TEORÍA DE GRUPOS

1.Definición y Propiedades Básicas

1.1.Magmas. Una *operación binaria* definida en un conjunto A es una función $*\colon A \times A \to A$. Como es usual, dados $a, b \in A$, escribiremos $a*b$ en lugar de $*(a, b)$. Decimos que $*$ es *asociativa* si $a*(b*c) = (a*b)*c$, para todo $a, b, c \in A$ y que es *conmutativa* si $a*b = b*a$, para todo $a, b \in A$. Un *magma* es un conjunto A provisto de una operación interna. Usualmente hablaremos de un magma A, mencionando sólo al conjunto subyacente y no a la operación. Esto es ambiguo, porque un conjunto puede tener dos operaciones binarias distintas. Como ejemplo podemos considerar a la suma y al producto de los números enteros. Así que procuraremos ser claros cuando sea necesario. Un magma es *asociativo* o *conmutativo* o *abeliano* si lo es su operación y es finito si lo es su conjunto subyacente. En este caso llamamos *orden* $|A|$ de A a la cantidad de elementos de A. Un magma asociativo se denomina también *semigrupo*. El *magma opuesto* de un magma A es el magma A^{op}, que tiene el mismo conjunto subyacente, pero cuya operación $*_{\mathrm{op}}$, está definida por $a *_{\mathrm{op}} b = b * a$. Es inmediato que A es asociativo o conmutativo si y sólo si A^{op} lo es, y que A es conmutativo si y sólo si $A^{\mathrm{op}} = A$.

Para cada elemento a de un magma A denotamos con $l_a\colon A \to A$ y $r_a\colon A \to A$ a las funciones definidas por $l_a(b) = a * b$ y $r_a(b) = b * a$, respectivamente. Es claro que A es conmutativo si y sólo si $l_a = r_a$ para todo $a \in A$ y que A es asociativo si y sólo si $l_a \circ r_b = r_b \circ l_a$ para todo $a, b \in A$ y que esto a su vez ocurre si y sólo si $l_a \circ l_b = l_{a*b}$ para todo $a, b \in A$ y también si y sólo si $r_a \circ r_b = r_{b*a}$ para todo $a, b \in A$. Decimos que $a \in A$ es *cancelable a izquierda* si $a * b = a * c$ implica $b = c$ y que *cancelable a derecha* si $b * a = c * a$ implica $b = c$. Finalmente decimos que a es *cancelable* si lo es a izquierda y a derecha. Es facil ver que a es cancelable a izquierda (respectivamente a derecha) si y sólo si l_a (respectivamente r_a) es inyectiva. Notemos que a es cancelable a un lado en A si y sólo si lo es al otro en A^{op}. Muchas otras definiciones y propiedades predicables sobre elementos y subconjuntos de un magma A tienen una versión a izquierda y otra a derecha, de modo de que cada una de ellas en A es equivalente a la otra en A^{op}. Muchas veces, cuando una definición o resultado tenga una versión a izquierda y otra a derecha daremos una de ellas, dejando al lector la tarea de enunciar la otra. Comenzamos con las siguiente definición. Un elemento $e \in A$ es *neutro a izquierda* si $e * a = a$, para todo $a \in A$. Como para el caso de elementos cancelables decimos que e es *neutro* si lo es a izquierda y a derecha. Si un magma A 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, A tiene a lo sumo un neutro. Diremos que un magma es *unitario* si tiene neutro. Es claro que A es unitario si y sólo si A^{op} lo es.

1.2.Monoides. Un *monoide* es un semigrupo unitario. Es evidente que A es un monoide si y sólo A^{op} lo es. Un elemento a de un monoide A es *inversible a izquierda* si existe $b \in A$ tal que $b * a = e$. En este caso decimos también que b

es una *inversa a izquierda* de a. Finalmente decimos que a es *inversible*, si lo es a izquierda y a derecha. Es facil ver que a es inversible a izquierda (respectivamente derecha) si y sólo si r_a (respectivamente l_a) es sobreyectiva. Si a tiene inversa a izquierda y a derecha, entonces estas son únicas y coinciden. En efecto, supongamos que b y c son inversas a izquierda y a derecha de a, respectivamente. Entonces $b = b * e = b * (a * c) = (b * a) * c = e * c = c$. Esto nos autoriza a decir que b es el inverso de a y a denotarlo por a'.

No es costumbre usar un símbolo especial como $*$ para denotar una operación 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 $-a$ denotan respectivamente al elemento neutro de $*$ y al inverso de un elemento $a \in A$. En el segundo, estas funciones la cumplen los símbolos 1 y a^{-1}. La notación aditiva nunca se usa para designar operaciones que no son conmutativas, ya que es muy feo encontrar expresiones como $a + b \neq b + a$. De ahora en más supondremos que A es un monoide no necesariamente conmutativo y usaremos la notación multiplicativa. También usaremos esta convención para magmas arbitrarios.

Observemos que 1 es inversible con $1^{-1} = 1$, que si a es inversible a izquierda con inversa a izquierda a', entonces a' es inversible a derecha con inversa a derecha a, y que si a y b son inversibles a izquierda con inversas a izquierda a' y b' respectivamente, entonces ab es inversible a izquierda con inversa a izquierda $b'a'$. En particular, si a es inversible, a^{-1} también lo es y $(a^{-1})^{-1} = a$ y si a y b son inversibles, ab también lo es y $(ab)^{-1} = b^{-1}a^{-1}$. Es claro también que si c es un inverso a izquierda de ab, entonces ca es un inverso a izquierda de b.

Se comprueba facilmente que si a es inversible a izquierda, entonces es cancelable a izquierda. Por supuesto, los elementos inversibles a derecha son cancelables a derecha. Si a y b son cancelables a izquierda o a derecha, entonces ab también lo es. En cambio, la hipótesis de que ab es cancelable a izquierda sólo implica que b lo es y similarmente la de que ab es cancelable a derecha sólo implica que a lo es.

Proposición 1.2.1. *Si A es finito, entonces para cada $a \in A$ son equivalentes:*

1) a es inversible.

2) a es cancelable a izquierda.

3) a es cancelable a derecha.

Demostración. En efecto, dado que $|A| < \infty$,

$$\begin{aligned} a \text{ es cancelable a izquierda} &\Leftrightarrow l_a \text{ es inyectivo} \\ &\Leftrightarrow l_a \text{ es sobreyectivo} \\ &\Leftrightarrow a \text{ es inversible a derecha} \\ &\Leftrightarrow a \text{ es cancelable a derecha} \\ &\Leftrightarrow r_a \text{ es inyectivo} \\ &\Leftrightarrow r_a \text{ es sobreyectivo} \\ &\Leftrightarrow a \text{ es inversible a izquierda,} \end{aligned}$$

de dónde se sigue la proposición. □

Ejercicio 1. *Pruebe que son equivalentes:*

1) a es inversible a izquierda y cancelable a derecha,

2) a es inversible a derecha y cancelable a izquierda,

3) a es inversible.

Dado $a \in A$ definimos a^n, para $n \geq 0$, recursivamente por $a^0 = 1$ y $a^{n+1} = a^n a$. Si a es inversible definimos a^n, para $n < 0$, por $a^n = (a^{-1})^{-n}$. Dejamos como ejercicio probar que $a^{n+m} = a^n a^m$ y $(a^m)^n = a^{mn}$, para todo $n, m \geq 0$, y que cuando a es inversible, estas igualdades valen para todo $n, m \in \mathbb{Z}$. Diremos que dos elementos a y b de A *conmutan entre si* cuando $ab = ba$. Si $a, b \in A$ conmutan entre si, entonces $(ab)^n = a^n b^n$, para todo $n \geq 0$. Nuevamente, en el caso en que a y b son inversibles, la fórmula vale para todo $n \in \mathbb{Z}$.

Ejercicio 2. *Pruebe que vale lo siguiente:*

1) Si a es inversible, entonces a conmuta con b si y sólo si a^{-1} lo hace.

2) Si a y b conmutan entre si, entonces a^m y b^n también lo hacen, para todo $n, m \geq 0$.

3) Si a y b conmutan entre si, entonces $(ab)^n = a^n b^n$, para todo $n \geq 0$.

4) Si a y b son inversibles y conmutan entre si, entonces $(ab)^n = a^n b^n$, para todo $n \in \mathbb{Z}$.

5) Si a es inversible, entonces $a^{-n} = (a^n)^{-1}$, para todo $n \in \mathbb{Z}$.

6) $a^n a^m = a^{n+m}$, para todo $n, m \geq 0$.

7) Si a es inversible, entonces $a^n a^m = a^{n+m}$, para todo $n, m \in \mathbb{Z}$.

8) $(a^n)^m = a^{nm}$, para todo $n, m \geq 0$.

9) Si a es inversible, entonces $(a^n)^m = a^{nm}$, para todo $n, m \in \mathbb{Z}$.

Supongamos que $a \in A$ es inversible y que la aplicación $n \mapsto a^n$ no es inyectiva. Tomemos $0 \leq m < n$ tales que $a^n = a^m$. Entonces $a^{n-m} = a^n a^{-m} = a^n (a^m)^{-1} = 1$. Al mínimo natural n tal que $a^n = 1$ se lo llama el *orden* $|a|$ de a. En este caso los elementos $a^0, \ldots, a^{|a|-1}$ son todos distintos, ya que si existieran $0 \leq m < n < |a|$ tales que $a^m = a^n$, tendríamos que $a^{n-m} = 1$, contradiciendo la definición de $|a|$. Además si $n \in \mathbb{Z}$ y $n = |a|q + r$ con $0 \leq r < |a|$, entonces $a^n = a^r (a^{|a|})^q = a^r$, de dónde $a^n = 1$ si y sólo si n es múltiplo de $|a|$. Así $|a|$ es la cantidad de elementos de $\{a^n : n \in \mathbb{N}\}$. Cuando no existe tal n decimos que a tiene *orden infinito*.

Algunos ejemplos. A continuación damos unos pocos ejemplos de monoides.

Ejemplo 1. El conjunto $\mathbb{N}_0$ de los enteros no negativos, con la suma como operación es un monoide abeliano que tiene al 0 como neutro.

Ejemplo 2. 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 anillo conmutativo k, son monoides abelianos que tienen al 1 como neutro, via el producto.

Ejemplo 3. El conjunto $\mathrm{Fun}(X, X)$ de funciones de un conjunto X en si mismo con la composición como operación es un monoide que tiene a la identidad de X como neutro. Es fácil ver que si X tiene más de un elemento, entonces $\mathrm{Fun}(X, X)$ no es abeliano.

Ejemplo 4. Denotemos con n a un número natural arbitario. El conjunto $\mathrm{M}_n(k)$, de las matrices de $n \times n$ con coeficientes en un anillo conmutativo k, con el producto de matrices como operación, es un monoide, que tiene a la matriz identidad como neutro.

Ejemplo 5. El conjunto $\mathrm{End}_k(V)$ de endomorfismos k-lineales de un k-espacio vectorial V, con la composición como operación, es un monoide que tiene a la identidad de V como neutro. Es fácil ver que si $\dim_k(V) \geq 2$, entonces $\mathrm{End}_k(V)$ no es abeliano.

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

Proposición 1.3.1. *Un monoide G es un grupo si y sólo si para cada par a, b de elementos de G, las ecuaciones $ax = b$ y $xa = b$ tienen solución única en G.*

Demostración. Si G es un grupo, entonces $= a^{-1}b$ es la única solución de $ax = b$ y $x = ba^{-1}$ es la única solución de $xa = b$. La recíproca se sigue inmediatamente considerando las ecuaciones $ax = 1$ y $xa = 1$. □

Proposición 1.3.2. *Si un semigrupo G tiene un neutro a izquierda 1 y satisface la propiedad de que para cada elemento $a \in G$ hay un elemento $a' \in G$ tal que $a'a = 1$, entonces es un grupo con neutro 1.*

Demostración. Veamos primero que $aa' = 1$ cualquiera sea $a \in G$. En efecto, $aa' = 1(aa') = (a''a')(aa') = a''((a'a)a') = a''(1a') = a''a' = 1$. Que 1 es neutro a derecha se lo deduce ahora de que $a1 = a(a'a) = (aa')a = 1a = a$ para todo $a \in G$. □

Algunos ejemplos. A continuación damos algunos pocos ejemplos de grupos.

Ejemplo 1. El conjunto A^* de las unidades o elementos inversibles de un monoide A, dotado de la operación inducida por la de A, es un grupo que se denomina el *grupo de unidades* de A.

Ejemplo 2. Los conjuntos $\mathbb{Z}$ 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 anillo conmutativo k, son grupos via la suma usual. Por el Ejemplo 1) también lo son $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{Z}_n^*$ y $k[X]^*$ via el producto. Todos estos grupos son abelianos.

Ejemplo 3. Denotemos con n a un número natural arbitario. Por definición $\mathrm{GL}(n, k)$ es el grupo de unidades del anillo de matrices $\mathrm{M}_n(k)$ de $n \times n$ con coeficientes en un anillo conmutativo k. Este grupo es abeliano si y sólo si $n = 1$.

Ejemplo 4. Una *permutación* de un conjunto no vacío X es una función biyectiva $f\colon X \to X$. El conjunto S_X, de las permutaciones de X, es un grupo bajo 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 probar que esto es verdaderamente así, es suficiente considerar $x_1, x_2, x_3 \in X$ y exhibir dos permutaciones σ y τ de X que son la identidad sobre $X \setminus \{x_1, x_2, x_3\}$ y no conmutan. Por ejemplo, podemos tomar $\sigma(x_1) = x_2$, $\sigma(x_2) = x_3$, $\sigma(x_3) = x_1$, $\tau(x_1) = x_2$, $\tau(x_2) = x_1$ y $\tau(x_3) = x_3$. 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.

Ejemplo 5. Consideremos un k-espacio vectorial V. Por definición $\mathrm{Aut}_k(V)$ es el grupo de unidades del anillo de endomorfismos $\mathrm{End}_k(V)$. Este grupo es abeliano si y sólo si $\dim_k(V) = 1$.

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

Ejercicio 3. *Pruebe que si un grupo G tiene exponente 2, entonces es abeliano.*

1.4.Submagmas. Un subconjunto B de un magma A es un *submagma* de A si es cerrado para el producto. Es evidente que entonces B es un magma en si mismo. Cada magma A tiene a A mismo como submagma y, si A es unitario, entonces el conjunto $\{1\}$, que tiene como único elemento a la unidad de A, también es un submagma de A. Estos son los llamados submagmas *triviales* de A. Un submagma de A es *propio* si es distinto de A. Es fácil comprobar que la intersección de una familia arbitraria de submagmas de A es un submagma de A. Por ejemplo, dada una familia S de elementos de A, la intersección de los submagmas de A que incluyen a S es el mínimo submagma $\langle S\rangle_s$ de A que contiene a S. Si $A = \langle S\rangle_s$, decimos que S *genera* a A. Siguiendo la práctica usual, si $S = \{x_1, \ldots, x_n\}$, escribiremos $\langle x_1, \ldots, x_n\rangle_s$, y no $\langle\{x_1, \ldots, x_n\}\rangle_s$. Esto se debe simplemente a una cuestión de estética. Un magma A es *finitamente generado* si existe un subconjunto finito S de A que lo genera. Es claro que si A es finito, entonces es finitamente generado. Por último decimos que A es *cíclico* si existe $a \in A$ tal que $A = \langle a\rangle_s$. Dejamos al lector comprobar que $\langle S\rangle_s$ es el conjunto de los "productos" de elementos $x_1, \ldots, x_n$ con $n > 0$ y $x_i \in S$, asociados de todas las maneras posibles. Cuando A es un semigrupo, entonces todo submagma B de A también lo es. Diremos en este caso que B es un *subsemigrupo* de A. Además para todo semigrupo A y todo subconjunto S de A, vale que

$$\langle S\rangle_s = \{a_1 \cdots a_n : n \geq 1 \text{ y } a_i \in S\},$$

ya que no nos vemos obligados a tomar los productos asociados de todas las maneras posibles. Decimos que un submagma B de un magma unitario A es *unitario* si contiene a la unidad de A. Es claro también que el mínimo submagma unitario $\langle S\rangle_u$, de un magma unitario A que contiene a una familia S de elementos de A, es el mínimo submagma de A que contiene a la unidad de A y a S. Si $\langle S\rangle_u$ es igual a A, decimos que S *genera a A como magma unitario*. De la misma manera que para el caso de submagmas de magmas no unitarios, cuando S sea $\{x_1, \ldots, x_n\}$, escribiremos $\langle x_1, \ldots, x_n\rangle_u$ en lugar no $\langle\{x_1, \ldots, x_n\}\rangle_u$. Notemos por último que si un magma es conmutativo, entonces todo submagma de él también lo es.

1.5.Submonoides. Es claro que si B es un submagma unitario de un monoide A, entonces B es en si mismo un monoide. Diremos en este caso que B es un *submonoide* de A. Es claro también que para cada familia S de elementos de un monoide A, vale que

$$\langle S\rangle_u = \{a_1 \cdots a_n : n \geq 0 \text{ y } a_i \in S\},$$

si usamos la convención de que el producto vacío es el neutro.

Dados subconjuntos H y L de un magma A, denotamos con HL al subconjunto de A formado por todos los productos ab con $a \in H$ y $b \in L$. Por supuesto que escribiremos aH y Ha en lugar de $\{a\}H$ y $H\{a\}$ respectivamente. Notemos que en general $HL \subseteq \langle H \cup L\rangle_s$ y que si A es un magma unitario y $1 \in H \cap L$, entonces $H \cup L \subseteq HL$. Es evidente además que si A es un semigrupo, entonces $(HL)M = H(LM)$ para toda terna H, L y M de subconjuntos de A, de manera que no escribiremos los paréntesis. A continuación veremos una condición necesaria y suficiente para que el producto de dos submonoides de un monoide A sea un submonoide de A.

Proposición 1.5.1. *Si H y L son submonoides de un monoide A, entonces HL es un submonoide de A si y sólo si $LH \subseteq HL$.*

Demostración. Supongamos que $LH \subseteq HL$. Entonces

$$HLHL \subseteq HHLH = HLHL$$

y así HL es un submonoide de A. Recíprocamente, si HL es un submonoide de A, entonces $LH \subseteq HLHL = HL$. $\square$

Finalmente dada una familia $\{A_i\}_{i\in I}$ de submonoides de A existe un mínimo submonoide $\prod_{i\in I} A_i$ de A que contiene a $\bigcup_{i\in I} A_i$. A este submonoide se lo llama el *producto* de $\{A_i\}_{i\in I}$. Es fácil ver que

$$\prod_{i\in I} A_i = \left\langle \bigcup_{i\in I} A_i \right\rangle_u = \{a_1 \cdots a_n : n \geq 0,\ i_1, \ldots, i_n \in I \text{ y } a_j \in A_{i_j} \text{ con } i_j \neq i_{j+1}\}.$$

Notemos que si $A_iA_j = A_jA_i$ para todo $i, j \in I$, y I es un conjunto provisto de un orden total $\leq$, entonces

$$\prod_{i\in I} A_i = \{a_{i_1} \cdots a_{i_n} : n \geq 0,\ i_1 < \cdots < i_n \in I \text{ y } a_{i_j} \in A_{i_j}\}.$$

Algunos ejemplos. Para cada monoide A, el subconjunto formado por los elementos de A que son cancelables a izquierda es un submonoide de A. Por supuesto que también lo son el subconjunto formado por los elementos de A que son cancelables a derecha, el formado por los elementos cancelables y el grupo A^* de las unidades de A.

