 8.5. \square

PROPOSICIÓN 8.8. *Si A es noetheriano a izquierda y M es un A -módulo finitamente generado, entonces M es noetheriano.*

DEMOSTRACIÓN. Por el Corolario 8.3, todo módulo libre finitamente generado es noetheriano a izquierda. El resultado se sigue ahora del Teorema 8.2, ya que al ser finitamente generado, M es un cociente de un módulo libre, que también lo es. \square

COROLARIO 8.9. *Todo anillo noetheriano a izquierda o a derecha satisface la ICB.*

DEMOSTRACIÓN. Por el ítem 1) de la Proposición 7.10 basta probarlo para anillos noetherianos a izquierda, y para estos vale por la Proposiciones 7.11, 8.4 y 8.8 \square

COROLARIO 8.10. *Los anillos de división satisfacen la ICB.*

PROPOSICIÓN 8.11. *Consideremos submódulos M_1, \dots, M_n de M . Son equivalentes:*

1. M_i es noetheriano para todo i .
2. $M_1 + \dots + M_n$ es noetheriano.

DEMOSTRACIÓN. Veamos primero que el segundo ítem es una consecuencia del primero. Por el Corolario 8.3, la suma directa $M_1 \oplus \dots \oplus M_n$ es noetheriana. En consecuencia, por el Teorema 8.2, el módulo $M_1 + \dots + M_n$ es noetheriano, debido a que es un cociente de $M_1 \oplus \dots \oplus M_n$. La recíproca se sigue inmediatamente del mismo teorema. \square

COROLARIO 8.12. *Consideremos submódulos M_1, \dots, M_n de M . Son equivalentes:*

1. Todos los cocientes M/M_i son noetherianos.
2. $\frac{M}{M_1 \cap \dots \cap M_n}$ es noetheriano.

DEMOSTRACIÓN. Supongamos que cada cociente M/M_i es noetheriano. Entonces, por el Corolario 8.3, también lo es $\bigoplus_{i=1}^n M/M_i$. Como las proyecciones canónicas $M \rightarrow M/M_i$ inducen un morfismo inyectivo

$$\frac{M}{M_1 \cap \dots \cap M_n} \longrightarrow \bigoplus_{i=1}^n \frac{M}{M_i},$$

se sigue del Teorema 8.2 que $\frac{M}{M_1 \cap \dots \cap M_n}$ es noetheriano. La recíproca es consecuencia inmediata del mismo teorema, porque cada M/M_i es un cociente de $\frac{M}{M_1 \cap \dots \cap M_n}$. \square

2. Módulos artinianos

En esta subsección introducimos los módulos artinianos y estudiamos algunas de sus propiedades básicas.

PROPOSICIÓN 8.13. *Son equivalentes:*

1. *Toda sucesión decreciente $M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$ 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

$$M_{i_1} \supsetneq M_{i_2} \supsetneq M_{i_3} \supsetneq \dots$$

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

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$$

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 $i \in \mathbb{N}$. \square

TEOREMA 8.14. *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

$$L_1 \supseteq L_2 \supseteq L_3 \supseteq \dots$$

de submódulos de M/N , porque $L_i = \pi(\pi^{-1}(L_i))$ para cada i , donde $\pi: M \rightarrow M/N$ es la proyección canónica, y

$$\pi^{-1}(L_1) \supseteq \pi^{-1}(L_2) \supseteq \pi^{-1}(L_3) \supseteq \dots$$

es estacionaria por hipótesis. Así, 1) implica 2). Para probar que vale la recíproca consideremos una sucesión decreciente

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$$

de submódulos de M . Por hipótesis existe $n \in \mathbb{N}$ tal que

$$M_i \cap N = M_n \cap N \quad \text{y} \quad \pi(M_i) = \pi(M_n)$$

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 ítem 2) de la Proposición 1.41 del Capítulo 1. \square

COROLARIO 8.15. *Una suma directa de A -módulos $M_1 \oplus \dots \oplus M_n$ es artiniana si y sólo si cada M_i lo es.*

DEMOSTRACIÓN. Por inducción en n , usando el teorema anterior. \square

Diremos que un A -módulo es *cohopfiano* si todo endomorfismo inyectivo $f: M \rightarrow M$ es un isomorfismo.

