ÁLGEBRA

Grupos, Anillos y Módulos

Jorge Alberto Guccione

y

Juan José Guccione

Índice general

Parte 1

Grupos

Capítulo 1

Teoría elemental

1. Monoides

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DEMOSTRACIÓN. Como S es finito,

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

Por dualidad,

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

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

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

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

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

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

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

Dejamos como ejercicio probar que

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Submonoides

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

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

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

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

Proposición 1.8. *Si K y L son submonoides de S, entonces KL es un submonoide de S si y sólo si $LK \subseteq KL$.*

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

$$KLKL \subseteq KKLL = KL.$$

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

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

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

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

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

2.1. Ejemplos

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

3. Morfismos de monoides

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

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

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

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

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

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

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

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

Son ejemplos de morfismos de monoides

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

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

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

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

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

Como

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

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

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

Ejemplo 1.9. *Supongamos que X es un subconjunto de Y. Definamos*

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

por

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

Es evidente que i es un morfismo inyectivo de monoides.

Ejemplo 1.10. *Supongamos que $i\colon X \to Y$ es una biyección. Definamos*

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

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

Ejemplo 1.11. *Supongamos que $i\colon X \to Y$ es una función inyectiva. Definamos*

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

por

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

Es fácil ver que:

- *i_* es un morfismo inyectivo de monoides cuya imagen es el conjunto de las funciones de Y en si mismo que dejan fijos a los elementos que están fuera de $i(X)$.*
- *Si X es un subconjunto de Y e i es la inclusión canónica de X en Y recuperamos la definición dada en el Ejemplo 1.9, mientras que si i es una biyección recuperamos la dada en el Ejemplo 1.10.*
- *Si $j\colon Y \to Z$ es otra función inyectiva, entonces $(j \circ i)_* = j_* \circ i_*$.*

4. Grupos

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

Proposición 1.12. *Un monoide G es un grupo si y sólo si para cada par g, h de elementos de G, las ecuaciones $gx = h$ y $xg = h$ tienen solución única en G.*

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

Proposición 1.13. *Un semigrupo G es un grupo si y sólo si tiene un neutro a izquierda e, y para cada $g \in G$ hay un $g' \in G$ tal que $g'g = e$.*

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

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

y

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

para todo $g \in G$. □

Nota 1.14. *También se puede probar que e es neutro de G de la siguiente manera: Tomemos $g \in G$ arbitrario. Entonces*

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

Cancelando g' (lo que puede hacerse por el Ejercicio 1.3) obtenemos que $ge = g$.

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

Ejemplo 1.16. *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 1.17. *Consideremos un k-espacio vectorial V. El* grupo lineal general $\mathrm{GL}(V)$ *es el grupo de unidades del anillo de endomorfismos $\mathrm{End}_k(V)$. Este grupo es abeliano si y sólo si $\dim_k(V) = 1$.*

Ejemplo 1.18. *El grupo $\mathrm{GL}(n, k)$ es el grupo de unidades del anillo $\mathrm{M}_n(k)$, de matrices de $n \times n$ con coeficiente en un cuerpo k. Este grupo es abeliano si y sólo si $n = 1$.*

Ejemplo 1.19. *Una* permutación *de un conjunto no vacío X es una función biyectiva $\varphi\colon X \to X$. El conjunto S_X, de las permutaciones de X, es un grupo vía la operación dada por la composición de funciones. Notemos que S_X es el grupo de unidades de $\mathrm{Fun}(X, X)$. Cuando $|X| \geq 3$ este grupo no es conmutativo. Para comprobarlo es suficiente considerar $x_1, x_2, x_3 \in X$ y exhibir dos permutaciones σ y τ de X que se restringen a la identidad sobre $X \setminus \{x_1, x_2, x_3\}$ y no conmutan. Por ejemplo, podemos tomar*

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

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

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

EJERCICIO 1.20. *Pruebe que si un grupo G tiene exponente 2, entonces es abeliano.*

5. Subgrupos

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

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

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

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

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

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

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

EJERCICIO 1.21. *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 1.22. *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 1.23. *Los conjuntos $\mathbb{Q}_{>0}$ y $\mathbb{R}_{>0}$ son subgrupos de $\mathbb{Q}^\times$ y $\mathbb{R}^\times$, respectivamente*