1.6.Subgrupos. Un submonoide H de un grupo G es un *subgrupo* si con cada uno de sus elementos contiene a su inverso. Es fácil ver que H es un subgrupo de G si y sólo si $H \neq \emptyset$ y $ab^{-1} \in H$ para todo $a, b \in H$ y que a su vez esto es equivalente a que $H \neq \emptyset$ y $a^{-1}b \in H$ para todo $a, b \in H$. Tomando $a = b$ en H se deduce que H contiene al 1. Es claro que $\{1\}$ y G son subgrupos de G. Además la intersección de una familia de subgrupos de G es un subgrupo de G. Así, dado un subconjunto S de G existe un mínimo subgrupo $\langle S\rangle$ de G que contiene a G. Es fácil ver que

$$\langle S\rangle = \{a_1 \cdots a_n : n \geq 0 \text{ y } a_i \in S \text{ o } a_i^{-1} \in S\}.$$

Notemos que en general $\langle S\rangle_s \subsetneq \langle S\rangle_u \subsetneq \langle S\rangle$. Por ejemplo si $\mathbb{Z}$ denota al grupo usual de los números enteros, entonces $\langle \mathbb{N}\rangle_s = \mathbb{N}$, $\langle \mathbb{N}\rangle_u = \{0\} \cup \mathbb{N}$ y $\langle \mathbb{N}\rangle = \mathbb{Z}$.

Notemos sin embargo que si $a \in G$ tiene orden finito y $a \in \langle S\rangle_s$, entonces 1 y a^{-1} pertenecen a $\langle S\rangle_s$, ya que ambos elementos son potencias de a. Así, si $S \neq \emptyset$ y todos los elementos de S tienen orden finito, $\langle S\rangle_s = \langle S\rangle$. Si $G = \langle S\rangle$, decimos que S *genera a* G *como grupo* o más simplemente que S *genera* a G. Al igual que para magmas escribiremos $\langle x_1, \ldots, x_n\rangle$ en lugar de $\langle\{x_1, \ldots, x_n\}\rangle$. Un grupo G es *finitamente generado* si existe un subconjunto finito S de G tal que $G = \langle S\rangle$, y es *cíclico* si existe $a \in G$ tal que $G = \langle a\rangle$. Si a tiene orden infinito, entonces la asignación $n \mapsto a^n$ es una biyección entre $\mathbb{Z}$ y G y si a tiene orden finito, entonces $G = \{a^0, \ldots, a^{|a|-1}\}$ tiene $|a|$ elementos. Notemos por último que el producto $\prod_{i\in I} G_i$ de una familia $\{G_i\}_{i\in I}$ de subgrupos de un grupo G (como está definido para una familia de submonoides de un monoide) es un subgrupo de G.

Ejercicio 4. *Pruebe que vale lo siguiente:*

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 $G = \langle G \setminus H\rangle$.

Algunos ejemplos. A continuación damos unos pocos ejemplos de subgrupos.

Ejemplo 1. El conjunto $\mathrm{SL}(n, k)$, formado por las matrices de $n\times n$ con coeficientes en un anillo conmutativo k, que tienen determinante 1, es un subgrupo de $\mathrm{GL}(n, k)$.

Ejemplo 2. 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 $\mathbb{C}^*$. Por supuesto que también lo es $\mathrm{G}_\infty = \bigcup_{n\in\mathbb{N}} \mathrm{G}_n$.

Ejemplo 3. Para $n > 1$ tomemos $\theta = 2\pi/n$. Al subgrupo de $\mathrm{GL}(2, \mathbb{R})$ generado por

$$a = \begin{pmatrix} \cos\theta & \operatorname{sen}\theta \\ -\operatorname{sen}\theta & \cos\theta \end{pmatrix} \qquad \text{y} \qquad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

se lo llama grupo diedral D_n. Veamos que $|D_n| = 2n$. Un cálculo directo muestra que

$$a^i = \begin{pmatrix} \cos i\theta & \operatorname{sen} i\theta \\ -\operatorname{sen} i\theta & \cos i\theta \end{pmatrix}, \quad b^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{y} \quad ba^i = \begin{pmatrix} -\operatorname{sen} i\theta & \cos i\theta \\ \cos i\theta & \operatorname{sen} i\theta \end{pmatrix} = a^{-i}b.$$

De esto se sigue facilmente que a y b satisfacen las relaciones $a^n = 1$, $b^2 = 1$ y $bab^{-1} = a^{-1}$ y que D_n consiste de los $2n$ elementos $1, a \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b$. Destaquemos además lo siguiente:

1) Los elementos de la forma a^ib tienen orden 2.

2) Los elementos de la forma a^i tienen orden $n/\operatorname{mdc}(n, i)$, donde $\operatorname{mdc}(n, i)$ denota al máximo de los divisores comunes de n e i. En consecuencia para cada divisor d de n hay $\varphi(d)$ elementos de orden d de la forma a^i.

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

Ejemplo 4. Para $n > 1$ fijemos una raíz $w \in \mathbb{C}$ de la unidad de orden $2n$. Al subgrupo de $\mathrm{GL}(2, \mathbb{C})$ generado por

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

se lo llama grupo cuaterniónico generalizado H_n. Veamos que $|H_n| = 4n$. Un cálculo directo muestra que

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

De esto se sigue facilmente que a y b satisfacen las relaciones $a^n = b^2$ y $bab^{-1} = a^{-1}$ y que H_n consiste de los $4n$ elementos $1, a \ldots, a^{2n-1}, b, ab, \ldots, a^{2n-1}b$. Notemos que de la relación $bab^{-1} = a^{-1}$ se sigue que $ba^nb^{-1} = a^{-n}$, lo que combinado con la relación $a^n = b^2$ da $a^{2n} = b^4 = 1$. Es útil además destacar lo siguiente:

1) Los elementos de la forma a^ib tienen orden 4.
2) Los elementos de la forma a^i tienen orden $2n/\operatorname{mdc}(2n, i)$, donde $\operatorname{mdc}(2n, i)$ denota al máximo de los divisores comunes de $2n$ e i. En consecuencia para cada divisor d de $2n$ hay $\varphi(d)$ elementos de orden d de la forma a^i.

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

Subgrupos de un grupo cíclico. Supongamos que $G = \langle a \rangle$ es cíclico infinito. Entonces la asignación $n \mapsto \langle a^n \rangle$ es una correspondencia biyectiva entre $\mathbb{N}_0$ y los subgrupos de G. En efecto es claro que $\langle a^n \rangle \neq \langle a^m \rangle$ si $n \neq m$ y que $\{1\} = \langle a^0 \rangle$. Tomemos un subgrupo $H \neq \{1\}$ de G y denotemos con n al mínimo natural tal que $a^n \in H$. Si $a^m \in H$ y $m = nq + r$ con $0 \leq r < n$, entonces $a^r = a^{m-nq} = a^m(a^n)^{-q} \in H$, de dónde $r = 0$. Esto muestra que $H = \langle a^n \rangle$. Notemos además que los subgrupos no triviales de $\langle a \rangle$ son cíclicos infinitos.

Supongamos ahora que $G = \langle a \rangle$ es cíclico finito. Entonces la asignación $n \mapsto \langle a^n \rangle$ define una correspondencia biyectiva entre el conjunto de los divisores positivos de $|a|$ y los subgrupos de G. Además para todo divisor positivo n de $|a|$, el orden de $\langle a^n \rangle$ es $|a|/n$ y si $n \in \mathbb{Z}$ es arbitrario $\langle a^n \rangle = \langle a^{(|a|:n)} \rangle$, dónde $(|a| : n)$ denota al máximo de los divisores comunes de $|a|$ y n (en particular a^n es un generador de $\langle a \rangle$ si y sólo si n es coprimo con $|a|$). En efecto, tomemos un subgrupo H de G y denotemos con n al mínimo natural tal que $a^n \in H$. Si $a^m \in H$ y $m = nq+r$ con $0 \leq r < n$, entonces $a^r = a^{m-nq} = a^m(a^n)^{-q} \in H$, de dónde $r = 0$. Así $H = \langle a^n \rangle$ y como $a^{|a|} = 1$ esto implica que n divide a $|a|$. Es inmediato que el orden de H es $|a|/n$. Tomemos ahora $n \in \mathbb{Z}$ arbitrario. Es claro que $\langle a^n \rangle \subseteq \langle a^{(|a|:n)} \rangle$. Como existen $r, s \in \mathbb{Z}$ tales que $(|a| : n) = r|a| + sn$, tenemos $a^{(|a|:n)} = (a^{|a|})^r(a^n)^s = (a^n)^s \in \langle a^n \rangle$, de dónde $\langle a^{(|a|:n)} \rangle = \langle a^n \rangle$.

Coclases a izquierda y a derecha. Fijemos un subgrupo H de un grupo G. Una *coclase a izquierda* de H en G es un subconjunto de G que tiene la forma aH para algún $a \in G$. Dos coclases a izquierda que no son disjuntas coinciden. En efecto, si $ah = bh'$ con $h, h' \in H$, entonces $aH = ahH = bh'H = bH$. Así, G es la unión disjunta de sus coclases a izquierda. Además, dado que la aplicación $h \mapsto ah$ induce una biyección de H en aH, todas las coclases a izquierda tienen el mismo cardinal. Esto muestra que

$$|G| = |G : H||H|,$$

donde $|G : H|$ a la cantidad de coclases a izquierda de H en G. Este número es llamado el índice de H en G. Un argumento similar al que llevamos a cabo hasta aquí se aplica a las coclases a derecha de H en G que son los subconjuntos de G de

la forma Ha para algún $a \in G$. Dado que la asignación $aH \mapsto Ha^{-1}$ establece una biyección entre el conjunto de las coclases a izquierda de H y el de las coclases a derecha, ambos tienen la misma cantidad de elementos.

La igualdad $|G| = |G : H||H|$ es conocida como el teorema de Lagrange y se generaliza de la siguiente forma.

Teorema 1.6.1. *Si $K \subseteq H$ son subgrupos de un grupo G, entonces*

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

Demostración. Expresemos G y H como uniones disjuntas

$$G = \bigcup_i a_i H \qquad \text{y} \qquad H = \bigcup_j b_j K,$$

de coclases a izquierda de H en G y de K en H respectivamente. Es claro que $G = \bigcup_{i,j} a_i b_j K$. Debemos probar que esta unión es disjunta. Supongamos que $a_i b_j K = a_{i'} b_{j'} K$. Multiplicando por H a la derecha obtenemos que $a_i H = a_{i'} H$, lo que implica que $i = i'$. Pero entonces $b_j K = b_{j'} K$, de donde $j = j'$. □

Corolario 1.6.2. *Si G es finito, entonces el exponente de G divide al orden de G.*

Corolario 1.6.3. *Si un grupo tiene orden primo, entonces es cíclico.*

Observación 1.6.4. *Del teorema de Lagrange se sigue en particular que si un grupo finito G tiene elementos de orden 2, entonces $|G|$ es par. Afirmamos que vale la recíproca. Supongamos así que $|G|$ es par y escribamos*

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

Dado que $|a| = 2$ si y sólo si $a \neq 1$ y $a^{-1} = a$, el conjunto $\{a \in G : |a| > 2\}$ tiene una cantidad par de elementos (estos se pueden agrupar de a pares, cada uno con su inverso). Así, $|\{a \in G : |a| = 2\}|$ es impar y, por lo tanto, $\{a \in G : |a| = 2\} \neq \emptyset$. Este resultado será generalizado más adelante.

Observación 1.6.5. *Si la intersección de una familia $(a_i H_i)_{i \in I}$ 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 $a \in \bigcap_{i \in I} a_i H_i$, entonces $aH_i = a_i H_i$ para todo $i \in I$ y, por lo tanto $\bigcap_{i \in I} a_i H_i = a \bigcap_{i \in I} H_i$.*

Dado un subconjunto H de un grupo G escribimos $H^{-1} = \{a^{-1} : a \in H\}$. Es inmediato que $(H^{-1})^{-1} = H$ y que si L es otro subconjunto de G, entonces $(HL)^{-1} = L^{-1} H^{-1}$.

Proposición 1.6.6. *Si H y L son subconjuntos de un grupo finito G y se satisface $\#(H) + \#(L) > |G|$, entonces $G = HL$.*

Demostración. Tomemos $a \in G$. Dado que $\#(H^{-1}a) = \#(H)$ tenemos por hipótesis que $\#(H^{-1}a) + \#(L) > |G|$ y así $H^{-1}a \cap L \neq \emptyset$. Por lo tanto existen $b \in H$ y $c \in L$ tales que $b^{-1}a = c$, de donde $a = bc \in HL$. □

Ejercicio 5. *Pruebe que cada elemento de un cuerpo finito es suma de dos cuadrados.*

A continuación damos tres proposiciones acerca del producto de subgrupos. La primera da dos propiedades generales conocidas como ley de Dedekind y ley modular, respectivamente, la segunda da una fórmula para calcular el cardinal de este producto y la tercera da una condición necesaria y suficiente para que este producto sea un subgrupo.

Proposición 1.6.7. *Si $K \subseteq H$ y L son subgrupos de un grupo G, entonces*

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

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

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

$$H = H \cap HL = H \cap KL = K(H \cap L) = K(K \cap L) = K. \quad \square$$

Proposición 1.6.8. *Si H y L son subgrupos de un grupo G, entonces*

$$\#(HL)|H \cap L| = |H||L|.$$

Demostración. Como la función $\phi\colon H \times L \to HL$, definida por $\phi(h, l) = hl$ es sobreyectiva, es suficiente ver que $|\phi^{-1}(a)| = |H \cap L|$, para todo $a \in HL$. Para ello bastará probar que si $a = hl$, entonces $\phi^{-1}(a) = \{(hb, b^{-1}l) : b \in H \cap L\}$. Es claro que $\{(hb, b^{-1}l) : b \in H \cap L\} \subseteq \phi^{-1}(a)$. Supongamos ahora que $(h', l') \in \phi^{-1}(a)$. Entonces $h'l' = a = hl$ y así, $b := h^{-1}h' = ll'^{-1} \in H \cap L$, de donde $h' = hb$ y $l' = b^{-1}l$. $\square$

Proposición 1.6.9. *Supongamos que H y L son subgrupos de un grupo G. Vale lo siguiente:*

1) Si $LH \subseteq HL$, entonces HL es un subgrupos de G.

2) Si HL es un subgrupo de G, entonces $LH = HL$.

Demostración. Supongamos que $LH \subseteq HL$. Entonces

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

y así HL es un subgrupo de G. Recíprocamente, si HL es un subgrupo de G, entonces $LH = L^{-1}H^{-1} = (HL)^{-1} = HL$. $\square$

Notemos que de la proposición anterior se sigue inmediatamente que si H y L son subgrupos de un grupo G y $LH \subseteq HL$, entonces $LH = HL$.

Observación 1.6.10. *Si H y L son subgrupos de un grupo G, entonces*

$$|H : H \cap L| \leq |G : L| \qquad y \qquad |G : H \cap L| \leq |G : H||G : L|.$$

En efecto la primera desigualdad se sigue de que la aplicación

$$\phi\colon H/(H \cap L) \to G/L, \quad \textit{definida por} \quad \phi(a(H \cap L)) = aL,$$

es inyectiva ya que $aL = bL$ equivale a que $a^{-1}b \in L$ y por lo tanto a que $a^{-1}b$ pertenece a $H \cap L$ (ya que $a, b \in H$) y, en consecuencia, $a(H \cap L) = b(H \cap L)$. La segunda desigualdad se sigue ahora de que $|G\colon H \cap L| = |G\colon H||H\colon H \cap L|$. Notemos también que la imagen de ϕ es $\{aL : a \in HL\}$, de manera de que si HL es un subgrupo de G, entonces

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

En particular si $HL = G$ las desigualdades de arriba se convierten en igualdades. Además se sigue claramente de todo esto que:

1) $|G : H \cap L|$ es finito si y sólo si $|G : H|$ y $|G : L|$ lo son.

2) Si $|G : L|$ es finito y $|H : H \cap L| = |G : L|$, entonces $HL = G$.

3) Si $|G : H|$ es finito y $|G\colon H \cap L| = |G : H||G : L|$, entonces $|H\colon H \cap L| = |G : L|$.

Por último, dado que por el Teorema 1.6.1, $|G : H|$ y $|G : L|$ dividen a $|G : H \cap L|$, en el caso en que $|G : H|$ y $|G : L|$ son finitos tenemos que

$$\operatorname{mmc}(|G : H|, |G : L|) \textit{ divide a } |G : H \cap L| \quad y \quad |G : H \cap L| \leq |G : H||G : L|,$$

donde $\operatorname{mmc}(|G : H|, |G : L|)$ *denota al mínimo de los múltiplos comunes de $|G : H|$ y $|G : L|$. Así, si $|G : H|$ y $|G : L|$ son coprimos, $|G : H \cap L| = |G : H||G : L|$.*

Coclases dobles. Denotemos con H y L a dos subgrupos (no necesariamente distintos) de un grupo G. Una (H, L)-coclase doble es un subconjunto de G de la forma HaL. Dado que la relación definida por $b \equiv a$ si y sólo si $b \in HaL$, es de equivalencia, G se parte como una unión disjunta $G = \bigcup_{i \in I} Ha_iL$. Supongamos que G es finito. Entonces

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

En efecto, claramente $|G| = \sum_{i \in I} |Ha_iL|$. Así que debemos calcular $|Ha_iL|$, pero $|Ha_iL| = |Ha_iLa_i^{-1}|$ y, dado que H y $a_iLa_i^{-1}$ son subgrupos de G, por la Proposición 1.6.8,

$$|Ha_iLa_i^{-1}| = \frac{|H||a_iLa_i^{-1}|}{|H \cap a_iLa_i^{-1}|} = \frac{|H||L|}{|H \cap a_iLa_i^{-1}|},$$

de donde (1) se sigue inmediatamente. Notemos que cuando $L = \{1\}$ la fórmula (1) se reduce al teorema de Lagrange.

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

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

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

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

Subgrupos normales. Un subgrupo H de un grupo G es *normal* o *invariante* si $aHa^{-1} = H$ para todo $a \in G$. A continuación damos una caracterización sencilla de los subgrupos normales, que muestra en particular que un subgrupo H de G es normal si y sólo si las coclases a izquierda y derecha de H coinciden (de todas las maneras en que sea razonable entender esto).