PROPOSICIÓN 8.16. *Todo A -módulo artiniano M es cohopfiano.*

DEMOSTRACIÓN. Si $f: M \rightarrow M$ es un morfismo inyectivo que no es sobrectivo, entonces

$$M \supsetneq f(M) \supsetneq f^2(M) \supsetneq f^3(M) \supsetneq \dots$$

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. \square

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 8.17. *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 8.18. *Todo anillo finito es artiniano.*

EJEMPLO 8.19. *Todo anillo que es un espacio vectorial de dimensión finita sobre un subanillo de división, es artiniano (por ejemplo, si A es un anillo de división y S es un monoide finito, entonces $A[S]$ es artiniano).*

PROPOSICIÓN 8.20. *Si A es artiniano a izquierda y M es un A -módulo finitamente generado, entonces M es artiniano.*

DEMOSTRACIÓN. Por el Corolario 8.15, todo módulo libre finitamente generado es artiniano a izquierda. El resultado se sigue ahora del Teorema 8.14, ya que al ser finitamente generado, M es un cociente de un módulo libre con base finita. \square

COROLARIO 8.21. *Consideremos submódulos M_1, \dots, M_n de M . Son equivalentes:*

1. M_i es artiniano para todo i .
2. $M_1 + \dots + M_n$ es artiniano.

DEMOSTRACIÓN. Veamos primero que el segundo item es consecuencia del primero. Por el Corolario 8.15, la suma directa $M_1 \oplus \dots \oplus M_n$ es artiniana. Así, por el Teorema 8.14, el módulo $M_1 + \dots + M_n$ es artiniano, debido a que es un cociente de $M_1 \oplus \dots \oplus M_n$. La recíproca es una consecuencia inmediata del mismo teorema. \square

PROPOSICIÓN 8.22. *Consideremos submódulos M_1, \dots, M_n de M . Son equivalentes:*

1. Todos los cocientes M/M_i son artinianos.
2. $\frac{M}{M_1 \cap \dots \cap M_n}$ es artiniano.

DEMOSTRACIÓN. Supongamos que cada cociente M/M_i es artiniiano. Entonces, por el Corolario 8.15, también lo es $\bigoplus_{i=1}^n M/M_i$. Como las proyecciones canónicas $M \rightarrow M/M_i$ inducen un morfismo inyectivo

$$\frac{M}{M_1 \cap \cdots \cap M_n} \longrightarrow \bigoplus_{i=1}^n \frac{M}{M_i},$$

del Teorema 8.14 se sigue que $\frac{M}{M_1 \cap \cdots \cap M_n}$ es artiniiano. 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

El anillo \mathbb{Z} es un ejemplo de grupo abeliano que es noetheriano y no artiniiano. También hay grupos abelianos que son artinianos y no noetherianos. Por ejemplo para cada primo $p \in \mathbb{N}$, el grupo

$$\mathbb{Z}_{p^\infty} := \frac{\{a/p^n : a \in \mathbb{Z} \text{ y } n \in \mathbb{N}\}}{\mathbb{Z}}$$

lo es. Para ver que esto es así será suficiente probar que si I es un subgrupo propio de \mathbb{Z}_{p^∞} , entonces $I = \langle [1/p^n] \rangle$, donde $n \in \mathbb{N}_0$ es el máximo entero no negativo tal que $[1/p^n] \in I$. Tomemos para ello $[a/p^m] \in I$ con a coprimo con p y escribamos $1 = ra + sp^m$ con r y s enteros. Entonces,

$$[1/p^m] = [(ra + sp^m)/p^m] = r[a/p^m] \in I.$$

En consecuencia $m \leq n$ y, por lo tanto, $[a/p^m] = ap^{n-m}[1/p^n] \in \langle [1/p^n] \rangle$.