EJEMPLO 1.24. *El conjunto $\mathbb{Z}[X]$, de polinomios con coeficientes enteros, es un subgrupo de $\mathbb{Q}[X]$.*

EJEMPLO 1.25. *Consideremos un espacio euclideano E. El* grupo ortogonal de E *es el subgrupo $\mathrm{O}(E)$ de $\mathrm{GL}(E)$, formado por las transformaciones ortogonales de E. El* grupo lineal especial $\mathrm{SO}(E)$ *es el subgrupo de $\mathrm{O}(E)$ formado por las transformaciones ortogonales que tienen determinante 1.*

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

EJEMPLO 1.27. *Para cada $n \in \mathbb{N}$, el subconjunto G_n de $\mathbb{C}$, formado por las raíces n-ésimas de la unidad, es un subgrupo de $\mathbb{C}^\times$. También lo es $\mathrm{G}_\infty := \bigcup_{n\in\mathbb{N}} \mathrm{G}_n$.*

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

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

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

EJEMPLO 1.28. *Consideremos el ángulo $\theta{:=}2\pi/n$, donde $n \in \mathbb{N}$ es mayor que 1. El subgrupo de $\mathrm{GL}(2,\mathbb{R})$ generado por*

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

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

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

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

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

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

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

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

EJEMPLO 1.29. *Tomemos* $w := e^{i\pi/n}$ *donde* $n \in \mathbb{N}$ *es mayor que* 1. *Es claro que* $w \in \mathbb{C}$ *es una raíz de la unidad de orden* $2n$. *El subgrupo de* $\mathrm{GL}(2,\mathbb{C})$ *generado por*

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

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

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

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

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

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

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

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

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

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

5.1. Subgrupos de un grupo cíclico

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

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

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

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

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

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

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

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

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

NOTA 1.30. *La función $\tau\colon \mathbb{N} \to \mathbb{N}$ satisface la siguiente propiedad: Si $n = p_1^{r_1} \dots p_s^{r_s}$ es la factorización de n como producto de primos positivos distintos, entonces*

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

5.2. Subgrupos de los grupos diedrales y cuaterniónicos

A continuación calculamos los subgrupos de D_n y H_n. Usaremos libremente las notaciones introducidas en los Ejemplos 1.28 y 1.29. Consideremos primero un subgrupo H de D_n. Si $H \subseteq \langle x\rangle$, entonces $H = \langle x^i\rangle$, donde i es un divisor de n. Supongamos ahora que $H \nsubseteq \langle x\rangle$ y que j es el mínimo entero no negativo tal que $x^j y \in H$. Denotemos con i al único divisor positivo de n tal que $H \cap \langle x\rangle = \langle x^i\rangle$. Claramente

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

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

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

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

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

NOTA 1.31. *La función $\sigma\colon \mathbb{N} \to \mathbb{N}$ satisface la siguiente propiedad: Si $n = p_1^{r_1} \dots p_s^{r_s}$ es la factorización de n como producto de primos positivos distintos, entonces*

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

6. Una caracterización de los grupos cíclicos finitos

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

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

LEMA 1.32. *Cada grupo G es la unión disjunta*

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

de los generadores de los subgrupos cíclicos C de G.

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

PROPOSICIÓN 1.33. *La igualdad $n = \sum_{d/n} \phi(d)$ vale para cada $n \in \mathbb{N}$.*

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

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

como queríamos. □

TEOREMA 1.34. *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 1.32 y la Proposición 1.33,

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

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

TEOREMA 1.35. *Si F es un cuerpo y G es un subgrupo finito de $F^\times$, entonces G es cíclico.*

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

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

LEMA 1.36. *Si $i \in \mathbb{N}$, $y, z \in \mathbb{Z}$ e $y \equiv z \pmod{p^i}$, entonces $y^p \equiv z^p \pmod{p^{i+1}}$.*

DEMOSTRACIÓN. Claramente

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

En consecuencia p^{2i} divide a

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

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

LEMA 1.37. *Si $p = 2$ e $i > 1$ o si p es un primo impar e $i \geq 1$, entonces*