Proposición 1.6.11. *Para cada subgrupo H de G son equivalentes:*

1) *Dado $a \in G$ existe $b \in G$ tal que $aH \subseteq Hb$,*
2) *Dado $a \in G$ existe $b \in G$ tal que $aHb^{-1} \subseteq H$,*
3) *Dado $a \in G$ existe $b \in G$ tal que $Ha \subseteq bH$,*
4) *Dado $a \in G$ existe $b \in G$ tal que $b^{-1}Ha \subseteq H$,*
5) *$Ha = aH$ para todo $a \in G$,*
6) *H es normal.*

Demostración. Es evidente que 5) implica 1) y 3) y claramente 1) es equivalente a 2), ya que de $aH \subseteq Hb$ se sigue que $aHb^{-1} \subseteq Hbb^{-1} = H$ y de $aHb^{-1} \subseteq H$ se sigue que $aH = aHb^{-1}b \subseteq Hb$. Similarmente 3) es equivalente a 4) y 5) a 6). Veamos que 1) implica 5). De $a \in aH \subseteq Hb$ se sigue facilmente que que $Ha = Hb$ y así $aH \subseteq Ha$. Similarmente $a^{-1}H \subseteq Ha^{-1}$ y, por lo tanto, $Ha = aa^{-1}Ha \subseteq aHa^{-1}a = aH$, de donde, $aH = Ha$. Para terminar la demostración resta ver que 3) implica 5), lo cual es similar a 1) implica 5). □

Ejercicio 6. *Pruebe que un subgrupo H de G es invariante si y sólo si $ab \in H$ implica que $ba \in H$.*

Observación 1.6.12. *Si $H \subseteq L$ son subgrupos de un grupo G y H es normal en G, entonces H es normal en L.*

Observación 1.6.13. *Si H es un subgrupo normal de G, entonces $HL = LH$ para todo subconjunto L de G. Si además L es un subgrupo de G, entonces HL también es un subgrupo de G. Por último si L es normal en G, entonces HL también lo es.*

La siguiente proposición será mejorada más adelante.

Proposición 1.6.14. *Todo subgrupo H de un grupo G de índice 2, es normal.*

Demostración. Tomemos $a \in G \setminus H$. Como H tiene índice 2, es

$$G = H \bigcup aH = H \bigcup Ha$$

con ambas uniones disjuntas. Así $aH = Ha$, de dónde H es normal. $\square$

Claramente la intersección de una familia de subgrupos normales de G es un subgrupo normal de G. Así, dado un subconjunto S de G existe un mínimo subgrupo normal $\overline{\langle S\rangle}$ de G que contiene a S. Es fácil ver que

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

Por supuesto que en general $\langle S\rangle$ está incluído estrictamente en $\overline{\langle S\rangle}$.

Proposición 1.6.15. Si $\{G_i\}_{i\in I}$ es una familia de subgrupos normales de un grupo G, entonces $\prod_{i\in I} G_i$ es normal. Si además le damos un orden total a I, entonces

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

Demostración. Lo último se sigue de que, por la Observación 1.6.13, $G_iG_j = G_jG_i$, para todo $i, j \in I$. Tomemos ahora $a_{i_1}\cdots a_{i_n} \in \prod_{i\in I} G_i$. Como, para cada $a \in G$ vale que $a(a_{i_1}\cdots a_{i_n})a^{-1} = (aa_{i_1}a^{-1})(aa_{i_2}a^{-1})\cdots(aa_{i_n}a^{-1}) \in \prod_{i\in I} G_i$, el subgrupo $\prod_{i\in I} G_i$ de G es normal. $\square$

1.7.Caracterización de los grupos cíclicos finitos. La función $\phi\colon \mathbb{N} \to \mathbb{N}$ de Euler está definida por

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

Es facil ver que si p es un número primo, entonces $\phi(p^n) = p^{n-1}(p-1)$ para todo $n \in \mathbb{N}$. En efecto esto se sigue de que $\{0, \ldots, p^n - 1\}$ tiene p^n elementos, de los cuales p^{n-1} son múltiplos de p. Por lo que hemos visto al estudiar los subgrupos de un grupo cíclico finito, si G es un grupo cíclico de orden n entonces G tiene $\phi(n)$ generadores y además si d divide a n, entonces G tiene exactamente un subgrupo de orden d, que además es cíclico.

Lema 1.7.1. *Cada grupo G se expresa como la unión disjunta*

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

donde C recorre el conjunto de los subgrupos cíclicos de G y $\operatorname{gen}(C)$ denota al conjunto de los generadores de C.

Demostración. Porque cada elemento de G es generador de un único subgrupo cíclico de G. $\square$

Proposición 1.7.2. *Vale que $n = \sum_{d/n} \phi(d)$ para todo $n \in \mathbb{N}$.*

Demostración. Por el lema anterior $n = |\mathbb{Z}_n| = \sum_{d/n} \phi(d)$, ya que como vimos arriba $\mathbb{Z}_n$ tiene exactamente un subgrupo cíclico de orden d para cada divisor d de n y este subgrupo tiene $\phi(d)$ generadores. $\square$

Teorema 1.7.3. *Un grupo G de orden n es cíclico si y sólo si, para cada divisor d de n, tiene a lo sumo un subgrupo de orden d.*

Demostración. Ya vimos que si G es cíclico, entonces tiene exactamente un subgrupo de orden d para todo divisor d de n. Veamos la recíproca. Supongamos que G es un grupo de orden n. Por el Lema 1.7.1 y la Proposición 1.7.2,

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

donde C recorre el conjunto de los subgrupos cíclicos de G y $\text{gen}(C)$ denota al conjunto de los generadores de C. Por lo tanto, dado 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 así es cíclico. □

Teorema 1.7.4. *Si F es un cuerpo y G es un subgrupo finito de F^*, entonces G es cíclico.*

Demostración. Si $|G| = n$ y si $x \in G$ satisface $x^d = 1$, donde d/n, 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 $X^d - 1$). Así, por el teorema anterior, G es cíclico. □

1.8.Morfismos de magmas. Un *morfismo de magmas* $f\colon A \to B$ es una terna formada por dos magmas A y B y una función f, del conjunto subyacente de A en el de B, que satisface $f(ab) = f(a)f(b)$. A A, B y f se los denomina *dominio*, *codominio* y *función subyacente* de $f\colon A \to B$, respectivamente. La *composición* $g \circ f\colon A \to C$ de dos morfismos de magmas $f\colon A \to B$ y $g\colon B \to C$, es por definición el morfismo que tiene a A como dominio, a C como codominio y a la composición $g \circ f$ como función subyacente. Un ejemplo de morfismo de magmas es el dado por la inclusión canónica de un submagma A de un magma B en B. Un caso particular de esto es la función identidad id_A de un magma A en si mismo. Si B es un magma unitario, entonces cualquiera sea el magma A, la aplicación $f\colon A \to B$, definida por $f(a) = 1$, para todo $a \in A$ es un morfismo de magmas. Es inmediato que si $f\colon A \to B$ es un morfismo de magmas, entonces $f(KL) = f(K)f(L)$ para todo par de subconjuntos K y L de A.

Ejercicio 7. *Supongamos que $f\colon A \to B$ es un morfismo sobreyectivo de magmas. Pruebe que:*

1) *Si A es asociativo, entonces B también lo es.*
2) *Si A es conmutativo, entonces B también lo es.*
3) *Si e es unidad a izquierda de A, entonces $f(e)$ es unidad a izquierda de B.*

Un *endomorfismo* de A es un morfismo con dominio y codominio A. Un ejemplo es la función identidad de A. Un morfismo $f\colon A \to B$ es un *isomorfismo* si existe un morfismo $f^{-1}\colon B \to A$, necesariamente único, llamado la *inversa* de f, tal que $f^{-1} \circ f = \text{id}_A$ y $f \circ f^{-1} = \text{id}_B$. Es fácil ver que esto ocurre si y sólo si f es biyectiva. Un *automorfismo* de A es un endomorfismo de A que es un isomorfismo. Los símbolos $\text{Hom}(A, B)$, $\text{Iso}(A, B)$, $\text{End}(A)$ y $\text{Aut}(A)$ denotan respectivamente a

los conjuntos de morfismos de A en B, isomorfismos de A en B, endomorfismos de A y automorfismos de A. Notemos que $\mathrm{End}(A)$, dotado de la operación dada por la composición de morfismos, es un monoide que tiene a la identidad de A como unidad, y que además $\mathrm{Aut}(A) = \mathrm{End}(A)^*$. Un *morfismo de magmas unitarios* $f\colon A \to B$, es un morfismo de magmas que satisface $f(1) = 1$, donde 1 denota tanto al neutro de A como al de B. Es claro que la inclusión canónica de un submagma unitario A de un magma unitario B en B es un morfismo de magmas unitarios y que la composición de dos morfismos de magmas unitarios también lo es. Además si un morfismo de magmas unitarios es biyectivo, entonces su inversa también es un morfismo de magmas unitarios. Dado un magma unitario A vamos a denotar con $U(A)$ a A considerado como magma no unitario. Analogamente si $f\colon A \to B$ es un morfismo de magmas unitarios denotamos con $U(f)\colon U(A) \to U(B)$ a la misma aplicación pero considerada como morfismo de magmas no unitarios. Es obvio que $U(\mathrm{id}_A) = \mathrm{id}_{U(A)}$ y que si $g\colon B \to C$ es otro morfismo de magmas unitarios, entonces $U(g \circ f) = U(g) \circ U(f)$. Con $\mathrm{Hom}(A, B)$, $\mathrm{Iso}(A, B)$, $\mathrm{End}(A)$ y $\mathrm{Aut}(A)$ denotamos a los subconjuntos de $\mathrm{Hom}(U(A), U(B))$, $\mathrm{Iso}(U(A), U(B))$, $\mathrm{End}(U(A))$ y $\mathrm{Aut}(U(A))$ respectivamente, formados por los morfismos de magmas unitarios. Es claro que

$$\mathrm{Iso}(A, B) = \mathrm{Iso}(U(A), U(B)) \cap \mathrm{Hom}(A, B) \quad \text{y} \quad \mathrm{Aut}(A) = \mathrm{Aut}(U(A)) \cap \mathrm{End}(A).$$

Finalmente diremos que un morfismo de magmas $f\colon A \to B$ es un *monomorfismo* si $f \circ g = f \circ g'$ implica $g = g'$, para todo par de morfismos de magmas $g, g'\colon C \to A$; un *epimorfismo* si $g \circ f = g' \circ f$ implica $g = g'$, para todo par de morfismos de magmas $g, g'\colon B \to C$; una *sección* si existe $g\colon B \to A$ tal que $g \circ f = \mathrm{id}_A$ y una *retracción* si existe $h\colon B \to A$ tal que $f \circ h = \mathrm{id}_B$. En el caso en que A y B son unitarios pedimos que todos los morfismos que aparecen en estas definiciones sean de magmas unitarios. Notemos de todos modos que si $f\colon A \to B$ es un morfismo de magmas unitarios y $g\colon U(B) \to U(A)$ es un morfismo de magmas, entonces de $g \circ U(f) = \mathrm{id}_{U(A)}$ se sigue que g es un morfismo de magmas unitarios. No vale sin embargo que si $f\colon A \to B$ es un morfismo de magmas unitarios y $h\colon U(B) \to U(A)$ es un morfismo de magmas, se siga de $U(f) \circ h = \mathrm{id}_{U(B)}$, que h es un morfismo de magmas unitarios. Denotemos con $f\colon A \to B$ y $g\colon B \to C$ a dos morfismos de magmas. Pruebe que:

1) Si f y g son monomorfismos, entonces $g \circ f$ también lo es.
2) Si $g \circ f$ es un monomorfismo, entonces f también lo es.
3) Si f y g son epimorfismos, entonces $g \circ f$ también lo es.
4) Si $g \circ f$ es un epimorfismo, entonces g también lo es.
5) Si f y g son secciones, entonces $g \circ f$ también lo es.
6) Si $g \circ f$ es una sección, entonces f también lo es.
7) Si f y g son retracciones, entonces $g \circ f$ también lo es.
8) Si $g \circ f$ es una retracción, entonces g también lo es.
9) Si f es inyectivo, entonces es un monomorfismo.
10) Si f es una sección, entonces es inyectiva.
11) Si f es sobreyectivo, entonces es un epimorfismo.
12) Si f es una retracción, entonces es sobreyectiva.

13) f es un isomorfismo si y sólo si es una sección y un epimorfismo y esto a su vez ocurre si y sólo si es una retracción y un monomorfismo.

Pruebe que estos todos estos items valen también en el caso de magmas unitarios y morfismos de magmas unitarios.

1.9.Morfismos de monoides. Un *morfismo* $f\colon A \to B$, de un monoide A en otro B, es simplemente un morfismo de magmas unitarios. Por ejemplo la inclusión canónica de un submonoide A de un monoide B en B es un morfismo de monoides. Observemos que en el caso de monoides la condición $f(1) = 1$ equivale a que $f(1)$ sea inversible, de modo de que no es necesario pedirla cuando B es un grupo. Esto se deduce multiplicando por $f(1)^{-1}$ la igualdad $f(1) = f(1)f(1)$. De la definición de morfismo se sigue inmediatamente que si b es inversa a izquierda de a, entonces $f(b)$ es inversa a izquierda de $f(a)$. En particular, si a es inversible, entonces $f(a)$ también lo es y $f(a)^{-1} = f(a^{-1})$. Finalmente diremos que un morfismo de monoides $f\colon A \to B$ es un *monomorfismo* si $f \circ g = f \circ g'$ implica $g = g'$, para todo par de morfismos de monoides $g, g'\colon C \to A$, y que es un *epimorfismo* si $g \circ f = g' \circ f$ implica $g = g'$, para todo par de morfismos de monoides $g, g'\colon B \to C$. Notemos que, al menos en principio, un morfismo de monoides puede ser un monomorfismo o un epimorfismo, cuando se lo considera como morfismo de monoides, pero puede dejar de serlo cuando se lo considera como morfismo de magmas. Hay también una definición de sección y de retracción, pero coincide con la dada anteriormente para morfismos de magmas unitarios. Es facil ver que los items 1) a 13) del ejercicio con que termina la sección anterior siguen valiendo es el contexto de monoides. Aquí también vale que todo monomorfismo $f\colon A \to B$ es inyectivo. En efecto, si no lo fuera, entonces existirían a y a' distintos en A con $f(a) = f(a')$ y para los morfismos $g, g'\colon \mathbb{N}_0 \to A$ definidos por $g(n) = a^n$ y $g'(n) = a'^n$ se cumpliría claramente que $f \circ g = f \circ g'$. De esto se sigue facilmente que un monomorfismo de monoides sigue siendo un monomorfismo cuando se lo considera como morfismo de magmas. Por último, si $f\colon A \to B$ es un morfismo de monoides y $a \in A$ es un elemento inversible de orden n, entonces de $f(a)^n = f(a^n) = f(1) = 1$ se sigue que el orden de $f(a)$ divide a n y que es exactamente n si f es inyectiva, ya que en este caso de $f(a^m) = f(a)^m = 1$ se sigue que $a^m = 1$.

1.10.Morfismos de grupos. Un *morfismo* $f\colon G \to G'$, de un grupo G en otro G', es por definición morfismo de monoides. Como vimos recién es innecesario pedir que $f(1)$ sea 1. Al igual que para el caso de monoides pueden darse aquí definiciones de *monomorfismo*, *epimorfismo*, *sección* y *retracción*. Nuevamente estas últimas coinciden con las definiciones dadas en el caso de magmas unitarios y, en principio, un morfismo de grupos puede ser un monomorfismo o un epimorfismo, cuando se lo considera como morfismo de grupos, pero puede dejar de serlo cuando se lo considera como morfismo de monoides o magmas. Sin embargo en este caso también vale que todo monomorfismo $f\colon G \to G'$ es inyectivo. En efecto, si no lo fuera, entonces existirían a y a' distintos en G con $f(a) = f(a')$ y para los morfismos $g, g'\colon \mathbb{Z} \to G$ definidos por $g(n) = a^n$ y $g'(n) = a'^n$ se cumpliría claramente que $f \circ g = f \circ g'$. De esto se sigue facilmente que un monomorfismo de grupos sigue siendo un monomorfismo cuando se lo considera como morfismo de monoides o de magmas. Se puede ver también que todo epimorfismo de grupos es sobreyectivo, pero esto es mucho más dificil (probaremos esto en la Observación 2.1.3). Nuevamente valen con las mismas demostraciones los items 1) a 13) del ejercicio con que termina la sección de morfismos de magmas. Por último es claro que si $f\colon G \to G'$ es un

morfismo de grupos, entonces $f(K^{-1}) = f(K)^{-1}$, para cada subconjunto K de G.

Ejercicio 8. *Denotemos con $f\colon G \to G'$ a un morfismo de grupos y con K y L a dos subconjuntos de G'.*

1) Pruebe que $f^{-1}(K^{-1}) = f^{-1}(K)^{-1}$.

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

Algunos ejemplos. A continuación damos unos pocos ejemplos de morfismos de grupos.

Ejemplo 1. El determinante $\det\colon \mathrm{GL}(n,k) \to k^*$ es un morfismo sobreyectivo de grupos.

Ejemplo 2. 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 3. La exponencial $x \mapsto e^{ix}$ es un morfismo del grupo aditivo $\mathbb{R}$ en el grupo multiplicativo $\mathbb{C}^*$, formado por los números complejos no nulos. Su imagen es el círculo unidad.

Ejemplo 4. La aplicación $\phi\colon \mathbb{C}^* \to \mathbb{R}_{>0}$, definida por $\phi(x) = |x|$, es un morfismo sobreyectivo del grupo multiplicativo de los números complejos no nulos en el grupo multiplicativo de los números reales positivos.

Ejemplo 5. La aplicación $\phi\colon \mathbb{Z}[X] \to \mathbb{Q}^*_{>0}$, definida por $\phi\big(\sum_{i\geq 0} n_i X^i\big) = \prod_{i\geq 0} p_i^{n_i}$, donde $p_0 < p_1 < p_2 \ldots$ es la sucesión de los números primos positivos, es un isomorfismo del grupo aditivo de los polinomios con coeficientes en $\mathbb{Z}$ en el grupo multiplicativo de los números racionales positivos.

Ejemplo 6. Denotemos con w a una raíz de orden n de la unidad de $\mathbb{C}$ (por ejemplo $w = \cos(2\pi/n) + i\,\mathrm{sen}(2\pi/n)$). La aplicación $\varphi\colon \mathbb{Z}_n \to \mathrm{G}_n$, definida por $\varphi(n) = w^n$, es un isomorfismo de grupos.

Ejemplo 7. El monomorfismo de $i\colon \mathbb{Z}_2 \to \mathbb{Z}_4$, definido por $\pi(0) = 0$ y $\pi(1) = 2$, no es una sección.

Ejemplo 8. La sobreyección canónica $\pi\colon \mathbb{Z}_4 \to \mathbb{Z}_2$, definida por $\pi(0) = \pi(2) = 0$ y $\pi(1) = \pi(3) = 1$, no es una retracción.

En general $\mathrm{Hom}(G, G')$ no tiene ninguna estructura algebraica, pero esto cambia cuando G' es abeliano.