3. Módulos de longitud finita

Ahora vamos a estudiar los módulos que son simultaneamente noetherianos y artinianos. Decimos que dos cadenas crecientes finitas

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_m \quad \text{y} \quad N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq N_n,$$

de submódulos de un A -módulo M , son *equivalentes* si $m=n$ y existe una permutación $\sigma \in S_m$ tal que

$$\frac{M_i}{M_{i-1}} \simeq \frac{N_{\sigma(i)}}{N_{\sigma(i)-1}} \quad \text{para todo } i \text{ entre } 1 \text{ y } m;$$

y decimos que la primera *refina* a la segunda si existen índices $1 \leq i_1 < \cdots < i_n \leq m$, tales que $M_{i_j} = N_j$ para todo j .

LEMA 8.23 (Lema de la Mariposa). *Dados submódulos $N_1 \subseteq N_2$ y $M_1 \subseteq M_2$ de M , existen isomorfismos canónicos*

$$\frac{N_1 + (N_2 \cap M_2)}{N_1 + (N_2 \cap M_1)} \simeq \frac{N_2 \cap M_2}{(N_1 \cap M_2) + (N_2 \cap M_1)} \simeq \frac{M_1 + (N_2 \cap M_2)}{M_1 + (N_1 \cap M_2)}.$$

DEMOSTRACIÓN. El primer isomorfismo se obtiene aplicando el isomorfismo $\frac{L}{L \cap K} \simeq \frac{L+K}{K}$ con $L = N_2 \cap M_2$ y $K = N_1 + (N_2 \cap M_1)$ y usando la modularidad del reticulado de submódulos de M . El segundo sale por simetría. \square

TEOREMA 8.24 (Schreier). *Dos cadenas finitas de submódulos de M siempre se pueden refinar a cadenas equivalentes.*

DEMOSTRACIÓN. Consideremos dos cadenas finitas

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_m \quad \text{y} \quad N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq N_n$$

de submódulos de M . Sin pérdida de generalidad podemos suponer que $M_0 = N_0 = 0$ y $M_m = N_n = M$. Escribamos

$$M_{ij} = M_{j-1} + (N_i \cap M_j) \quad \text{y} \quad N_{ij} = N_{i-1} + (N_i \cap M_j),$$

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

$$\frac{M_{ij}}{M_{i-1,j}} \simeq \frac{N_{ij}}{N_{i,j-1}} \quad \text{para } 1 \leq i \leq n \text{ y } 1 \leq j \leq m.$$

El resultado es consecuencia inmediata de esto. □

Una cadena $0 = M_0 \subseteq \cdots \subseteq M_n = M$ de submódulos de M es una *serie de composición de longitud n* de M si cada cociente M_i/M_{i-1} es simple.

TEOREMA 8.25 (Jordan-Hölder). *Si M tiene una serie de composición, entonces cada cadena estrictamente creciente de submódulos de M se puede refinar a una serie de composición. Además todas las series de composición de M son equivalentes y, en particular, tienen la misma longitud.*

DEMOSTRACIÓN. Es un corolario inmediato del teorema de Schreier. □

Definimos la *longitud* $\ell(M)$ de un A -módulo M , por

$$\ell(M) := \begin{cases} 0 & \text{si } M = 0, \\ n & \text{si } M \text{ tiene una serie de composición de longitud } n, \\ \infty & \text{en otro caso.} \end{cases}$$

Por el teorema de Jordan Hölder, esta definición no es ambigua.