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

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

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

En consecuencia para terminar la demostración será suficiente comprobar que

$$(1+p^i)^p \equiv 1 + p^{i+1} \pmod{p^{i+2}}. \tag{4}$$

Pero, como por la fórmula del binomio,

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

la congruencia (4) se sigue de que

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

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

TEOREMA 1.38. *Si p es un primo impar, entonces el grupo de unidades del anillo de congruencias $\mathbb{Z}_{p^r}$ es cíclico de orden $(p-1)p^{r-1}$, para todo $r \in \mathbb{N}$. En cambio, $\mathbb{Z}_{2^r}^\times$ es cíclico de orden 2^{r-1} si $r \leq 2$, e isomorfo a $\mathbb{Z}_{2^{r-2}} \oplus \mathbb{Z}_2$ si $r \geq 3$. Además, en este caso*

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

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

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

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

Probaremos esto por inducción en i. El caso $i = 0$ es trivial. Supongamos que la afirmación vale para i. Entonces por los Lemas 1.36 y 1.37,

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

como queremos. En particular, $1+p$ tiene orden p^{r-1} en $\mathbb{Z}_{p^r}^\times$. Debido a esto, para concluir la prueba de la primera afirmación será suficiente ver que existe $x \in \mathbb{Z}_{p^r}^\times$ de orden $p-1$, pues entonces $x(1+p)$ será un generador de $\mathbb{Z}_{p^r}^\times$. Pero si $z \in \mathbb{Z}_{p^r}$ es tal que $\pi(z)$ tiene orden $p-1$, donde $\pi\colon \mathbb{Z}_{p^r} \to \mathbb{Z}_p$ es la proyección canónica, entonces z es inversible (pues p no divide a z) y tiene orden $(p-1)p^i$ con $0 \le i < r$, con lo cual $x := z^{p^i}$ tiene orden $p-1$, como queremos. Consideremos ahora el caso $p = 2$. Es obvio que el grupo de unidades de $\mathbb{Z}_{2^r}$ es cíclico si $r = 2$. Supongamos entonces que $r > 2$. Como $5 = 1 + 2^2$, se sigue de los Lemas 1.36 y 1.37 (razonando por inducción en i como arriba), que

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

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

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

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

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

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

PROPOSICIÓN 1.39. *Si s tiene orden p–1 en $\mathbb{Z}_{p^2}^\times$, entonces s+p tiene orden $(p$–1$)p$ en $\mathbb{Z}_{p^2}^\times$.*

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

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

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

PROPOSICIÓN 1.40. *Tomemos un número natural $s < p^2$, coprimo con p, tal que el orden de s en $\mathbb{Z}_{p^2}^\times$ es $(p-1)p$. Entonces para todo $r \ge 2$, el orden de s en $\mathbb{Z}_{p^r}^\times$ es $(p-1)p^{r-1}$.*

DEMOSTRACIÓN. Es suficiente probar por inducción en i que

$$p^i \nmid s^{(p-1)p^{i-2}} - 1 \qquad \text{para todo } i \geq 2 \tag{5}$$

El caso $i = 2$ vale porque el orden de s en $\mathbb{Z}_{p^2}^{\times}$ es $(p-1)p$. Supongamos ahora que $i \geq 2$ y que (5) vale para i. Por el teorema de Euler-Fermat sabemos que

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

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

$$s^{(p-1)p^{i-1}} = (1 + kp^{i-1})^p \equiv 1 + kp^i \pmod{p^{i+1}}. \tag{6}$$

Dado que, debido a (5) sabemos que $p \nmid k$, se sigue de (6), que

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

como queremos. □

7. Coclases a izquierda y a derecha

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

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

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

TEOREMA 1.41 (Lagrange). *Para cada $H \leq G$, los ordenes de H y G están relacionados por la igualdad*

$$|G| = |G : H||H|, \tag{7}$$

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

El mismo razonamiento, aplicado a las coclases a derecha de H en G (las cuales son los subconjuntos de G de la forma Hg para algún $g \in G$) prueba que estas parten G y satisfacen una fórmula similar a (7). Más aún, como la aplicación $gH \mapsto Hg^{-1}$ (que está bien definida pues de $g_1H = g_2H$ se sigue que $Hg_1^{-1} = H^{-1}g_1^{-1} = (g_1H)^{-1} = (g_2H)^{-1} = H^{-1}g_2^{-1} = Hg_2^{-1}$) es una función biyectiva del conjunto G/H de las coclases a izquierda de H en G, en el conjunto $G\backslash H$ de las coclases a derecha H en G, ambos tienen el mismo cardinal.