Proposición 1.10.1. *Si G' es abeliano, entonces $\mathrm{Hom}(G, G')$ es un grupo abeliano via $(fg)(a) = f(a)g(a)$. El neutro de este grupo es el morfismo 1 que envía todo elemento de G en el neutro de G' y la inversa f de un elemento de $\mathrm{Hom}(G, G')$ es la función f^{-1}, definida por $f^{-1}(a) = f(a)^{-1}$.*

Demostración. Como G' es abeliano,

$$(fg)(ab) = f(ab)g(ab) = f(a)f(b)g(a)g(b) = f(a)g(a)f(b)g(b) = (fg)(a)(fg)(b)$$

y así, fg es un morfismo de grupos. Es claro que $fg = gf$ y que el neutro de $\mathrm{Hom}(G, G')$ es el morfismo 1 que envía todo elemento de G en el neutro de G'. Finalmente, si $f\colon G \to G'$ es un morfismo de grupos, entonces la aplicación $f^{-1}\colon G \to G'$ definida por $f^{-1}(a) = f(a)^{-1}$ también lo es, ya que

$$f^{-1}(ab) = f(ab)^{-1} = (f(a)f(b))^{-1} = f(a)^{-1}f(b)^{-1} = f^{-1}(a)f^{-1}(b),$$

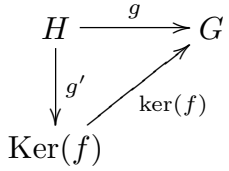
donde la anteúltima igualdad se sigue de que G' es abeliano. □

Observación 1.10.2. *de la misma manera se puede ver que si A y A' son semigrupos y A' es abeliano, entonces* $\mathrm{Hom}(A, A')$ *es un semigrupo abeliano y similarmente que si A y A' son monoides y A' es abeliano, entonces* $\mathrm{Hom}(A, A')$ *es un monoide abeliano*

El núcleo de un morfismo. El *núcleo* de un morfismo de grupos $f\colon G \to G'$ es $\mathrm{Ker}(f) = \{a \in G : f(a) = 1\}$. Es inmediato que $\mathrm{Ker}(f)$ es un subgrupo normal de G. Vamos a denotar con $\ker(f)$ a la inclusión canónica de $\mathrm{Ker}(f)$ en G. Es facil ver que $\ker(f)$ tiene las siguientes propiedades:

1) $f \circ \ker(f) = 1$,
2) Si $g\colon H \to G$ satisface que la propiedad de que $f \circ g = 1$, entonces existe un único morfismo $g'\colon H \to \mathrm{Ker}(f)$ tal que $g = \ker(f) \circ g'$.

Esta última igualdad se expresa habitualmente diciendo que el triángulo



conmuta.

A la propiedad establecida arriba se la denomina *propiedad universal del núcleo.*

Algunos ejemplos. A continuación damos unos pocos ejemplos de núcleo de morfismos.

Ejemplo 1. El núcleo del determinante $\det\colon \mathrm{GL}(n,k) \to k^*$ es $\mathrm{SL}(n,k)$.

Ejemplo 2. El núcleo de la exponencial $x \mapsto e^{ix}$ es el conjunto $\{2\pi k\colon k \in \mathbb{Z}\}$.

Ejemplo 3. El núcleo del morfismo $\phi\colon \mathbb{C}^* \to \mathbb{R}_{>0}$, definido por $\phi(x) = |x|$, es el círculo unidad.

Proposición 1.10.2. *Si $f\colon G \to G'$ es un morfismo de grupos y $a, b \in G$, entonces $f(a) = f(b)$ si y sólo si $a\,\mathrm{Ker}(f) = b\,\mathrm{Ker}(f)$.*

Demostración. En efecto

$$f(a) = f(b) \Leftrightarrow ab^{-1} \in \mathrm{Ker}(f) \Leftrightarrow a\,\mathrm{Ker}(f) = b\,\mathrm{Ker}(f),$$

como afirmamos. □

Corolario 1.10.3. *Un morfismo $f\colon G \to G'$ de grupos es inyectivo si y sólo si su núcleo es* $\{1\}$.

1.11.Relaciones de equivalencia compatibles y cocientes de grupos. Consideremos una relación de equivalencia $\sim$ definida en un magma A. Denotemos con con $A/\!\sim$ al conjunto cociente de A por esta relación y con $\pi\colon A \to A/\!\sim$ a la sobreyección canónica, de manera de que $a \sim b$ si y sólo si $\pi(a) = \pi(b)$. Es fácil ver que $A/\!\sim$ tiene una estructura de magma tal que π es un morfismo si y sólo si

$$a \sim a' \text{ y } b \sim b' \text{ implica que } ab \sim a'b'$$

En este caso decimos que $\sim$ es una *relación de equivalencia compatible*. Notemos que si A es asociativo, entonces también $A/\sim$ lo es. En efecto tenemos

$$\pi(a)(\pi(b)\pi(c)) = \pi(a(bc)) = \pi((ab)c) = (\pi(a)\pi(b))\pi(c).$$

Algo completamente análogo sucede si A es conmutativo. Además, si A tiene neutro e, entonces $\pi(e)$ es el neutro de $A/\sim$ y π es un morfismo de magmas unitarios. Por último si a es inversible, entonces $\pi(a)$ también lo es y su inversa es $\pi(a^{-1})$. En particular si A es un monoide o un grupo, $A/\sim$ también lo es. Se pueden decir muchas cosas acerca de los cocientes de magmas y monoides por relaciones de equivalencia compatibles, pero casi todas son de caracter formal. Así que a partir de ahora vamos a concentranos en el caso de grupos, donde los resultados son más elegantes. Supongamos entonces que $\sim$ es una relación de equivalencia compatible definida en un grupo G. Denotemos con $\pi\colon G \to G/\sim$ al morfismo cociente y con H a $\mathrm{Ker}(\pi)$. Como ya hemos visto H es un subgrupo normal de G. Es claro que

$$a^{-1}b \in H \Leftrightarrow b \in aH \Leftrightarrow b \sim a \Leftrightarrow b \in Ha \Leftrightarrow ba^{-1} \in H,$$

de manera de que $\sim$ queda determinada por H y $\{b \in G : b \sim a\} = aH = Ha$ para todo $a \in H$. Recíprocamente si H es un subgrupo normal de G, entonces por la Proposición 1.6.11, las relaciones de equivalencias

$$b \sim a \Leftrightarrow ba^{-1} \in H \Leftrightarrow b \in Ha \quad \text{y} \quad b \sim' a \Leftrightarrow a^{-1}b \in H \Leftrightarrow a \in aH$$

coinciden y así son compatibles con la operación de G, ya que entonces

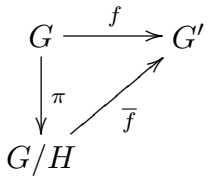
$$aHa'H = aa'HH = aa'H.$$

Dado un subgrupo normal H de G vamos a denotar con G/H al grupo cociente por la relación de equivalencia $\sim$ definida arriba, en lugar de usar la expresión $G/\sim$. A G/H lo llamaremos el *cociente* de G por H. Por ejemplo $\mathbb{Z}_n$ es el cociente de $\mathbb{Z}$ por $\langle n\rangle = n\mathbb{Z}$.

Proposición 1.11.1. *El morfismo canónico $\pi\colon G \to G/H$ tiene las siguientes propiedades:*

1) $\mathrm{Ker}(\pi) = H$,
2) *Si $f\colon G \to G'$ es un morfismo de grupos tal que $H \subseteq \mathrm{Ker}(f)$, entonces existe un único morfismo de grupos $\overline{f}\colon G/H \to G'$ tal que $f = \overline{f}\circ\pi$. Además $\mathrm{Ker}(\overline{f}) = \mathrm{Ker}(f)/H$ e $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f)$. En particular si H y $\mathrm{Ker}(f)$ coinciden, $\overline{f}$ es inyectiva y si f es sobreyectiva, $\overline{f}$ también lo es.*

La igualdad $f = \overline{f}\circ\pi$ se expresa habitualmente diciendo que el triángulo



conmuta.

Demostración. Por definición $\pi(a) = 1$ significa que $a \sim 1$ o, lo que es lo mismo, que $a = a1^{-1} \in H$. Esto prueba el item 1). Dado $a \in G$ denotemos con $\overline{a}$ a su clase en G/H. Para la primera parte del item 2) basta observar que si $a \sim b$ entonces $ab^{-1} \in H \subseteq \operatorname{Ker}(f)$ y así, $f(a) = f(b)$, lo que permite definir $\overline{f}(\overline{a})$ como $f(a)$. Dado que $\overline{a} = \pi(a)$, esto dice que $f = \overline{f} \circ \pi$. Además $\overline{f}$ es un morfismo de grupos ya que

$$\overline{f}(\overline{a}\,\overline{b}) = \overline{f}(\overline{ab}) = f(ab) = f(a)f(b) = \overline{f}(\overline{a})\overline{f}(\overline{b}).$$

Es claro de la definición que $\operatorname{Im}(\overline{f}) = \operatorname{Im}(f)$. Por último de que $\overline{f}(\overline{a}) = f(a)$ se sigue que $\overline{a} \in \operatorname{Ker}(\overline{f})$ si y sólo si $a \in \operatorname{Ker}(f)$, de donde

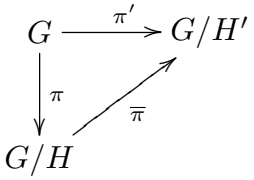
$$\operatorname{Ker}(\overline{f}) = \{aH : a \in \operatorname{Ker}(f)\} = \frac{\operatorname{Ker}(f)}{H}. \quad \square$$

La propiedad establecida en la proposición anterior se denomina *propiedad universal del cociente.*

Corolario 1.11.2. *Todo morfismo de grupos $f\colon G \to G'$ induce un isomorfismo $\overline{f}\colon G/\operatorname{Ker}(f) \to \operatorname{Im}(f)$.*

Observación 1.11.3. *Supongamos que H y L son subgrupos de un grupo G con H normal en G. Denotemos con $\bar{\imath}\colon L \to G/H$ a la composición de la inclusión canónica de L en G con el epimorfismo canónico $\pi\colon G \to G/H$. Claramente $\operatorname{Ker}(\bar{\imath}) = \operatorname{Ker}(\pi) \cap L = H \cap L$ e $\operatorname{Im}(\bar{\imath}) = HL/H$. Así, nuevamente por la proposición anterior, $\bar{\imath}$ induce un isomorfismo de $L/(H \cap L)$ en HL/H. En particular $H \cap L$ es un subgrupo normal de L.*

Observación 1.11.4. *Supongamos que H y H' son subgrupos normales de un grupo G y que $H \subseteq H'$. Donotemos con $\pi\colon G \to G/H$ y con $\pi'\colon G \to G/H'$ a los epimorfismos canónicos. Por la proposición anterior existe un único morfismo $\overline{\pi}\colon G/H \to G/H'$ tal que el diagrama*



conmuta y además $\overline{\pi}$ es sobreyectiva y su núcleo es H'/H. Así H'/H es un subgrupo normal de G/H y, nuevamente por la proposición anterior, $\overline{\pi}$ induce un isomorfismo de $\frac{G/H}{H'/H}$ en G/H'. En otras palabra, si tenemos dos subgrupos normales H y H' de un grupo G y $H \subseteq H'$, da lo mismo dividir primero G por H y luego G/H por su subgrupo normal H'/H, que dividir directamente G por H'.

Al corolario y a las dos observaciones anteriores se las conoce como primero, segundo y tercer teorema de isomorfismo de Noether, respectivamente.

Teorema 1.11.5. *Si $f\colon G \to G'$ es un morfismo de grupos, entonces*

$$|G| = |\operatorname{Im}(f)||\operatorname{Ker}(f)|.$$

Demostración. Por el Teorema de Lagrange $|G| = |G : \operatorname{Ker}(f)||\operatorname{Ker}(f)|$. Así, por el Corolario 1.11.2, $|G| = |\operatorname{Im}(f)||\operatorname{Ker}(f)|$, como afirmamos. $\square$

Observación 1.11.6. *Si $f\colon G \to G'$ es un morfismo de grupos, entonces por el teorema de Lagrange, $|\operatorname{Im}(f)|$ divide a $|G'|$ y, por el Teorema 1.11.5, $|\operatorname{Im}(f)|$ divide a $|G|$. Así, si G y G' son finitos, $|\operatorname{Im}(f)|$ divide a $\operatorname{mdc}(|G|, |G'|)$, donde $\operatorname{mdc}(|G|, |G'|)$ denota al máximo de los divisores comunes de $|G|$ y $|G'|$. En consecuencia si $|G|$ y $|G'|$ son coprimos, entonces f es trivial. Por ejemplo si G es un subgrupo de orden impar de S_n y $\pi\colon G \to \{\pm 1\}$ es el morfismo signo, entonces f es trivial y, por lo tanto, $G \subseteq A_n$. En particular si $x \in \mathrm{S}_n$ tiene orden impar, entonces tiene signo par.*

Vamos a ver ahora que para cada morfismo de grupos $f\colon G \to G'$ hay una biyección entre el conjunto $S(G)$ de los subgrupos de G que contienen a $\operatorname{Ker}(f)$ y el conjunto $S(G')$ de los subgrupos de G' que están incluídos en $\operatorname{Im}(f)$.

Observación 1.11.7. *Vale lo siguiente:*

1) *$f(H) \in S(G')$, para cada subgrupo H de G (en particular $\operatorname{Im}(f)$ es un subgrupo de G'). Además si H es un subgrupo invariante de G, entonces $f(H)$ es un subgrupo invariante de $\operatorname{Im}(f)$.*
2) *$f^{-1}(H') \in S(G)$, para cada subgrupo H' de G'. Además si H' es un subgrupo invariante de $\operatorname{Im}(f)$, entonces $f^{-1}(H')$ es un subgrupo invariante de G.*

Dado que cualesquiera sean $H \subseteq G$ y $H' \subseteq G'$ vale que

$$f^{-1}(f(H)) = H \operatorname{Ker}(f) \quad y \quad f(f^{-1}(H')) = H' \cap \operatorname{Im}(f),$$

queda determinada una biyección entre $S(G)$ y $S(G')$ y también entre los subconjuntos de $S(G)$ y $S(G')$ formados por los subgrupos normales de G y por los subgrupos normales de $\operatorname{Im}(f)$, respectivamente. Además si $\operatorname{Ker}(f) \subseteq H \subseteq G$, entonces

$$f(H) \simeq \frac{H}{\operatorname{Ker}(f)} \quad y \quad |f(G) : f(H)| = |G : H|.$$

En efecto, para esto último es suficiente ver que la aplicación $aH \mapsto f(a)f(H)$ es una biyección del conjunto de coclases a izquierda de H en G en el conjunto de coclases a izquierda de $f(H)$ en $f(G)$. Es claro que esta aplicación es sobreyectiva. Para ver que también es inyectiva basta notar que de $f(a)f(H) = f(b)f(H)$ se sigue que $f(a^{-1}b) = f(a^{-1})f(b) \in f(H)$, de donde $a^{-1}b \in H \operatorname{Ker}(f) = H$, lo que implica que $aH = bH$. Por último si H es un subgrupo normal de G, entonces $f(H)$ es un subgrupo normal de $f(G)$ y

$$\frac{f(G)}{f(H)} \simeq \frac{G/\operatorname{Ker}(f)}{H/\operatorname{Ker}(f)} \simeq \frac{G}{H}.$$

Definición y Observación 1.11.8. *Un grupo es simple si no tiene subgrupos normales distintos de los triviales. Un subgrupo normal H de un grupo G es maximal si $H \neq G$ y no existe ningún subgrupo normal L de G tal que $H \subsetneq L \subsetneq G$. Es claro que un subgrupo normal H de un grupo G es maximal si y sólo si G/H es simple.*

Ejercicio 9. *Pruebe que si $\pi\colon G \to G'$ es un morfismo sobreyectivo de grupos y H es un subgrupo normal de G, entonces $\pi(H)$ es un subgrupo normal de G' y $G/(H\operatorname{Ker}(\pi)) \simeq G'/\pi(H)$.*

Supongamos ahora que $f\colon G \to G'$ es un morfismo de grupos y que H y H' son subgrupos normales de G y G' respectivamente. Denotemos con $\pi\colon G \to G/H$ y $\pi'\colon G' \to G'/H'$ a los epimorfismos canónicos. Si $f(H) \subseteq H'$, entonces $\pi'(f(a)) = 1$ para todo $a \in H$. Por la propiedad universal del cociente queda definido un único morfismo $\overline{f}\colon G/H \to G'/H'$ tal que $\overline{f}\circ\pi = \pi'\circ f$. Esta igualdad se expresa también diciendo que el cuadrado

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

conmuta. Además $\operatorname{Im}(\overline{f}) = \pi'(\operatorname{Im}(f)) = \operatorname{Im}(f)H'/H'$ y $\operatorname{Ker}(\overline{f}) = f^{-1}(H')/H$. En efecto, todo esto se sigue del item 2) de la Proposición 1.11.1, aplicada a $\pi'\circ f$ y de que $\operatorname{Im}(\pi'\circ f) = \pi'(\operatorname{Im}(f))$ y $\operatorname{Ker}(\pi'\circ f) = f^{-1}(H')$.

Observación 1.11.9. *Vale lo siguiente:*

1) *Si H es un subgrupo normal de un grupo G, entonces $\overline{\mathrm{id}_G}$ es igual a $\mathrm{id}_{G/H}$.*
2) *Supongamos que $f\colon G \to G'$ y $f'\colon G' \to G''$ son morfismos de grupos y que H, H' y H'' son subgrupos normales de G, G' y G'' respectivamente. Si $f(H) \subseteq H'$ y $f'(H') \subseteq H''$, entonces $f'(f(H)) \subseteq H''$ y $\overline{f'\circ f} = \overline{f'}\circ\overline{f}$.*

Demostración. 1) se sigue de la unicidad del morfismo $\overline{\mathrm{id}_G}$ y de que el diagrama

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

conmuta y 2) es consecuencia de la unicidad del morfismo $\overline{f'\circ f}$ y de que el rectángulo exterior del diagrama

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

conmuta. □

Ejercicio 10. *Pruebe que si $f\colon G \to G'$ es un morfismo de grupos y H' es un subgrupo normal de G', entonces $f^{-1}(H')$ es un subgrupo normal de G y existe un único morfismo inyectivo $\overline{f}\colon G/f^{-1}(H') \to G'/H'$ de grupos, tal que el diagrama*

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

donde $\pi\colon G \to G/f^{-1}(H')$ *y* $\pi'\colon G' \to G'/H'$ *son las proyecciones canónicas, conmuta y que además* $\mathrm{Im}(\overline{f}) = \pi'(\mathrm{Im}(f)) = \mathrm{Im}(f)H'/H'$.