TEOREMA 8.26. *Consideremos un submódulo N de un A -módulo M . Entonces M tiene una serie de composición si y sólo si N y M/N la tienen. Además $\ell(M) = \ell(N) + \ell(M/N)$.*

DEMOSTRACIÓN. Evidentemente podemos suponer que N es un submódulo no trivial de M . Es claro que si M tiene una serie de composición, entonces refinando la cadena $0 \subseteq N \subseteq M$ a una serie de composición

$$(44) \quad 0 = N_0 \subseteq \cdots \subseteq N_i = N \subseteq \cdots \subseteq N_m = M,$$

obtenemos series de composición

$$(45) \quad 0 = N_0 \subseteq \cdots \subseteq N_i = N \quad \text{y} \quad 0 = \frac{N_i}{N} \subseteq \cdots \subseteq \frac{N_m}{N} = \frac{M}{N},$$

de N y M/N , respectivamente. Notemos que además

$$\ell(M) = m = i + (m - i) = \ell(N) + \ell(M/N).$$

Recíprocamente, si M tiene un submódulo N tal que N y M/N tienen series de composición como (45), combinándolas se obtiene una serie de composición como (44). \square

TEOREMA 8.27 (Teorema de la dimensión). *Dos submódulos M_1 y M_2 de M tienen longitud finita si y sólo si su suma e intersección la tienen. Además*

$$\ell(M_1 + M_2) + \ell(M_1 \cap M_2) = \ell(M_1) + \ell(M_2).$$

DEMOSTRACIÓN. Basta aplicar el teorema anterior a los submódulos y módulos cocientes que aparecen en las sucesiones exactas cortas

$$0 \longrightarrow M_1 \cap M_2 \longrightarrow M_1 \longrightarrow \frac{M_1}{M_1 \cap M_2} \longrightarrow 0$$

y

$$0 \longrightarrow M_2 \longrightarrow M_1 + M_2 \longrightarrow \frac{M_1 + M_2}{M_2} \longrightarrow 0,$$

y usar que $\frac{M_1}{M_1 \cap M_2} \simeq \frac{M_1 + M_2}{M_2}$. \square

PROPOSICIÓN 8.28. *Un A -módulo M tiene una serie de composición si y sólo si es noetheriano y artiniiano.*

DEMOSTRACIÓN. Supongamos que M tiene longitud finita. Dado que toda cadena estrictamente creciente o estrictamente decreciente de submódulos de M tiene a lo sumo $\ell(M) + 1$ componentes, es inmediato que M es noetheriano y artiniiano. Supongamos ahora que M es noetheriano y artiniiano. 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 . \square

Capítulo 9

Módulos sobre dominios principales

Recordemos que A es un dominio principal si es un dominio conmutativo y todo ideal de A es cíclico y que todo dominio principal es de factorización única. Una consecuencia particular de esto es que los primos no nulos de A coinciden con los irreducibles.

1. Módulos libres

En toda esta sección A denota a un dominio principal.

TEOREMA 9.1. *Todo submódulo de un A -módulo libre es libre.*

DEMOSTRACIÓN. Supongamos que L es un A -módulo libre y que M es un submódulo de L . Fijemos una base bien ordenada $\mathcal{B} = (v_i)_{i \in I}$ de L y, para cada $i \in I$, consideremos los submódulos

$$L_i := \bigoplus_{j < i} \langle v_j \rangle, \quad \bar{L}_i := \bigoplus_{j \leq i} \langle v_j \rangle, \quad M_i = M \cap L_i \quad \text{y} \quad \bar{M}_i = M \cap \bar{L}_i,$$

de L . Notemos que $\bar{L}_i = L_i \oplus \langle v_i \rangle$ y que cada $m \in \bar{M}_i$ tiene una escritura única

$$m = m_i + \lambda_m \cdot v_i, \quad \text{con } m_i \in M_i \text{ y } \lambda_m \in A.$$