EJERCICIO 1.42. *Calcule las coclases a izquierda y a derecha de $\langle y \rangle$ en D_n y muestre que en general no coinciden.*

EJERCICIO 1.43. *Calcule las coclases a izquierda y a derecha de $\langle y\rangle$ en H_n y muestre que en general no coinciden.*

OBSERVACIÓN 1.44. *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 1.45. *Si G es finito, entonces el exponente de G divide al orden de G.*

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

COROLARIO 1.46. *Si un grupo G tiene orden primo, entonces es cíclico.*

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

OBSERVACIÓN 1.47. *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 (7).

TEOREMA 1.48. *Si K y H son subgrupos de un grupo G y $K \subseteq H$, entonces*

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

DEMOSTRACIÓN. Escribamos G y H como uniones disjuntas

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

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

OBSERVACIÓN 1.49. *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 1.50. *Si la intersección de una familia $(g_i H_i)_{i\in I}$ de coclases a izquierda de un grupo G no es vacía, entonces es una coclase a izquierda de la intersección de los H_i's. En efecto, si $g \in \bigcap_{i\in I} g_i H_i$, entonces $gH_i = g_i H_i$ 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 1.51. *Consideremos dos subgrupos H y L de un grupo G. Dado que, para todo $h, h' \in H$,*

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

la aplicación

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

es inyectiva. Dado que además

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

se sigue de esto que

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

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

$$|H : H \cap L| \leq |G : L| \qquad y \qquad |G : H \cap L| \leq |G : H||G : L|, \tag{9}$$

con estas desigualdades convertidas en igualdades si $HL = G$. De la presente exposición se sigue que:

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

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

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

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

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

Ejercicio 1.53. *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 1.54. *Si $K \leq H$ y L son subgrupos de un grupo G, entonces*

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

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

2) Por el item 1) y las hipótesis,

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

como queríamos. □

Proposición 1.55. *Si H y L son subgrupos de un grupo G, entonces*

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

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

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

No hay duda de que $\{(hy, y^{-1}l) : y \in H \cap L\} \subseteq \varsigma^{-1}(g)$. Recíprocamente, si $(h', l') \in \varsigma^{-1}(g)$, entonces $h^{-1}h' = ll'^{-1} \in H \cap L$ y, así, $h' = hy$ y $l' = y^{-1}l$, con $y \in H \cap L$. □

Proposición 1.56. *Para cada par de subgrupos H y L de un grupo G son equivalentes:*

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

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

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

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

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

como queremos. □

8. Coclases dobles

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

$$|G : L| = \sum_{i \in I} |H : H \cap g_iLg_i^{-1}|. \tag{10}$$

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 1.55 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 (10) se reduce a la establecida en el teorema de Lagrange.

EJEMPLO 1.57. *Escribamos* $\mathrm{S}_3 = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$, *donde*

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

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

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

9. Subgrupos normales

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

PROPOSICIÓN 1.58. *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. □

EJEMPLO 1.59. *Recordemos que el grupo diedral D_n es el subgrupo de $\mathrm{GL}(2,\mathbb{R})$ generado por las matrices*

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

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

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

Lo primero es obvio y lo segundo se sigue de que

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

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

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

y, por lo tanto,

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

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

EJEMPLO 1.60. *Recordemos que el grupo cuaterniónico generalizado H_n es el subgrupo de $\mathrm{GL}(2,\mathbb{C})$ generado por las matrices*

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

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

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

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

EJERCICIO 1.61. *Pruebe que un subgrupo N de G es invariante si y sólo si $hg \in N$ siempre que $gh \in N$.*

OBSERVACIÓN 1.62. *Si $N \subseteq L$ son subgrupos de un grupo G y $N \lhd G$, entonces $N \lhd L$.*

OBSERVACIÓN 1.63. *Si $N \lhd G$, entonces $NL = LN$ para todo subconjunto L de G. Si además $L \le G$, entonces $NL \le G$. Por último, si $L \lhd G$, entonces $NL \lhd G$.*

El siguiente resultado será mejorado más adelante.

PROPOSICIÓN 1.64. *Todo subgrupo N de índice 2 de un grupo G es normal.*

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

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

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

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

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

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

PROPOSICIÓN 1.65. *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 1.63, sabemos que $G_iG_j = G_jG_i$ para todo $i, j \in I$. □