1.12.Grupos libres. Presentaciones por generadores y relaciones. Dado un conjunto X denotemos 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* es una expresión

$$w = x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n} \qquad (\epsilon_i = \pm 1,\, i = 1, \ldots, n).$$

Si en esta expresión ningún símbolo x^{+1} está junto a su asociado x^{-1}, decimos que w es una palabra *reducida*. Al número n que aparece en la expresión de w lo llanaremos la longitud $l(w)$ de w. Consideramos también como una palabra reducida a la expresión vacía. Por definición esta palabra tiene longitud cero. A continuación definimos 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

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

Si esta es una palabra reducida, declaramos que (*) es w_1w_2. Si no eliminamos de (*) sucesivamente pares de símbolos asociados hasta obtener una palabra reducida. Es claro que la palabra vacía es el elemento neutro para este producto. Afirmamos que el conjunto de la palabras reducidas forma un grupo que llamaremos *grupo libre* $L(X)$ *generado por* X. Veamos que $w_1(w_2w_3) = (w_1w_2)w_3$ para toda terna w_1, w_2, w_3 de palabras reducidas. Demostraremos esto por inducción en $l(w_2)$. Supongamos primero que $l(w_2) = 1$, es decir que $w_2 = x_\alpha^\epsilon$ con $\epsilon = \pm 1$. 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_α^ϵ; que el último símbolo de w_1 sea igual al elemento de $X^{\pm 1}$ asociado a x_α^ϵ, pero que el primero de w_3 no lo sea; que el primer símbolo de w_3 sea igual al elemento de $X^{\pm 1}$ asociado a x_α^ϵ, pero que el último de w_1 no lo sea; y que el último símbolo que w_1 y el primero de w_3 sean iguales al elemento de $X^{\pm 1}$ asociado a x_α^ϵ. Es fácil ver que en todos estos casos vale que $w_1(w_2w_3) = (w_1w_2)w_3$. Supongamos ahora que la asociatividad vale cuando $l(w_2) \leq n$ y que $l(w_2) = n + 1$. Escribamos $w_2 = w_2'x_\alpha^\epsilon$. Entonces, por hipótesis inductiva

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

Resta ver que cada palabra reducida tiene inversa, pero es claro que el inverso de la palabra reducida $x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n}$ es la palabra reducida $x_{\alpha_n}^{-\epsilon_n} \cdots x_{\alpha_1}^{-\epsilon_1}$, donde $-\epsilon_i = -1$ si $\epsilon_1 = 1$ y $-\epsilon_i = +1$ si $\epsilon_1 = -1$. Dado que toda palabra en $L(X)$ es un producto de

símbolos de $X^{\pm 1}$ tenemos que X genera efectivamente a $L(X)$. Definimos el *rango* $r(L(X))$ de $L(X)$ como el cardinal de X. Es claro que si dos conjuntos X e Y son biyectivos, entonces $L(X) \simeq L(Y)$ y que el grupo libre de rango 1 es un grupo cíclico infinito. Por otra parte un grupo libre $L(X)$ de rango mayor que 1 no es conmutativo ya que si x, y son elementos distintos de X, entonces $x^{+1}y^{+1} \neq y^{+1}x^{+1}$. Nosotros vamos a identificar cada $x \in X$ con su correspondiente elemento $x^{+1} \in X^{+1}$. Así, de ahora en más consideramos que $X = X^{+1} \subseteq L(X)$. El grupo libre $L(X)$ satisface la siguiente propiedad (que se denomina propiedad universal del grupo libre):

> Si $f\colon X \to G$ es una función de X en un grupo G, existe un único morfismo de grupos $\widetilde{f}\colon L(X) \to G$ que extiende a f.

En efecto para que $\widetilde{f}$ sea un morfismo de grupos que extienda a f debe ser

$$\widetilde{f}(x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n}) = f(x_{\alpha_1})^{\epsilon_1} \cdots f(x_{\alpha_n})^{\epsilon_n}.$$

Es inmediato que con esta definición $\widetilde{f}$ un morfismo de grupos.

Observación 1.12.1. *Supongamos X es un conjunto de generadores de un grupo G. Por la propiedad universal del grupo libre la inclusión canónica de $i\colon X \to G$ se extiende a un morfismo sobreyectivo $\widetilde{i}\colon L(X) \to G$ y así, por el primer teorema de isomorfismo de Noether $G \simeq L(X)/H$, donde $H = \mathrm{Ker}(\widetilde{i})$. En particular un grupo G generado por un conjunto X es un cociente de un grupo libre de rango igual al cardinal de X. Notemos que H consiste de las expresiones formales $x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n}$ en $L(X)$ tales que su producto $x_{\alpha_1}^{\epsilon_1} \cdots x_{\alpha_n}^{\epsilon_n}$ en G es 1. A H se lo llama el conjunto de las relaciones que satisfacen los elementos de X. Tomemos una famila R, de elementos de H, tal que H es el subgrupo normal de $L(X)$ generado por R. Todos los elementos de H se obtienen de R, ya que se pueden expresar como productos de potencias de los elementos de R y de sus conjugados. En consecuencia el grupo G queda completamente determinado por X y R, lo que suele expresarse diciendo que G es el grupo generado por X sujeto a las relaciones R. Notemos que recíprocamente, dado un conjunto X cualquiera y una familia R, de elementos de $L(X)$, obtenemos un grupo G generado por X sujeto a las relaciones R, tomando $G = L(X)/\overline{\langle R \rangle}$, donde $\overline{\langle R \rangle}$ denota al subgrupo normal de $L(X)$ generado por R.*

Ejemplo 1. $\mathbb{Z}$ es el grupo generado por un elemento x sin relaciones.

Ejemplo 2. Veamos que $\mathbb{Z}_n$ es el grupo generado por x sujeto a las relación $x^n = 1$. Consideremos la aplicación $i\colon L(\{x\}) \to \mathbb{Z}_n$, definida por $i(x) = 1$. Debido a que $i(x^n) = 0$ queda inducido un morfismo

$$\bar{i}\colon \frac{L(\{x\})}{\overline{\langle x^n \rangle}} \to \mathbb{Z}_n,$$

que es claramente sobreyectivo. Denotemos con $\overline{x}$ a la clase de x en $\frac{L(\{x\})}{\overline{\langle x^n \rangle}}$. De las igualdad $\overline{x}^n = 1$ se sigue facilmente que

$$\frac{L(\{x\})}{\overline{\langle x^n \rangle}} = \{1, \overline{x}, \ldots, \overline{x}^{n-1}\},$$

de donde en particular, $\left|\frac{L(\{x\})}{\overline{\langle x^n \rangle}}\right| \leq n$. Dado que $|\mathbb{Z}_n| = n$ esto prueba que $\bar{i}$ es un isomorfismo.

Ejemplo 3. Veamos que $\mathbb{Z}_n \oplus \mathbb{Z}_m$ es el grupo generado por x, y sujeto a las relaciones $x^n = 1$, $y^m = 1$ y $yxy^{-1}x^{-1} = 1$. Consideremos la aplicación

$$i\colon L(\{x,y\}) \to \mathbb{Z}_n \oplus \mathbb{Z}_m$$

definida por $i(x) = (1,0)$ e $i(y) = (0,1)$. Como $i(x^n) = (0,0)$, $i(y^m) = (0,0)$ e $i(yxy^{-1}x^{-1}) = (0,0)$ queda inducido un morfismo

$$\bar{i}\colon \frac{L(\{x,y\})}{\langle x^n, y^m, yxy^{-1}x^{-1}\rangle} \to \mathbb{Z}_n \oplus \mathbb{Z}_m,$$

que es claramente sobreyectivo. Denotemos con $\overline{x}$ e $\overline{y}$ a las clases de x e y en $\frac{L(\{x,y\})}{\langle x^n, y^m, yxy^{-1}x^{-1}\rangle}$, respectivamente. Usando las igualdades $\overline{x}^n = 1$, $\overline{y}^m = 1$ y $\overline{y}\,\overline{x}\,\overline{y}^{-1}\,\overline{x}^{-1} = 1$ se ve facilmente que

$$\frac{L(\{x,y\})}{\langle x^n, y^m, yxy^{-1}x^{-1}\rangle} = \{\overline{x}^i\overline{y}^j : 0 \le i < n \text{ y } 0 \le j < m\},$$

de donde en particular, $\left|\frac{L(\{x,y\})}{\langle x^n, y^m, yxy^{-1}x^{-1}\rangle}\right| \le nm$. Dado que $|\mathbb{Z}_n \oplus \mathbb{Z}_m| = nm$ esto prueba que $\bar{i}$ es un isomorfismo.

Ejemplo 4. Veamos que D_n es el grupo generado por x, y sujeto a las relaciones $x^n = 1$, $y^2 = 1$ y $yxy^{-1}x = 1$. Consideremos el morfismo $i\colon L(\{x,y\}) \to \mathrm{GL}(2,\mathbb{R})$ definido por $i(x) = a$ e $i(y) = b$, donde a y b son

$$a = \begin{pmatrix} \cos\theta & \operatorname{sen}\theta \\ -\operatorname{sen}\theta & \cos\theta \end{pmatrix} \qquad \text{y} \qquad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Como $i(x^n) = a^n = 1$, $i(y^2) = b^2 = 1$ e $i(yxy^{-1}x) = bab^{-1}a = 1$ queda inducido un morfismo

$$\bar{i}\colon \frac{L(\{x,y\})}{\langle x^n, y^2, yxy^{-1}x\rangle} \to D_n,$$

que es claramente sobreyectivo. Denotemos con $\overline{x}$ e $\overline{y}$ a las clases de x e y en $\frac{L(\{x,y\})}{\langle x^n, y^2, yxy^{-1}x\rangle}$, respectivamente. De las igualdades $\overline{x}^n = 1$, $\overline{y}^2 = 1$ y $\overline{y}\,\overline{x}\,\overline{y}^{-1}\,\overline{x} = 1$ se sigue facilmente que

$$\frac{L(\{x,y\})}{\langle x^n, y^2, yxy^{-1}x\rangle} = \{1, \overline{x}, \ldots, \overline{x}^{n-1}, \overline{y}, \overline{x}\,\overline{y}, \ldots, \overline{x}^{n-1}\overline{y}\},$$

de donde en particular, $\left|\frac{L(\{x,y\})}{\langle x^n, y^2, yxy^{-1}x\rangle}\right| \le 2n$. Dado que $|D_n| = 2n$ esto prueba que $\bar{i}$ es un isomorfismo.

Ejemplo 5. Veamos que H_n es el grupo generado por x, y sujeto a las relaciones $x^n y^{-2} = 1$ y $yxy^{-1}x = 1$. Consideremos el morfismo $i\colon L(\{x,y\}) \to \mathrm{GL}(2,\mathbb{C})$ definido por $i(x) = a$ e $i(y) = b$, donde a y b son

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

Como $i(x^n y^{-2}) = a^n b^{-2} = 1$ e $i(yxy^{-1}x) = bab^{-1}a = 1$ queda inducido un morfismo

$$\bar{i}\colon \frac{L(\{x,y\})}{\overline{\langle x^n y^{-2}, yxy^{-1}x\rangle}} \to H_n,$$

que es claramente sobreyectivo. Denotemos con $\overline{x}$ e $\overline{y}$ a las clases de x e y en $\frac{L(\{x,y\})}{\overline{\langle x^n y^{-2}, yxy^{-1}x\rangle}}$, respectivamente. De las igualdades $\overline{x}^n\overline{y}^{-2} = 1$ y $\overline{yxy}^{-1}\overline{x} = 1$ se sigue que $\overline{x}^{2n} = \overline{y}^4 = 1$, de donde

$$\frac{L(\{x,y\})}{\overline{\langle x^n y^{-2}, yxy^{-1}x\rangle}} = \{1, \overline{x}, \ldots, \overline{x}^{2n-1}, \overline{y}, \overline{x}\,\overline{y}, \ldots, \overline{x}^{2n-1}\overline{y}\},$$

Esto muestra en particular que $\left|\frac{L(\{x,y\})}{\overline{\langle x^n y^{-2}, yxy^{-1}x\rangle}}\right| \leq 4n$ y así, dado que $|H_n| = 4n$, el morfismo $\bar{i}$ es biyectivo.

A continuación mostramos como puede ser usada la noción de presentación de un grupo por generadores y relaciones.

Ejemplo 1. Supongamos que estamos en la situación del Ejemplo 4) de arriba. Entonces para todo divisor r de n el subgrupo $\langle a^r\rangle$ de D_n es normal. En efecto, dado que a e b son generadores de D_n, para comprobar esto basta ver que

$$a\langle a^r\rangle a^{-1} \subseteq \langle a^r\rangle \qquad \text{y} \qquad b\langle a^r\rangle b^{-1} \subseteq \langle a^r\rangle.$$

Lo primero es obvio y lo segundo se sigue de que

$$ba^{rj}b^{-1} = (bab^{-1})^{rj} = (a^{-1})^{rj} = a^{-rj}.$$

Es claro también que el orden de $\langle a^r\rangle$ es n/r y así, $D_n/\langle a^r\rangle$ es un grupo de orden $2r$ que está generado por las clases $\overline{a}$ e $\overline{b}$ de a e b en $D_n/\langle a^r\rangle$. Afirmamos que $D_n/\langle a^r\rangle \simeq D_r$. Consideremos el morfismo $i\colon L(\{x,y\}) \to D_n/\langle a^r\rangle$ definido por $i(x) = \overline{a}$ e $i(y) = \overline{b}$. Como $\overline{b}^2 = 1$, $\overline{a}^r = 1$ (pues $a^r \in \langle a^r\rangle$) y $\overline{b}\,\overline{a}\,\overline{b}^{-1} = \overline{a}^{-1}$, queda inducido un morfismo

$$\bar{i}\colon \frac{L(\{x,y\})}{\overline{\langle x^r, y^2, yxy^{-1}x\rangle}} \to \frac{D_n}{\langle a^r\rangle},$$

que es claramente sobreyectivo. Dado que

$$|D_r| = 2r = |D_n/\langle a^r\rangle| \qquad \text{y} \qquad D_r \simeq \frac{L(\{x,y\})}{\overline{\langle x^r, y^2, yxy^{-1}x\rangle}},$$

este morfismo también es inyectivo, y así, $D_n/\langle x^r\rangle \simeq D_r$.

Ejemplo 2. Supongamos ahora que estamos en la situación del Ejemplo 5) de arriba. El mismo argumento que en el Ejemplo 1) muestra que para todo divisor r de n el subgrupo $\langle a^r\rangle$ de H_n es normal y que $H_n/\langle a^r\rangle \simeq D_r$. Además las clases $\overline{a}$ y $\overline{b}$ de a e b en $H_n/\langle a^r\rangle$ forman un conjunto de generadores de $H_n/\langle a^r\rangle$ que satisfacen $\overline{a}^r = 1$, $\overline{b}^2 = 1$ y $\overline{a}\,\overline{b}\,\overline{a}^{-1}\,\overline{b}^{-1} = 1$.

Observación 1.12.2 (Descripción de conjuntos de homomorfismos). *Por definición, para cada conjunto X y cada grupo G, la aplicación*

$$\theta\colon \mathrm{Hom}(L(X),G) \to \{(a_x)_{x\in X} : a_x \in G \text{ para todo } x \in X\},$$

definida por $\theta(f) = (f(x))_{x\in X}$, es biyectiva. Por ejemplo si $\langle g\rangle$ es un grupo cíclico infinito, entonces

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

es la biyección definida por $\theta(f) = f(g)$. Por la propiedad universal del cociente de grupos se obtiene ahora que si $R = (r_i)_{i\in I}$ es una familia de elementos de $L(X)$, entonces la aplicación

$$\theta\colon \mathrm{Hom}(L(X)/\overline{\langle R\rangle}, G) \to \{(a_x)_{x\in X} : a_x \in G \text{ para todo } x \in X\},$$

definida por $\theta(f) = (f(x))_{x\in X}$ es una inyección cuya imagen es

$$\{(a_x)_{x\in X} : a_x \in G \text{ para todo } x \in X \text{ y } s_i = 1 \text{ para todo } i \in I\},$$

donde s_i denota al elemento de G obtenido reemplazando en r_i cada $x \in X$ por a_x. Por ejemplo si $\langle g\rangle$ es un grupo cíclico de orden n, entonces

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

es una inyección cuya imagen es $\{a \in G : a^n = 1\}$. Similarmente tenemos biyecciones

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

y

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

Teorema 1.12.3. *Si G es un grupo finito y si $a, b \in G$ tienen orden 2, entonces $\langle a,b\rangle \simeq D_n$, donde n es el orden de ab.*

Demostración. Escribamos $s = ab$. Por defnción $asa^{-1}s = aaba^{-1}ab = a^2b^2 = 1$. Así, como $\langle a,b\rangle = \langle a,s\rangle$, sólo hay que probar que $|\langle a,b\rangle| = 2n$. Afirmamos que $as^i \neq 1$ para todo $i \geq 0$. Supongamos que esto es falso y tomemos el mínimo $i \geq 0$ tal que $as^i = 1$. Como $a \neq 1$ y $as = aab = b \neq 1$ debe ser $i \geq 2$. Pero por definición $bs^{i-1} = aabs^{i-1} = as^i = 1$, de donde $s^{i-1}b = b(bs^{i-1})b = 1$, lo que a su vez implica que $as^{i-2} = as^{i-2}a^2 = as^{i-2}ab^2a = as^{i-1}ba = a^2 = 1$, contradiciendo la minimalidad de i. Se sigue de esto que $as^i \neq s^j$ para todo $i, j \geq 0$, de donde $\langle a,b\rangle$ contiene a la unión disjunta de $\langle s\rangle$ y $a\langle s\rangle$ y, en consecuencia, $|\langle a,b\rangle| \geq 2n$. Para probar la desigualdad contraria es suficiente ver que $\langle s\rangle \cup a\langle s\rangle$ es un grupo, lo que se sigue de que $s^is^j = s^{i+j}$, $as^is^j = as^{i+j}$, $as^ias^j = s^{j-i}$ y $s^ias^j = a^2s^ias^j = as^{j-i}$. $\square$

1.13.Automorfismos interiores y subgrupos característicos. A cada elemento a de un grupo G se le puede asignar una función $\Phi_a\colon G \to G$, definida por $\Phi_a(b) = aba^{-1}$. Es fácil ver Φ_a es un automorfismo de G y que la asignación $G \to \mathrm{Aut}(G)$ que manda a en Φ_a es un morfismo de grupos. En efecto, lo primero se sigue de que

$$\Phi_a(bc) = abca^{-1} = (aba^{-1})(aca^{-1}) = \Phi_a(b)\Phi_a(c)$$

y lo segundo de que

$$\Phi_{ab}(c) = abc(ab)^{-1} = a(bcb^{-1})a^{-1} = \Phi_a(\Phi_b(c)).$$

Notemos que a está en el núcleo del morfismo $G \to \mathrm{Aut}(G)$ que acabamos de definir si y sólo si $aba^{-1} = \Phi_a(b) = b$ para todo $b \in G$. Dado que $aba^{-1} = b$ equivale a $ab = ba$ es natural decir definir el centro $\mathrm{Z}(G)$ de G como este núcleo y decir que $b \in G$ es *central* si pertenece a $\mathrm{Z}(G)$. A la imagen del morfismo $G \to \mathrm{Aut}(G)$ la denotamos $\mathrm{Int}(G)$ y a sus elementos *automorfismos interiores* de G. Decimos que dos elementos a e b de un grupo G son conjugados si existe $c \in G$ tal que $b = cac^{-1}$, es decir si $b = \Phi_c(a)$. En particular los ordenes de dos elementos conjugados coinciden. La relación definida por $a \sim b$ si y sólo si a e b son conjugados es claramente de equivalencia, de manera que G queda partido en clases, llamadas *clases de conjugación*. Es evidente que si a y b son elementos arbitrarios de un grupo G, entonces ab es conjugado de ba, ya que $ba = a^{-1}(ab)a$. Recíprocamente, si a y b son conjugados y $b = cac^{-1} = c(ac^{-1})$, entonces $(ac^{-1})c = a$. Practicamente por definición un subgrupo H de G es normal si y sólo si $\Phi_a(H) \subseteq H$ para todo $a \in G$ (en otras palabras si con cada elemento a de G contiene a su clase de conjugación). Es fácil ver que entonces $\Phi_a(H) = H$ para todo $a \in G$, ya que de $a^{-1}Ha = \Phi_{a^{-1}}(H) \subseteq H$ se sigue que $H \subseteq aHa^{-1} = \Phi_a(H)$. Decimos que H es un subgrupo *característico* de G si $\varphi(H) \subseteq H$ para todo $\varphi \in \mathrm{Aut}(G)$. Claramente $\varphi(H) = H$ para todo $\varphi \in \mathrm{Aut}(G)$, ya que de $\varphi^{-1}(H) \subseteq H$ se sigue que $H \subseteq \varphi(H)$. Evidentemente todo subgrupo característico es normal. Afirmamos que $\mathrm{Z}(G)$ es un subgrupo característico de G (claramente es normal ya que es el núcleo de un morfismo). Debemos ver que si $a \in \mathrm{Z}(G)$ y $g \in \mathrm{Aut}(G)$, entonces $g(a) \in \mathrm{Z}(G)$, pero

$$g(b)a = g(b)g(g^{-1}(a)) = g(bg^{-1}(a)) = g(g^{-1}(a)b) = g(g^{-1}(a))g(b) = ag(b),$$

para todo $b \in G$. Veamos por último que $\mathrm{Int}(G)$ es un subgrupo normal de $\mathrm{Aut}(G)$. En efecto si $a \in G$ y $g \in \mathrm{Aut}(G)$, entonces $g \circ \Phi_a \circ g^{-1} = \Phi_{g(a)}$, ya que

$$(g \circ \Phi_a \circ g^{-1})(b) = g(\Phi_a(g^{-1}(b))) = g(ag^{-1}(b)a^{-1}) = g(a)bg(a)^{-1} = \Phi_{g(a)}(b),$$

para todo $b \in G$. Al cociente $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Int}(G)$ se lo llama el grupo de los *automorfismos exteriores* de G (notemos que sus elementos no son automorfismos de G sino clases de automorfismos). Por todo lo que acabamos de probar la sucesión de morfismos

$$1 \longrightarrow \mathrm{Z}(G) \longrightarrow G \longrightarrow \mathrm{Aut}(G) \longrightarrow \mathrm{Out}(G) \longrightarrow 1$$

tiene la peculiaridad de que la imagen de cada uno de sus morfismos es igual al núcleo del morfismo siguiente. Esto se expresa diciendo que dicha sucesión es *exacta*.