Es evidente que la fórmula $g_i(m) := \lambda_m$ define una aplicación A -lineal $g_i: \bar{M}_i \rightarrow A$. 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 $M_i = \bar{M}_i$ o no). En ambos casos la sucesión exacta corta

$$0 \longrightarrow M_i \xrightarrow{\iota} \bar{M}_i \xrightarrow{g_i} \text{Im}(g_i) \longrightarrow 0,$$

donde ι es la inclusión canónica, es escindida y, por lo tanto, existe un submódulo M'_i de \bar{M}_i , tal que $\bar{M}_i = M_i \oplus M'_i$ y $M'_i \simeq \text{Im}(g_i)$. Afirmamos que $\sum_{i \in I} M'_i$ es directa y que $M = \bigoplus_{i \in I} M'_i$. Veamos primero que la suma es directa. Para ello escribimos

$$0 = m_{i_1} + \cdots + m_{i_r}, \quad \text{con } r \geq 1, m_{i_h} \in M'_{i_h} \text{ e } i_1 < i_2 < \cdots < i_r,$$

y procedemos por inducción en r . Es claro que si $r = 1$, entonces $m_{i_1} = 0$. Supongamos ahora que $r > 1$. Como

$$m_{i_1} + \cdots + m_{i_{r-1}} \in M_{i_r} \quad \text{y} \quad \overline{M}_{i_r} = M_{i_r} \oplus M'_{i_r},$$

debe ser $m_{i_r} = 0$ y, a posteriori, $m_{i_1} = \cdots = m_{i_{r-1}} = 0$. Veamos a continuación que

$$M = \bigoplus_{i \in I} M'_i.$$

Es evidente que $\bigoplus_{i \in I} M'_i \subseteq M$. Supongamos que la inclusión recíproca no vale y tomemos $m \in M \setminus \bigoplus_{i \in I} M'_i$ con $i(m)$ mínimo, donde para cada $m \in M \setminus \{0\}$, denotamos con $i(m)$ al menor de los $i \in I$ tal que $m \in \overline{L}_i$. Como

$$m \in \overline{L}_{i(m)} \cap M = \overline{M}_{i(m)} = M_{i(m)} \oplus M'_{i(m)},$$

existen $m' \in M_{i(m)}$ y $m'' \in M'_{i(m)}$ tales que $m = m' + m''$. Como, debido a la minimalidad de $i(m)$,

$$m' \in \bigoplus_{i \in I} M'_i,$$

también

$$m = m' + m'' \in \bigoplus_{i \in I} M'_i,$$

contradiciendo la suposición hecha arriba. Por lo tanto, M es la suma directa de los M'_i , como queremos. \square

COROLARIO 9.2. *Todo A -módulo finitamente generado sin torsión es libre.*

DEMOSTRACIÓN. Es consecuencia inmediata de los Teoremas 7.26 y 9.1. \square

COROLARIO 9.3. *Para todo A -módulo finitamente generado M existe $n \in \mathbb{N}_0$ tal que*

$$(46) \quad M = T(M) \oplus \frac{M}{T(M)} \simeq T(M) \oplus A^{(n)}.$$

Además n no depende del isomorfismo elegido.

DEMOSTRACIÓN. Basta observar que la sucesión exacta corta

$$0 \longrightarrow T(M) \xrightarrow{\iota} M \xrightarrow{p} M/T(M) \longrightarrow 0,$$

se parte porque, por el corolario anterior existe $n \in \mathbb{N}_0$ tal que $M/T(M) \simeq A^{(n)}$. La unicidad de n se sigue de que el isomorfismo que aparece en (46) induce un isomorfismo

$$\frac{M}{T(M)} \simeq \frac{T(M) \oplus A^{(n)}}{T(T(M) \oplus A^{(n)})} = \frac{T(M) \oplus A^{(n)}}{T(M)} \simeq A^{(n)}$$

y de que todo anillo conmutativo satisface la ICB. \square

2. Módulos de torsión

Consideremos un dominio principal A y un elemento irreducible $p \in A \setminus \{0\}$. Un A -módulo M es p -primario si para todo $m \in M$ existe $n \in \mathbb{N}$ tal que $p^n \cdot m = 0$. Para cada A -módulo M , el conjunto

$$M_p := \{m \in M : p^n \cdot m = 0 \text{ para algún } n \in \mathbb{N}\}$$

es un submódulo p -primario de M , llamado *la componente p -primaria de M* .

OBSERVACIÓN 9.4. Para todo morfismo de A -módulos $f: M \rightarrow N$ y cada primo $p \in A$ no nulo, $f(M_p) \subseteq N_p$. En efecto esto se sigue de que si $p^n \cdot m = 0$, entonces

$$p^n \cdot f(m) = f(p^n \cdot m) = f(0) = 0.$$

TEOREMA 9.5. 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,

$$m_s = ap_1^{h_1} \cdots p_{s-1}^{h_{s-1}} \cdot m_s + bp_s^{h_s} \cdot m_s = 0.$$

Ahora $m_1 = \cdots = m_{s-1} = 0$, por hipótesis inductiva. □

TEOREMA 9.6. Si $M \neq 0$ es un A -módulo p -primario y existe $r \in \mathbb{N}$ tal que $p^r M = 0$, entonces M es suma directa de módulos cíclicos.

DEMOSTRACIÓN. Denotemos con V a M/pM y consideremos las filtraciones

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots \quad \text{y} \quad V_0 \subseteq V_1 \subseteq V_2 \subseteq V_3 \subseteq \dots$$

de M y V respectivamente definidas por

$$M_i := \{m \in M : p^i \cdot m = 0\} \quad \text{y} \quad V_i := \frac{M_i + pM}{pM}.$$

Es evidente que $M = \bigcup M_i$ y $V = \bigcup V_i$. Tomemos una base S de V tal que $S \cap V_i$ es una base de V_i y para cada $s \in S$ denotemos con $i(s)$ al mínimo i tal que $s \in V_i$ y elijamos un representante s' de s en $M_{i(s)}$ (es decir elijamos $s' \in M_{i(s)}$ tal que $\pi(s') = s$). Definamos

$$\varphi: \bigoplus_{s \in S} \frac{A}{p^{i(s)}A} \longrightarrow M$$

por

$$\varphi((a_s)_{s \in S}) := \sum_{s \in S} a_s \cdot s'.$$

Es fácil comprobar que φ está bien definido y que es un morfismo de A -módulos. Así, para terminar la demostración, sólo debemos ver que también es biyectivo. Veamos primero que si $\varphi((a_s)_{s \in S}) = 0$, entonces $a_s = 0$ para todo $s \in S$. Claramente para esto es suficiente probar que

$$(47) \quad a_s \in \frac{p^i A}{p^{i(s)}A} \quad \text{para todo } s \in S \text{ y todo } i \in \mathbb{N}_0.$$

Procedemos por inducción en i . Para $i = 0$ no hay nada que probar. Supongamos ahora que (47) vale para $i = k$ con $k \in \mathbb{N}_0$ fijo. Entonces

$$\sum_{\substack{s \in S \\ i(s) \geq k+1}} a_s \cdot s' = \sum_{s \in S} a_s \cdot s' = 0,$$

pues de (47) se sigue que $a_s = 0$ para todo s tal que $i(s) \leq k$. Para cada $s \in S$ tal que $i(s) \geq k + 1$ elijamos $a'_s \in A/p^{i(s)}A$ tal que $a_s = p^k a'_s$. Claramente

$$p^k \sum_{\substack{s \in S \\ i(s) \geq k+1}} a'_s \cdot s' = \sum_{\substack{s \in S \\ i(s) \geq k+1}} p^k a'_s \cdot s' = \sum_{\substack{s \in S \\ i(s) \geq k+1}} a_s \cdot s' = 0,$$

lo cual implica que

$$\sum_{\substack{s \in S \\ i(s) \geq k+1}} a'_s \cdot s' \in M_k.$$

Considerando la imagen de esta igualdad en V obtenemos que

$$\sum_{\substack{s \in S \\ i(s) \geq k+1}} a'_s \cdot s \in V_k,$$

de donde $a'_s \equiv 0 \pmod{p}$ para todo $s \in S$ tal que $i(s) \geq k + 1$. En consecuencia

$$a_s = p^k a'_s \in p^{k+1}A \quad \text{para todo } s \in S \text{ tal que } i(s) \geq k + 1,$$

como queremos. Resta ver que φ es sobreyectivo. Afirmamos que

$$(48) \quad M = \text{Im } \varphi + p^i M \quad \text{para todo } i \in \mathbb{N}.$$