Ejemplo. A continuación calculamos el centro de los grupos diedrales y cuaterniónicos. Recordemos que D_n es el grupo generado por a, b sujeto a las relaciones $a^n = 1$, $b^2 = 1$ y $bab^{-1}a = 1$ y que $D_n = \{1, a, \dots, a^{n-1}, b, ab, \dots, a^{n-1}b\}$. Es claro que D_2 es conmutativo. Consideremos el caso $n > 2$. Entonces $a^2 \neq 1$ y así de $a(a^ib)a^{-1} = a^{i+2}b$ se sigue que $a^ib \notin \mathrm{Z}(D_n)$. Dado que $ba^ib^{-1} = a^{-i}$ y que a^i claramente conmuta con a tenemos que $a^i \in \mathrm{Z}(D_n)$ si y sólo si $i = 0$ o $i = n/2$. Así, para todo $m \geq 2$ vale que $\mathrm{Z}(D_{2m-1}) = \{1\}$ y $\mathrm{Z}(D_{2m}) = \{1, a^m\}$. Recordemos ahora que H_n es el grupo generado por a, b, sujeto a las relaciones $a^nb^{-2} = 1$ y $bab^{-1}a = 1$ y que $H_n = \{1, a, \dots, a^{2n-1}, b, ab, \dots, a^{2n-1}b\}$. De la igualdad $a(a^ib)a^{-1} = a^{i+2}b$ se sigue que $a^ib \notin \mathrm{Z}(H_n)$. Dado que $ba^ib^{-1} = a^{-i}$ y que a^i claramente conmuta con a tenemos que $a^i \in \mathrm{Z}(H_n)$ si y sólo si $i = 0$ o $i = n$ y así, $\mathrm{Z}(H_n) = \{1, a^n\}$.

Ejercicio 11. *Muestre que si $g\colon G \to G$ es un endomorfismo de grupos, entonces no necesariamente $g(\mathrm{Z}(G)) \subseteq \mathrm{Z}(G)$.*

Ejercicio 12. *Pruebe que si $g\colon G \to G'$ es un morfismo sobreyectivo de grupos, entonces $g(\mathrm{Z}(G)) \subseteq \mathrm{Z}(G')$.*

Proposición 1.13.1. *Si G no es abeliano, entonces $G/\mathrm{Z}(G)$ no es cíclico.*

Demostración. Si $G/\mathrm{Z}(G)$ fuera cíclico, entonces existiría $a \in G \setminus \mathrm{Z}(G)$ tal que $G = \langle a \rangle \mathrm{Z}(G)$. Dado que para todo $b, b' \in \mathrm{Z}(G)$ y todo $\alpha, \alpha' \in \mathbb{Z}$,

$$(a^\alpha b)(a^{\alpha'} b') = a^\alpha a^{\alpha'} bb' = a^{\alpha'} a^\alpha b'b = (a^{\alpha'} b')(a^\alpha b),$$

esto es absurdo. □

Observación 1.13.2. *Puede ocurrir que $H \subseteq L \subseteq G$ sea una cadena de subgrupos con H normal en L y L normal en G, pero que H no sea normal en G. Para un ejemplo podemos tomar como G al grupo S_4 de permutaciones de $\{1, 2, 3, 4\}$, como L a $\{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$, donde σ_1, σ_2 y σ_3 son las permutaciones definidas por*

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

y como H a $\{\mathrm{id}, \sigma_1\}$. Afirmamos que esto no sucede si H es un subgrupo característico de L. En efecto, tomemos $a \in G$. Debemos ver que $\Phi_a(H) = H$. Como L es normal en G, el automorfismo interior Φ_a de G define por restricción un automorfismo (no necesariamente interior) de L y así, dado que H es un subgrupo característico de L, vale que $\Phi_a(H) = H$. 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 un automorfismo interior Φ_a de G hay que considerar un automorfismo arbitrario.

Observación 1.13.3. *Decimos que un subgrupo H de un grupo G es completamente normal si $\varphi(H) \subseteq H$ para todo $\varphi \in \mathrm{End}(G)$. Claramente todo subgrupo completamente normal de G es característico. Por el Ejercicio 11 el centro de G, que siempre es característico, no siempre es completamente invariante. Vale lo siguiente: 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 la misma que la desarrollada en la observación anterir, pero considerando un endomorfismo de G en lugar de Φ_a.*

Ejercicio 13. *Pruebe que si H es un subgrupo normal de un grupo finito G y $|H|$ y $|G:H|$ son coprimos, entonces H es un subgrupo completamente normal de G.*

Ejercicio 14. *Supongamos que $H \subseteq L$ son subgrupos de un grupo G y que H es característico en G. Pruebe que si L/H es característico en G/H, entonces L es característico en G.*

Ejercicio 15. *Supongamos que $H \subseteq L$ son subgrupos de un grupo G y que H es completamente normal en G. Pruebe que si L/H es completamente normal en G/H, entonces L es completamente normal en G.*

Subgrupo conmutador y abelianizado. Dado un grupo G denotamos con $[G,G]$ al subgrupo de G generado por todos lo conmutadores $[a,b] := aba^{-1}b^{-1}$ con $a,b \in G$. A $[G,G]$ se lo llama *subgrupo conmutador* de G. Si $f\colon G \to G'$ es un morfismo de grupos, entonces claramente $f([a,b]) = [f(a),f(b)]$, de modo de que $f([G,G]) \subseteq [G',G']$. En particular tomando $G' = G$ deducimos que $[G,G]$ es un subgrupo completamente normal de G. Además $G/[G,G]$ es conmutativo ya que $ab = [a,b]ba$. En consecuencia si H es un subgrupo de G que contiene a $[G,G]$, entonces H es invariante y G/H es conmutativo. Recíprocamente supongamos que H es un subgrupo invariante de G y que G/H es conmutativo. Entonces de $ab \equiv ba \pmod{H}$ se sigue que $[a,b] = aba^{-1}b^{-1} \in H$ y, así $[G,G] \subseteq H$. Una consecuencia particular de todo esto es que $[G,G] = \{1\}$ si y sólo si G es conmutativo (lo que por otra parte es obvio). Por la propiedad universal del cociente, si f es un morfismo de G en un grupo conmutativo G', entonces existe un único morfismo f' de $G/[G,G]$ en G' tal que el diagrama

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

donde π denota al epimorfismo canónico, conmuta. A $G/[G,G]$ se lo llama el *abelianizado* de G y a la propiedad mencionada recién *propiedad universal del abelianizado* de G. Por el comentario que precede a la Observación 1.11.9, dado un morfismo de grupos $f\colon G \to G'$ existe un único morfismo $\overline{f}\colon \frac{G}{[G,G]} \to \frac{G'}{[G',G']}$ tal que el diagrama

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & G' \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ G/[G,G] & \xrightarrow{\ \overline{f}\ } & G'/[G',G'] \end{array}$$

donde π y π' denotan a los epimorfismo canónicos, conmuta. Por último vale que $\overline{\mathrm{id}_G} = \mathrm{id}_{G/[G,G]}$ y si $f\colon G \to G'$ y $g\colon G' \to G''$ son dos morfismos de grupos, entonces $\overline{g \circ f} = \overline{g} \circ \overline{f}$.

Ejemplo. A continuación calculamos el conmutador de los grupos diedrales y cuaterniónicos. Recordemos que D_n es el grupo generado por a,b sujeto a las relaciones $a^n = 1$, $b^2 = 1$ y $bab^{-1}a = 1$ y que $D_n = \{1, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\}$. Dado que $[b,a] = bab^{-1}a^{-1} = a^{-2}$, el subgrupo $\langle a^2 \rangle$ de D_n está incluído en $[D_n, D_n]$. Como, por otra parte $\langle a^2 \rangle$ es un subgrupo normal de D_n y $D_n/\langle a^2 \rangle \simeq D_2$ es abeliano, tenemos que $[D_n, D_n] \subseteq \langle a^2 \rangle$ y así $[D_n, D_n] = \langle a^2 \rangle$. Recordemos ahora

que H_n es el grupo generado por a, b sujeto a las relaciones $a^n b^{-2} = 1$ y $bab^{-1}a = 1$ y que $H_n = \{1, a, \dots, a^{2n-1}, b, ab, \dots, a^{2n-1}b\}$. Como $[b, a] = bab^{-1}a^{-1} = a^{-2}$, el subgrupo $\langle a^2 \rangle$ de H_n es normal y $H_n/\langle a^2 \rangle$ es abeliano (tiene orden 4), vale que $[H_n, H_n] = \langle a^2 \rangle$.

El conmutador de un subgrupo con otro. Dados dos subgrupos H y L de un grupo G definimos $[L, H]$ como el grupo generado por los conmutadores $[l, h]$ con $l \in L$ y $h \in H$. Notemos $[L, H] = \{1\}$ si y sólo si todos los elementos de L conmutan con los de H y que $[L, H] = [H, L]$ ya que $[l, h] = [h, l]^{-1}$.

Proposición 1.13.4. *Vale lo siguiente:*

1) *Si $f\colon G \to G'$ es un morfismo de grupos, entonces $f([L, H]) = [f(L), f(H)]$.*
2) *Si H y L son subgrupos completamente normales de G, entonces $[L, H]$ también lo es.*
3) *Si H y L son subgrupos característicos de G, entonces $[L, H]$ también lo es.*
4) *Si H y L son subgrupos normales de G, entonces $[L, H]$ también lo es.*

Demostración. El item 1) es trivial. Veamos el item 2). Tomemos un endomorfismo f de G. Como H y L son subgrupos completamente normales de G, sabemos que $f(H) \subseteq H$ y $f(L) \subseteq L$ y así, $f([L, H]) = [f(L), f(H)] \subseteq [L, H]$. La demostración de los items 3) y 4) es similar, pero tomando como f un automorfismo y un automorfismo interior de G, respectivamente. □

Observación 1.13.5. *Si H y L son subgrupos de un grupo G y K es un subgrupo normal de G, entonces $[L, H] \subseteq K$ si y sólo si las imagenes de los elementos de H en G/K conmutan con las de los elementos de L. En particular $[G, H] \subseteq K$ si y sólo si $HK/K \subseteq \mathrm{Z}(G/K)$. Denotemos con $\overline{H}$, $\overline{L}$ y $\overline{[L, H]}$ a los mínimos subgrupos normales de G que contienen a H, L y $[L, H]$ respectivamente. El mínimo K tal que $[L, H] \subseteq K$ es obviamente $\overline{[L, H]}$. Dado que $[L, H] \subseteq [\overline{L}, \overline{H}]$ y que, por el item 4) de la Proposición 1.13.4, $[\overline{L}, \overline{H}]$ es un subgrupo normal de G, es claro que $\overline{[L, H]} \subseteq [\overline{L}, \overline{H}]$.*

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

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

donde π denota al epimorfismo canónico, conmuta. Supongamos ahora que H y L son subgrupos normales de un grupo G y que H' y L' son subgrupos normales de un grupo G'. Por el comentario que precede a la Observación 1.11.9, dado un morfismo de grupos $f\colon G \to G'$ tal que $f(H) \subseteq H'$ y $f(L) \subseteq L'$, existe un único morfismo $\overline{f}\colon \frac{G}{[L,H]} \to \frac{G'}{[L',H']}$ tal que el diagrama

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

donde π y π' denotan a los epimorfismo canónicos, conmuta. Por último vale que $\overline{\mathrm{id}_G} = \mathrm{id}_{G/[L,H]}$ y que si f es como arriba y $g\colon G' \to G''$ es un morfismo de grupos que satisface $g(H') \subseteq H''$ y $g(L') \subseteq L''$, donde H'' y L'' son subgrupos normales de G'', entonces $\overline{g \circ f} = \overline{g} \circ \overline{f}$.

Ejercicio 16. *Demuestre que el conmutador* $[\ ,\ ]\colon G \times G \to G$ *satisface las siguientes propiedades.*

1) $[a, bc] = [a, b]b[a, c]b^{-1}$ *y* $[ab, c] = a[b, c]a^{-1}[a, c]$.

2) $[cac^{-1}, [b, c]][bcb^{-1}, [a, b]][aba^{-1}, [c, a]] = 1$ *(identidad de Hall).*

3) $b[a, [b^{-1}, c]]b^{-1}c[b, [c^{-1}, a]]c^{-1}a[c, [a^{-1}, b]]a^{-1} = 1$ *(identidad de Jacobi).*

Subgrupos conjugados. Similarmente al caso de elementos decimos que dos subgrupos H y L de un grupo G son conjugados si existe $a \in G$ tal que $L = aHa^{-1}$. Es claro que los ordenes de dos subgrupos conjugados coinciden. Veamos que también los índices lo hacen. Fijemos $a \in G$ y consideremos el automorfismo $\Phi_a\colon G \to G$ definido por $\Phi_a(b) = aba^{-1}$. Por la Obsevación 1.11.7, $|G : \Phi_a(H)| = |G : H|$ y así, para terminar la demostración basta observar que $\Phi_a(H) = aHa^{-1}$. Además la relación, definida entre los subgrupos de G, por $H \sim L$ si y sólo si H y L son conjugados, es claramente de equivalencia. En consecuencia, el conjunto formado por los subgrupos de G queda partido en clases, llamadas *clases de conjugación*. Es evidente que un subgrupo de G es invariante si y sólo si su clase de conjugación lo tiene a él como único elemento. Notemos ahora que si H es un subgrupo de G, entonces $N = \bigcap_{a\in G} aHa^{-1}$ es el máximo subgrupo normal de G que está incluído en H. En efecto, N es normal ya que

$$bNb^{-1} \subseteq \bigcap_{a\in G} baHa^{-1}b^{-1} = \bigcap_{a\in G} aHa^{-1} = N,$$

y la maximalidad de N se sigue de que si $L \subseteq H$ es un subgrupo normal de G, entonces $L = aLa^{-1} \subseteq aHa^{-1}$ para todo $a \in G$ y así, $L \subseteq N$. Notemos por último que si $\{a_i\}_{i\in I}$ es un conjunto de representantes de las coclases a izquierda de H en G (es decir que para cada $a \in G$ la intesección $\{a_i\}_{i\in I} \cap aH$ tiene exactamente un elemento), entonces $N = \bigcap_{i\in I} a_iHa_i^{-1}$, ya que $(a_ih)H(a_ih)^{-1} = a_iHa_i^{-1}$, para todo $i \in I$ y todo $h \in H$.

Observación 1.13.6. *Supongamos H es un subgrupo de G de índice finito n. Denotemos con $a_1, \ldots, a_n$ a representantes de las coclases a izquierda de H en G y con N a $\bigcap_{i=1}^n a_iHa_i^{-1}$. Por la Observación 1.6.10,*

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

Esta desigualdad será mejorada más adelante.

El normalizador y centralizador. El *normalizador* y *centralizador* de un subconjunto H de un grupo G son los subconjuntos $\mathrm{N}_G(H)$ y $\mathrm{C}_G(H)$ de G, definidos por

$$\mathrm{N}_G(H) = \{a \in G : aHa^{-1} = H\} \qquad \text{y}$$
$$\mathrm{C}_G(H) = \{a \in G : aha^{-1} = h \quad \text{para todo } h \in H\}$$

Es inmediato que $\mathrm{C}_G(H) \subseteq \mathrm{N}_G(H)$ son subgrupos de G. Además si $a \in \mathrm{N}_G(H)$ y $b \in \mathrm{C}_G(H)$, entonces

$$aba^{-1}h(aba^{-1})^{-1} = ab(a^{-1}ha)b^{-1}a^{-1} = a(a^{-1}ha)a^{-1} = h,$$

para todo $h \in H$, de manera de que $\mathrm{C}_G(H)$ es un subgrupo normal de $\mathrm{N}_G(H)$. Por último es claro de la definición que

1) $\mathrm{C}_G(H) = \bigcap_{h\in H} \mathrm{C}_G(h)$,
2) $H \subseteq \mathrm{C}_G(H)$ si y sólo si los elementos de H conmutan entre si y, en ese caso, $\mathrm{C}_G(H)$ es el máximo subgrupo de G en el que los elementos de H son centrales,
3) Si H es un subgrupo de G, entonces $\mathrm{N}_G(H)$ es máximo subgrupo de G en el que H es normal.

Decimos que un subgrupo L de G *normaliza* a otro subgrupo H si $L \subseteq \mathrm{N}_G(H)$. Similarmente decimos que L *centraliza* a H si $L \subseteq \mathrm{C}_G(H)$. Es fácil ver que L normaliza a H si y sólo si $[L, H] \subseteq H$ y que centraliza a H si y sólo si $[L, H] = \{1\}$. Supongamos que L normaliza a H. Dado que entonces $H, L \subseteq \mathrm{N}_G(H)$ y que H es normal en $\mathrm{N}_G(H)$ tenemos que HL es un subgrupo de $\mathrm{N}_G(H)$ y, por lo tanto de G. Además H es normal en $\mathrm{N}_G(H)$ y así, $H/(H \cap L) \simeq HL/H$.

Observación 1.13.7. *Si H y L son subgrupos de un grupo G y L normaliza a H, entonces como vimos recién $[L, H] \subseteq H$ y, en consecuencia de $[L, H] \cap H = \{1\}$, se sigue que $[L, H] = \{1\}$ o, en otras palabras que los elementos de L conmutan con los de H. En particular si H es un subgrupo normal de G y $[G, H] \cap H = \{1\}$ (lo que ocurre por ejemplo si $[G, G] \cap H = \{1\}$), entonces $H \subseteq \mathrm{Z}(G)$.*

Ejercicio 17. *Supongamos que H y L son subgrupos de un grupo G y que L está incluído en $\mathrm{N}_G(H)$. Pruebe que si K es un subgrupo normal de L, entonces HK es un subgrupo normal de HL.*

1.14.Producto directo de grupos. Si H y L son grupos, entonces sobre el producto cartesiano $H \times L$ queda definida una estructura de grupo poniendo

$$(h, l)(h', l') = (hh', ll')$$

Es claro que $(1, 1)$ es el neutro de $H \times L$ y que $(h, l)^{-1} = (h^{-1}, l^{-1})$. A $H \times L$ se lo llama el *producto directo* de H y L. Es fácil ver que las aplicaciones canónicas

$$\pi_H \colon H \times L \to H, \quad \pi_L \colon H \times L \to L, \quad \iota_H \colon H \to H \times L \quad \text{y} \quad \iota_L \colon L \to H \times L,$$

definidas por

$$\pi_H(h, l) = h, \quad \pi_L(h, l) = l, \quad \iota_H(h) = (h, 1) \quad \text{y} \quad \iota_L(l) = (1, l)$$

son morfismos de grupos que satisfacen

$$h = \pi_H(\iota_H(h)), \quad l = \pi_L(\iota_L(l)) \quad \text{y} \quad (h, l) = \iota_H(\pi_H(h, l))\iota_L(\pi_L(h, l))$$

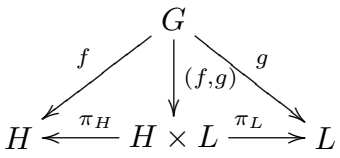
para todo $h \in H$ y $l \in L$, y además

$$\mathrm{Ker}(\pi_H) = \{1\} \times L = \mathrm{Im}(\iota_L) \qquad \text{y} \qquad \mathrm{Ker}(\pi_L) = H \times \{1\} = \mathrm{Im}(\iota_H).$$

En particular la sucesión

$$1 \longrightarrow H \xrightarrow{\iota_H} H \times L \xrightarrow{\pi_L} L \longrightarrow 1$$

es exacta (es decir que ι_H es inyectiva, π_L es sobreyectiva y $\mathrm{Ker}(\pi_L) = \mathrm{Im}(\iota_H)$) y ι_H y π_L son una sección y una retracción, respectivamente. El producto $H \times L$, junto con los morfismos π_H y π_L, tiene la siguiente propiedad (que se denomina *propiedad universal del producto directo*):

> Si $f\colon G \to H$ y $g\colon G \to L$ son morfismos de grupos, entonces existe un único morfismo de grupos $(f,g)\colon G \to H \times L$ tal que el diagrama
>
> 
>
>
> conmuta. Es decir que $\pi_H \circ (f,g) = f$ y $\pi_L \circ (f,g) = g$.

En efecto, estas igualdades fuerzan a que sea $(f,g)(a) = (f(a), g(a))$ y es claro que con esta definición (f,g) es un morfismo de grupos que satisface las igualdades mencionadas arriba. Es también claro que $\mathrm{Ker}(f,g) = \mathrm{Ker}(f) \cap \mathrm{Ker}(g)$.

Notemos que la propiedad universal del producto directo dice simplemente que para todo grupo G, la aplicación

$$\Psi\colon \mathrm{Hom}(G, H \times L) \to \mathrm{Hom}(G,H) \times \mathrm{Hom}(G,L),$$

definida por $\Psi(\varphi) = (\pi_H \circ \varphi, \pi_L \circ \varphi)$, es biyectiva. Es fácil ver que si H y L son conmutativos, entonces Ψ también es un isomorfismo de grupos.

Observación 1.14.1. *El orden de un elemento (h,l) de $H \times L$ es igual al mínimo de los múltiplos comunes de los órdenes de h y l. En efecto, dado que $(h,l)^n = (h^n, l^n)$, vale que $(h,l)^n = 1$ si y sólo si $h^n = 1$ y $l^n = 1$.*

Observación 1.14.2. *Supongamos que H y L son subgrupos normales de un grupo G y denotemos con $\pi_H\colon G \to G/H$ y $\pi_L\colon G \to G/L$ a las sobreyecciones canónicas. Por lo que acabamos de ver $(\pi_H, \pi_L)\colon G \to \frac{G}{H} \times \frac{G}{L}$ es un morfismo con núcleo igual a $H \cap L$. Afirmamos que este morfismo es sobreyectivo si y sólo si $HL = G$. Supongamos primero que se cumple esta condición y tomemos $(\overline{a}, \overline{b}) \in \frac{G}{H} \times \frac{G}{L}$, donde $\overline{a}$ denota a la clase de $a \in G$ en G/H y $\overline{b}$ a la de $b \in G$ en G/L. Por hipótesis existen $h, h' \in H$ y $l, l' \in L$ tales que $a = hl$ y $b = h'l'$ y así,*

$$(\pi_H(h'l), \pi_L(h'l)) = (\pi_H(l), \pi_L(h')) = (\pi_H(hl), \pi_L(h'l')) = (\overline{a}, \overline{b}),$$

de modo de que la imagen de (π_H, π_L) es $\frac{G}{H} \times \frac{G}{L}$. Supongamos ahora que (π_H, π_L) es sobreyectivo. Entonces dado $a \in G$ existe $l \in G$ tal que $(\pi_H(l), \pi_L(l)) = (\pi_H, \pi_L)(l) = (\overline{a}, 1)$, donde $\overline{a}$ denota a la clase de $a \in G$ en G/H. Pero entonces $\pi_L(l) = 1$ y $\pi_H(l) = \pi_H(a)$ lo que significa que $l \in L$ y que existe $h \in H$ tal que $a = hl$.

Observación 1.14.3. *Si $f\colon H \to H'$ y $g\colon L \to L'$ son morfismos de grupos, entonces por la propiedad universal del producto directo queda definido un único morfismo de grupos $f \times g\colon H \times L \to H' \times L'$ tal que $\pi_{H'} \circ (f \times g) = f \circ \pi_H$ y $\pi_{L'} \circ (f \times g) = g \circ \pi_L$. Estas igualdades se expresan también diciendo que los cuadrados*

$$\begin{array}{ccc} H \times L & \xrightarrow{f\times g} & H' \times L' \\ \downarrow{\scriptstyle \pi_H} & & \downarrow{\scriptstyle \pi_{H'}} \\ H & \xrightarrow{f} & H' \end{array} \qquad y \qquad \begin{array}{ccc} H \times L & \xrightarrow{f\times g} & H' \times L' \\ \downarrow{\scriptstyle \pi_L} & & \downarrow{\scriptstyle \pi_{L'}} \\ L & \xrightarrow{g} & L' \end{array}$$

conmutan. Es claro que $(f \times g)(h, l) = (f(h), g(l))$.

Observación 1.14.4. *Vale lo siguiente:*

1) $\mathrm{id}_H \times \mathrm{id}_L = \mathrm{id}_{H\times L}$.
2) *Si $f\colon H \to H'$ y $f'\colon H' \to H''$, $g\colon L \to L'$ y $g'\colon L' \to L''$ son morfismos de grupos, entonces $(f' \times g') \circ (f \times g) = (f' \circ f) \times (g' \circ g)$.*
3) *Si $f\colon H \to H'$ y $g\colon L \to L'$ y son morfismos de grupos, entonces*

$$\mathrm{Im}(f \times g) = \mathrm{Im}(f) \times \mathrm{Im}(g) \quad y \quad \mathrm{Ker}(f \times g) = \mathrm{Ker}(f) \times \mathrm{Ker}(g).$$

Demostración. Cálculo directo. □

Equivalencia de sucesiones exactas cortas. Una sucesión exacta corta de grupos es una sucesión exacta de la forma

$$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{\pi} L \longrightarrow 1$$

Decimos que la sucesión exacta corta de arriba y la sucesión exacta corta

$$1 \longrightarrow H \xrightarrow{i'} G' \xrightarrow{\pi'} L \longrightarrow 1$$

son equivalentes si existe un morfismo $\varphi\colon G \to G'$ tal que el diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{i} & G & \xrightarrow{\pi} & L & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_H} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_L} & & \\ 1 & \longrightarrow & H & \xrightarrow{i'} & G' & \xrightarrow{\pi'} & L & \longrightarrow & 1 \end{array}$$

conmuta (es decir tal que $\varphi \circ i = i'$ y $\pi' \circ \varphi = \pi$). Afirmamos que entonces φ es un isomorfismo. Veamos primero que es inyectiva. Supongamos que $\varphi(a) = 1$. Entonces $\pi(a) = \pi'(\varphi(a)) = 1$ y, por la exactitud de la primera fila, existe $h \in H$ tal que $a = i(h)$. Pero entonces $1 = \varphi(a) = \varphi(i(h)) = i'(h)$ y, como i' es inyectiva, $h = 1$. En consecuencia $a = i(h) = i(1) = 1$. Veamos ahora que φ es sobreyectiva. Tomemos $b \in G'$. Como π es sobreyectiva existe $a \in G$ tal que $\pi(a) = \pi'(b)$. Por lo tanto $\pi'(\varphi(a)^{-1}b) = \pi(a)^{-1}\pi'(b) = 1$ y así, por la exactitud de la segunda fila, existe $h \in H$ tal que $\varphi(a)^{-1}b = i'(h)$, de donde $b = \varphi(a)i'(h) = \varphi(a)\varphi(i(h)) = \varphi(ai(h))$. Es fácil ver ahora que la relación definida entre sucesiones exactas cortas con extremos H y L, diciendo que son equivalentes si lo son en el sentido mencionado arriba, es verdaderamente de equivalencia. Notemos que si dos sucesiones como las mencionadas arriba son equivalentes, entonces i es una sección si y sólo si i' lo es y, similarmente, π es una retracción si y sólo si π' lo es. A continuación caracterizamos las sucesiones exactas cortas tales que el primer morfismo no necesaramente trivial es una sección.

Proposición 1.14.5. *Si*

$$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{\pi} L \longrightarrow 1$$

es una sucesión exacta y si existe $r\colon G \to H$ *tal que* $r \circ i = \mathrm{id}_H$*, entonces hay un isomorfismo* $\varphi\colon G \to H \times L$ *tal que el diagrama*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{i} & G & \xrightarrow{\pi} & L & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_H} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_L} & & \\ 1 & \longrightarrow & H & \xrightarrow{\iota_H} & H \times L & \xrightarrow{\pi_L} & L & \longrightarrow & 1 \end{array}$$

conmuta. En consecuencia π *es una retracción.*

Demostración. Tomemos $\varphi = (r, \pi)$. Por definición

$$\varphi(i(h)) = (r(i(h)), \pi(i(h))) = \iota_H(h) \quad \text{y} \quad \pi_L(\varphi(a)) = \pi_L(r(a), \pi(a)) = \pi(a),$$

de modo de que el diagrama mencionado arriba conmuta. □

Hay otra propiedad universal relacionada con $H \times L$. Notemos que las aplicaciones canónicas $\iota_H\colon H \to H \times L$ y $\iota_L\colon L \to H \times L$ satisfacen $\iota_H(h)\iota_L(l) = \iota_L(l)\iota_H(h)$ para todo $h \in H$ y $l \in L$. El producto $H \times L$, junto con los morfismos ι_H y ι_L, tiene la siguiente propiedad:

Si $f\colon H \to G$ y $g\colon L \to G$ son morfismos de grupos que satisfacen $f(h)g(l) = g(l)f(h)$ para todo $h \in H$ y $l \in L$, entonces existe un único morfismo de grupos $fg\colon H \times L \to G$ tal que el diagrama

$$\begin{array}{ccccc} & & G & & \\ & {\scriptstyle f}\nearrow & \uparrow{\scriptstyle fg} & \nwarrow{\scriptstyle g} & \\ H & \xrightarrow{\iota_H} & H \times L & \xleftarrow{\iota_L} & L \end{array}$$

conmuta. Es decir que $(fg) \circ \iota_H = f$ y $(fg) \circ \iota_L = g$.

En efecto, estas igualdades fuerzan a que sea

$$(fg)(h, l) = (fg)((h, 1)(1, l)) = (fg)(\iota_H(h))(fg)(\iota_L(l)) = f(h)g(l).$$

Veamos que la aplicación fg, definida de esta manera, es un morfismo de grupos:

$$\begin{aligned} (fg)((h, l)(h', l')) &= (fg)(hh', ll') \\ &= f(hh')g(ll') \\ &= f(h)f(h')g(l)g(l') \\ &= f(h)g(l)f(h')g(l') \\ &= (fg)(h, l)(fg)(h', l'). \end{aligned}$$

Es claro que fg satisface las igualdades mencionadas arriba y es claro también que $\mathrm{Im}(fg) = \mathrm{Im}(f)\,\mathrm{Im}(g)$.

Notemos que la propiedad mencionada arriba dice simplemente que para todo grupo G, la aplicación

$$\Psi\colon \mathrm{Hom}(H \times L, G) \to \mathrm{Hom}(H, G) \times \mathrm{Hom}(L, G),$$

definida por $\Psi(\varphi) = (\varphi \circ \iota_H, \varphi \circ \iota_L)$, es una inyección cuya imagen es

$$\{(f, g) \in \mathrm{Hom}(H, G) \times \mathrm{Hom}(L, G) : f(h)g(l) = g(l)f(h) \text{ para todo } h \in H \text{ y } l \in L\}.$$

En particular, si G es conmutativo, entonces Ψ es una bijección. Es fácil ver que en este caso Ψ también es un isomorfismo de grupos.

Observación 1.14.6. *Supongamos que H y L son subgrupos de un grupo G y que los elementos de H conmutan con los de L (es decir que $hl = lh$ para todo $h \in H$ y $l \in L$). Por la propiedad universal que acabamos de ver existe un morfismo $\varphi\colon H \times L \to G$ que está definido por $\varphi(h,l) = hl$. Es claro que $\mathrm{Im}(\varphi) = HL$ y que $\mathrm{Ker}(\varphi) = \{(a, a^{-1}) : a \in H \cap L\} \simeq H \cap L$. En particular φ es un isomorfismo si y sólo si $HL = G$ y $H \cap L = \{1\}$.*

Teorema 1.14.7. *Si H y L son subgrupos normales de un grupo G son equivalentes:*

1) *$H \cap L = \{1\}$,*
2) *La aplicación $\phi\colon H \times L \to G$, definida por $\phi(h,l) = hl$ es un morfismo inyectivo.*
3) *Cada elemento de HL se escribe de manera única como un producto hl con $h \in H$ y $l \in L$.*
4) *El 1 (que claramente está en HL) satisface la propiedad mencionada en el item 3).*

Demostración. Veamos que 1) implica 2). Tomemos $h \in H$ y $l \in L$. Dado que H y L son normales, $h(lh^{-1}l^{-1}) = (hlh^{-1})l^{-1} \in H \cap L$ y así, por hipótesis, $hlh^{-1}l^{-1} = 1$, lo que implica que $hl = lh$. Por la Observación 1.14.6, la aplicación $\phi\colon H \times L \to G$, definida por $\phi(h,l) = hl$ es un morfismo inyectivo. Es claro que 2) implica 3) y 3) implica 4). Veamos ahora que 4) implica 1). Tomemos $a \in H \cap L$. Dado que el 1 de G se escribe como $1 = 1_H 1_L$ y $1 = aa^{-1}$ es $a = 1$. □

Ejemplo. Supongamos que $\langle a\rangle$ es cíclico de orden $n = \alpha\beta$ con α y β coprimos. Afirmamos que $\langle a^\alpha\rangle \cap \langle a^\beta\rangle = \{1\}$. En efecto, si $a^{\alpha r} = a^{\beta s}$, entonces $\alpha r \equiv \beta s \pmod n$ y así, como α y β coprimos, β divide a r, lo que implica que $a^{\alpha r} = 1$. Por lo tanto la aplicación

$$\psi\colon \langle a^\alpha\rangle \times \langle a^\beta\rangle \to \langle a\rangle,$$

definida por $\psi(a^{\alpha r}, a^{\beta s}) = a^{\alpha r}a^{\beta s} = a^{\alpha r+\beta s}$ es un morfismo inyectivo y así, por cuestiones de cardinabilidad, también sobreyectivo. Notemos que esto implica que la función $\phi\colon \mathbb{N} \to \mathbb{N}$ de Euler, satisface $\phi(n) = \phi(\alpha)\phi(\beta)$. En efecto esto se sigue de que $\phi(n)$, $\phi(\alpha)$ y $\phi(\beta)$ son la cantidad de generadores de $\langle a\rangle$, $\langle a^\beta\rangle$ y $\langle a^\alpha\rangle$, respectivamente, y de que

$$\begin{aligned}
\psi(a^{\alpha r}, a^{\beta s}) \text{ genera } \langle a\rangle &\Leftrightarrow (a^{\alpha r}, a^{\beta s}) \text{ genera } \langle a^\alpha\rangle \times \langle a^\beta\rangle \\
&\Leftrightarrow (a^{\alpha r}, a^{\beta s}) \text{ tiene orden } n \\
&\Leftrightarrow a^{\alpha r} \text{ tiene orden } \beta \text{ y } a^{\beta s} \text{ tiene orden } \alpha \\
&\Leftrightarrow a^{\alpha r} \text{ genera } \langle a^\alpha\rangle \text{ y } a^{\beta s} \text{ genera } \langle a^\beta\rangle.
\end{aligned}$$

Ejercicio 18. *Pruebe que si N es un subgrupo normal de $H \times L$ y*

$$N \cap (H \times \{1\}) = N \cap (\{1\} \times L) = \{(1,1)\},$$

entonces $N \subseteq \mathrm{Z}(H \times L)$.

Ejercicio 19. *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 $G = H \times L$.*

Observación 1.14.8. *Combinando la Observación 1.14.2 y el Teorema 1.14.7 obtenemos que si H y L son subgrupos normales de un grupo G, entonces $H \cap L = \{1\}$ y $HL = G$ si y sólo si las aplicaciones*

$$\phi\colon H \times L \to G \quad y \quad \psi\colon G \to \frac{G}{H} \times \frac{G}{L}$$

definidas por $\phi(h,l) = hl$ y $\psi(a) = (\pi_H(a), \pi_L(a))$, donde $\pi_H\colon G \to G/H$ y $\pi_L\colon G \to G/L$ denotan a las sobreyecciones canónicas, son isomorfismos. Es fácil ver que la composición de estos isomorfismos identifica a $H \times \{1\}$ con $\{1\} \times \frac{G}{L}$ y a $\{1\} \times L$ con $\frac{G}{H} \times \{1\}$.