En efecto para $i = 1$ esto se sigue de que la imagen en V de $\text{Im } \varphi$ coincide con V . Supongamos ahora que la igualdad (48) vale para $i = k$ con $k \in \mathbb{N}$ fijo. Entonces

$$M = \text{Im } \varphi + pM = \text{Im } \varphi + p(\text{Im } \varphi + p^i M) = \text{Im } \varphi + p \text{Im } \varphi + p^{i+1} M = \text{Im } \varphi + p^{i+1} M,$$

como queremos. Como $p^r M = 0$ se sigue de la igualdad (48) para $i := r$ que $M = \text{Im } \varphi$. \square

OBSERVACIÓN 9.7. *Supongamos que $M \neq 0$ es un A -módulo p -primario y finitamente generado donde p es un primo no nulo de A y que $r \in \mathbb{N}$ es el mínimo natural tal que $p^r M = 0$. El teorema anterior dice que existen $n_1, \dots, n_r \in \mathbb{N}_0$ con $n_r > 0$ tales que*

$$(49) \quad M \simeq \bigoplus_{j=1}^r \left(\frac{A}{Ap^j} \right)^{(n_j)}.$$

Afirmamos que los n_i 's no dependen del isomorfismo (49). Probaremos esto por inducción en r . Cuando $r = 1$ el resultado es evidente pues en este caso n_1 es la dimensión de M como $\frac{A}{(p)}$ -espacio vectorial. Supongamos ahora que $r > 1$ y que el resultado vale para $r-1$. Dado que

$$(50) \quad pM \simeq \bigoplus_{j=1}^r \left(\frac{Ap}{Ap^j} \right)^{(n_j)} \simeq \bigoplus_{j=2}^r \left(\frac{A}{Ap^{j-1}} \right)^{(n_j)} \quad \text{y} \quad \frac{M}{pM} \simeq \left(\frac{A}{Ap^j} \right)^{(n_1 + \dots + n_r)},$$

se sigue de la hipótesis inductiva que los $|n_j|$ no dependen del isomorfismo (49).

3. Teoremas de estructura

En lo que sigue A es un dominio principal y \mathcal{P} es una familia de representantes de las clases de equivalencia de los irreducibles de A , módulo asociados.

TEOREMA 9.8. *Para todo módulo finitamente generado M hay un isomorfismo*

$$f: M \longrightarrow A^{(n)} \oplus \bigoplus_{p \in \mathcal{P}'} \bigoplus_{j=1}^{r_p} \left(\frac{A}{Ap^j} \right)^{(n_{pj})}$$

donde \mathcal{P}' es un subconjunto finito de \mathcal{P} , n y los n_{pj} son enteros no negativos que no dependen del isomorfismo f y $n_{pr_p} > 0$ para todo $p \in \mathcal{P}'$.

DEMOSTRACIÓN. La existencia de f se sigue del Corolario 9.3 y de los Teoremas 9.5 y 9.6. Por otro lado del Corolario 9.3 se sigue también que n no depende de f . Para ver que los n_{pj} tampoco lo hacen basta notar que, por la Observación 9.4, para cada $p \in \mathcal{P}'$ el morfismo f induce un isomorfismo

$$f_p: M_p \longrightarrow \bigoplus_{j=1}^{r_p} \left(\frac{A}{Ap^j} \right)^{(n_{pj})}$$

y aplicar la Observación 9.7. \square