Observación 1.14.9. *Supongamos que K, H y L son tres grupos. Es claro que las aplicaciones $\alpha\colon (K \times H) \times L \to K \times (H \times L)$ y $\beta\colon L \times H \to H \times L$, definidas por $\alpha((k,h),l) = (k,(h,l))$ y $\beta(l,h) = (h,l)$, son isomorfismos naturales de grupos. Esto último por definición significa que si $\phi\colon K \to K'$, $\varphi\colon H \to H'$ y $\psi\colon L \to L'$ son morfismos de grupos, entonces los diagramas*

$$\begin{array}{ccc} (K \times H) \times L & \xrightarrow{\alpha} & K \times (H \times L) \\ \downarrow{\scriptstyle (\phi\times\varphi)\times\psi} & & \downarrow{\scriptstyle \phi\times(\varphi\times\psi)} \\ (K' \times H') \times L' & \xrightarrow{\alpha} & K' \times (H' \times L') \end{array} \qquad y \qquad \begin{array}{ccc} L \times H & \xrightarrow{\beta} & H \times L \\ \downarrow{\scriptstyle \psi\times\varphi} & & \downarrow{\scriptstyle \varphi\times\psi} \\ H' \times K' & \xrightarrow{\beta} & K' \times H' \end{array}$$

conmutan.

Teorema 1.14.10. *Si $H_1, \ldots, H_n$ son subgrupos normales de un grupo G son equivalentes:*

1) *$H_i \cap (H_1 \cdots H_{i-1}) = \{1\}$ para todo $1 < i \leq n$,*
2) *La aplicación $\phi\colon H_1 \times \cdots \times H_n \to G$, definida por $\phi(h_1, \ldots, h_n) = h_1 \cdots h_n$ es un morfismo inyectivo de grupos.*
3) *Cada elemento de $H_1 \cdots H_n$ se escribe de manera única como un producto $h_1 \cdots h_n$, con $h_i \in H_i$ para $1 \leq i \leq n$.*
4) *El 1 (que claramente está en $H_1 \cdots H_n$) satisface la propiedad mencionada en el item 3).*

Demostración. Veamos que 1) implica 2). Vamos a demostrar esto por inducción en n. El caso $n = 1$ es trivial. Supongamos que $n > 1$ y que el resultado vale para $n-1$, de manera que la aplicación $\phi'\colon H_1 \times \cdots \times H_{n-1} \to G$, definida por $\phi'(h_1, \ldots, h_{n-1}) = h_1 \cdots h_{n-1}$, es un morfismo inyectivo. Dado que por el Teorema 1.14.7, también lo es la aplicación $\phi''\colon (H_1 \cdots H_{n-1}) \times H_n \to G$, definida por $\phi''(h, h_n) = hh_n$, el resultado se sigue entonces de que $\phi = \phi'' \circ (\phi' \times \mathrm{id}_{H_n})$. Es claro que 2) implica 3) y 3) implica 4). Vemos ahora que 4) implica 1). Tomemos $h_i \in H_i \cap (H_1 \cdots H_{i-1})$ y escribamos $h_i = h_1 \cdots h_{i-1}$ con $h_j \in H_j$ para todo $1 \leq j < i$. Dado que el 1 de G se escribe como $1 = 1_{H_1} \cdots 1_{H_i}$ y $1 = h_1 \cdots h_{i-1} h_i^{-1}$, sabemos por hipótesis que $h_i = 1$. $\square$

Corolario 1.14.11. *Si $H_1, \ldots, H_n$ son subgrupos normales y finitos de un grupo G y $|H_i|$ es coprimo con $|H_j|$ para todo $i \neq j$, entonces la aplicación*

$$\phi\colon H_1 \times \cdots \times H_n \to G,$$

definida por $\phi(h_1,\dots,h_n)=h_1\cdots h_n$ *es un morfismo inyectivo de grupos. Además* ϕ *es un isomorfismo si y sólo si* $|G|=|H_1|\cdots|H_n|$.

Demostración. Por la Proposición 1.6.8, $|H_1\cdots H_{i-1}|$ divide a $|H_1|\cdots|H_{i-1}|$ y, en consecuencia, es coprimo con $|H_i|$. Por lo tanto $H_i\cap(H_1\cdots H_{i-1})=\{1\}$ para todo $1<i\leq n$ y así, por el Teorema 1.14.10, ϕ es un morfismo inyectivo. Es claro ahora que ϕ es un isomorfismo si y sólo si $|G|=|H_1|\cdots|H_n|$. □

Observación 1.14.12. *Para toda familia* $G_1,\dots,G_n$ *de grupos vale lo siguiente:*

1) $\mathrm{Z}(G_1\times\cdots\times G_n)=\mathrm{Z}(G_1)\times\cdots\times\mathrm{Z}(G_n)$.

2) $[G_1\times\cdots\times G_n,G_1\times\cdots\times G_n]=[G_1,G_1]\times\cdots\times[G_n,G_n]$.

3) Si H_i,L_i *son subgrupos de* G_i *para* $1\leq i\leq n$, *entonces*

$$[H_1\times\cdots\times H_n,L_1\times\cdots\times L_n]=[H_1,L_1]\times\cdots\times[H_n,L_n].$$

4) Si H_i *es un subconjunto de* G_i *para* $1\leq i\leq n$, *entonces*

$$\mathrm{C}_{G_1\times\cdots\times G_n}(H_1\times\cdots\times H_n)=\mathrm{C}_{G_1}(H_1)\times\cdots\times\mathrm{C}_{G_n}(H_n)$$

y

$$\mathrm{N}_{G_1\times\cdots\times G_n}(H_1\times\cdots\times H_n)=\mathrm{N}_{G_1}(H_1)\times\cdots\times\mathrm{N}_{G_n}(H_n).$$

Observación 1.14.13. *Supongamos que* H_i *es un subgrupo normal de* G_i *para todo* $1\leq i\leq n$. *Entonces las proyecciones canónicas* $\pi_i\colon G_i\to G_i/H_i$ *inducen un morfismo*

$$\pi_1\times\cdots\times\pi_n\colon G_1\times\cdots\times G_n\to\frac{G_1}{H_1}\times\cdots\times\frac{G_n}{H_n},$$

cuyo núcleo es $H_1\times\cdots\times H_n$ *y así,*

$$\frac{G_1\times\cdots\times G_n}{H_1\times\cdots\times H_n}\simeq\frac{G_1}{H_1}\times\cdots\times\frac{G_n}{H_n}.$$

Observación 1.14.14. *Supongamos que* $H_1,\dots,H_r$ *y* $L_1,\dots,L_s$ *son dos familias de grupos y denotemos con* $\mathrm{Mor}((H_i)_{1\leq i\leq r},(L_j)_{1\leq j\leq s})$ *al conjunto formado por las familias de morfismos* $(f_{ji}\colon H_i\to L_j)_{\substack{1\leq i\leq r\\1\leq j\leq s}}$ *que satisfacen*

$$(*)\qquad f_{ji}(a)f_{ji'}(a')=f_{ji'}(a')f_{ji}(a),$$

para todo $1\leq i<i'\leq r$, $1\leq j\leq s$, $a\in H_i$ *y* $a'\in H_{i'}$. *Consideremos la aplicación*

$$\theta\colon\mathrm{Mor}((H_i)_{1\leq i\leq r},(L_j)_{1\leq j\leq s})\to\mathrm{Hom}(H_1\times\cdots\times H_r,L_1\times\cdots\times L_s),$$

definida por

$$\theta\left((f_{ij}\colon H_i\to L_j)_{\substack{1\leq i\leq r\\1\leq j\leq s}}\right)=\begin{pmatrix}f_{11}&\cdots&f_{1r}\\\vdots&\ddots&\vdots\\f_{s1}&\cdots&f_{sr}\end{pmatrix}$$

Por definición esta matriz actúa sobre un elemento $(a_1, \dots, a_r) \in H_1 \times \cdots \times H_r$, *via*

$$(**) \qquad \begin{pmatrix} f_{11} & \dots & f_{1r} \\ \vdots & \ddots & \vdots \\ f_{s1} & \dots & f_{sr} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix} = \begin{pmatrix} f_{11}(a_1) \dots f_{1r}(a_r) \\ \vdots \\ f_{s1}(a_1) \dots f_{sr}(a_r). \end{pmatrix}$$

Notemos que en cada fila de la matriz columna del lado derecho de la igualdad, los signos suma que aparecen usualmente en el producto de las matrices de la izquierda, han sido reemplazadas por signos producto. Esto se debe a que la operación en cada uno de los L_j *es denotada multiplicativamente. De las dos propiedades universales que hemos visto en esta sección se sigue que* θ *es una aplicación biyectiva. Más aún es facil ver que* $\theta^{-1}(f) = (\pi_j \circ f \circ \iota_i)_{\substack{1 \le i \le r \\ 1 \le j \le s}}$, *donde*

$$\iota_i \colon H_i \to H_1 \times \cdots \times H_r \qquad y \qquad \pi_j \colon L_1 \times \cdots \times L_s \to L_j$$

son los morfismos canónicos. Notemos que si los L_j*'s son abelianos entonces la condición* $(*)$ *es vacía y el producto de morfismos obtenido en la Proposición 1.10.1 se corresponde con la operación de matrices definida por*

$$(***) \qquad \begin{pmatrix} f_{11} & \dots & f_{1r} \\ \vdots & \ddots & \vdots \\ f_{s1} & \dots & f_{sr} \end{pmatrix} \begin{pmatrix} f'_{11} & \dots & f'_{1r} \\ \vdots & \ddots & \vdots \\ f'_{s1} & \dots & f'_{sr} \end{pmatrix} = \begin{pmatrix} f_{11}f'_{11} & \dots & f_{1r}f'_{1r} \\ \vdots & \ddots & \vdots \\ f_{s1}f'_{s1} & \dots & f_{sr}f'_{sr} \end{pmatrix}$$

Si además usamos la notación aditiva para la operación de cada uno de los L_j, *entonces las fórmulas* $(**)$ *y* $(***)$ *toman un aspecto más habitual. Supongamos ahora que* $N_1, \dots, N_t$ *es otra famila de grupos y que*

$$\begin{pmatrix} g_{11} & \dots & g_{1s} \\ \vdots & \ddots & \vdots \\ g_{t1} & \dots & g_{ts} \end{pmatrix}$$

es un morfismo de $L_1 \times \cdots \times L_s$ *en* $N_1 \times \cdots \times N_t$. *Usando que* $g_{jk}(f_{ki}(a_i))$ *conmuta con* $g_{jk'}(f_{k'i'}(a'_{i'}))$ *si* $k' \neq k$ *o* $i' \neq i$, *se puede ver que*

$$(****) \qquad \begin{pmatrix} g_{11} & \dots & g_{1s} \\ \vdots & \ddots & \vdots \\ g_{t1} & \dots & g_{ts} \end{pmatrix} \circ \begin{pmatrix} f_{11} & \dots & f_{1r} \\ \vdots & \ddots & \vdots \\ f_{s1} & \dots & f_{sr} \end{pmatrix} = \begin{pmatrix} h_{11} & \dots & h_{1r} \\ \vdots & \ddots & \vdots \\ h_{t1} & \dots & h_{tr} \end{pmatrix}$$

donde $h_{ji} = (g_{j1} \circ f_{1i})(g_{j2} \circ f_{2i}) \cdots (g_{js} \circ f_{si})$ *para* $1 \le i \le r$ *y* $1 \le j \le t$. *Notemos ahora que si los* N_j*'s son abelianos y usamos la notación aditiva para la operación de cada uno de ellos, entonces la fórmula* $(****)$ *toma también un aspecto más habitual. En particular se sigue de todo lo que estuvimos viendo que si* G *es un grupo conmutatico y su operación está denotada aditivamente, entonces* $\mathrm{End}(G^n) \simeq M_n(\mathrm{End}(G))$ *y este isomorfismo respeta tanto la suma como la composición.*

1.15.Producto semidirecto. A continuación generalizamos el producto directo. Recordemos que si H es un grupo, entonces el conjunto $\mathrm{Aut}(H)$ de los automorfismos de H es un grupo con el producto dado por la composición. Así si L es otro grupo podemos considerar los morfismos de grupos

$$\phi\colon L \to \mathrm{Aut}(H).$$

Fijemos uno de estos morfismos y escribamos $l\cdot_\phi h$ en lugar de $\phi(l)(h)$ o incluso $l\cdot h$ si ϕ está claro. Que $\phi(l)$ sea un morfismo de grupos significa que

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

y que ϕ sea un morfismo de grupos que

$$(ll')\cdot h = l\cdot(l'\cdot h) \quad \text{y} \quad 1\cdot h = h \qquad \text{para todo } l, l' \in L \text{ y } h \in H.$$

Notemos que las condiciones $l\cdot 1 = 1$ y $1\cdot h = h$ son redundantes. El producto cartesiano $H \times L$, con la operación

$$(h, l)(h', l') = (h(l\cdot h'), ll')$$

es un grupo con neutro $(1, 1)$ e inverso dado por $(h, l)^{-1} = (l^{-1}\cdot h^{-1}, l^{-1})$. A este grupo lo llamaremos *producto semidirecto* de H y L asociado a ϕ y lo denotaremos $H \times_\phi L$. Veamos primero que $H \times_\phi L$ es asociativo. En efecto

$$\big((h, l)(h', l')\big)(h'', l'') = (h(l\cdot h'), ll')(h'', l'') = \big(h(l\cdot h')((ll')\cdot h''), ll'l''\big)$$

y

$$(h, l)\big((h', l')(h'', l'')\big) = (h, l)(h'(l'\cdot h''), l'l'') = \big(h(l\cdot(h'(l'\cdot h'')), ll'l''\big),$$

que coinciden ya que

$$l\cdot(h'(l'\cdot h'') = (l\cdot h')(l\cdot(l'\cdot h'')) = (l\cdot h')((ll')\cdot h'').$$

Por la Proposición 1.3.2, para terminar la demostración es suficiente ver que $(1, 1)$ es neutro a izquierda de $H \times_\phi L$ y que $(l^{-1}\cdot h^{-1}, l^{-1})$ es inverso a izquierda de (h, l), pero

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

y

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

Proposición 1.15.1. *Vale que:*

1) Hay una sucesión exacta de morfismos de grupos

$$1 \longrightarrow H \xrightarrow{\ i\ } H \times_\phi L \xrightarrow{\ \pi\ } L \longrightarrow 1,$$

que está definida por $i(h) = (h, 1)$ *y* $\pi(h, l) = l$. *Además* π *es una retracción con inversa a derecha* $s\colon L \to H \times_\phi L$ *definida por* $s(l) = (1, l)$.

2) $H \times \{1\}$ *es un subgrupo normal de* $H \times_\phi L$,

3) $\{1\} \times L$ *es un subgrupo de* $H \times_\phi L$,

4) $(H \times \{1\}) \cap (\{1\} \times L) = \{1\}$ *y* $(H \times \{1\})(\{1\} \times L) = H \times_\phi L$,

Demostración. Es inmediato que π y s son morfismos de grupos, que $\pi \circ s = \mathrm{id}_L$ y que $\mathrm{Ker}(\pi) = \mathrm{Im}(i)$. Como

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

también i es un morfismo de grupos. Los items 2) y 3) se siguen ahora de que $H \times \{1\} = \mathrm{Ker}(\pi)$ y $\{1\} \times L = \mathrm{Im}(s)$. Veamos que vale el item 4). Es claro que $(H \times \{1\}) \cap (\{1\} \times L) = \{1\}$ y que $(H \times \{1\})(\{1\} \times L) = H \times_\phi L$ se lo deduce de que $(h, 1)(1, l) = (h(1 \cdot 1), l) = (h, l)$. $\square$

A continuación vamos a caracterizar la sucesiones exactas cortas

$$1 \longrightarrow H \xrightarrow{\ i\ } G \xrightarrow{\ \pi\ } L \longrightarrow 1$$

en las que π es una retracción. Supongamos por lo tanto que este es el caso y fijemos un morfismo $s\colon L \to G$ tal que $\pi \circ s = \mathrm{id}_L$. Llamemos $\phi\colon L \to \mathrm{Aut}(H)$ a la aplicación definida por $i(\phi(l)(h)) = s(l)i(h)s(l)^{-1}$ (notemos que $\pi(s(l)i(h)s(l)^{-1}) = \pi(s(l))\pi(i(h))\pi(s(l))^{-1} = l1l^{-1} = 1$ y que por lo tanto $s(l)i(h)s(l)^{-1} \in \mathrm{Im}(i)$). Es claro que $\phi(l)$ es un morfismo ya que

$$\begin{aligned} i(\phi(l)(hh')) &= s(l)i(hh')s(l)^{-1} \\ &= (s(l)i(h)s(l)^{-1})(s(l)i(h')s(l)^{-1}) \\ &= i(\phi(l)(h))i(\phi(l)(h')) \\ &= i(\phi(l)(h)\phi(l)(h')) \end{aligned}$$

y que $\phi(l)$ es biyectiva con inversa $\phi(l^{-1})$ ya que

$$i\big(\phi(l^{-1})(\phi(l)(h))\big) = s(l^{-1})i(\phi(l)(h))s(l) = s(l^{-1})s(l)i(h)s(l^{-1})s(l) = i(h).$$

Además $\phi\colon L \to \mathrm{Aut}(H)$ es un morfismo de grupos, pues

$$\begin{aligned} i(\phi(ll')(h)) &= s(ll')i(h)s(ll')^{-1} \\ &= s(l)s(l')i(h)s(l')^{-1}s(l)^{-1} \\ &= s(l)i(\phi(l')(h))s(l)^{-1} \\ &= i\big(\phi(l)(\phi(l')(h))\big). \end{aligned}$$

Proposición 1.15.2. *La aplicación* $\varphi\colon H \times_\phi L \to G$, *definida por*

$$\varphi(h, l) = i(h)s(l)$$

es un morfismo de grupos que hace conmutativo al diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\iota_H} & H \times_\phi L & \xrightarrow{\pi_L} & L & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_H} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_L} & & \\ 1 & \longrightarrow & H & \xrightarrow{i} & G & \xrightarrow{\pi} & L & \longrightarrow & 1 \end{array}$$

En particular φ es un isomorfismo.

Demostración. Es claro que

$$\varphi(i_H(h)) = \varphi(h,1) = i(h) \quad \text{y} \quad \pi(\varphi(h,l)) = \pi(i(h)s(l)) = \pi(i(h))\pi(s(l)) = l,$$

de modo de que el diagrama conmuta. Resta ver que φ es un morfismo de grupos, pero

$$\begin{aligned} \varphi((h,l)(h',l')) &= \varphi(h(l\cdot h'), ll') \\ &= i\big(h(l\cdot h')\big)s(ll') \\ &= i(h)i(l\cdot h')s(l)s(l') \\ &= i(h)s(l)i(h')s(l)^{-1}s(l)s(l') \\ &= i(h)s(l)i(h')s(l') \\ &= \varphi(h,l)\varphi(h',l'), \end{aligned}$$

como queríamos ver. □

De acuerdo con la Proposición 1.15.1 podemos (y es usual) identificar a $h \in H$ y a $l \in L$ con $(h,1) \in H \times_\phi L$ y $(1,l) \in H \times_\phi L$, respectivamente. Con esta identificación tenemos que $(h,l) = hl$ y $hlh'l' = h(l\cdot h')ll'$. Por supuesto que es importante distinguir bien a los elementos de H de los de L, usando letras diferentes para ellos.

Ejemplo 1. Supongamos G tiene un subgrupo normal H y un subgrupo L tales que $H \cap L = \{1\}$ y $HL = G$. Entonces $G/H = HL/H \simeq L/(H \cap L) = L$. De manera de que hay una suceción exacta corta

$$1 \longrightarrow H \longrightarrow G \xrightarrow{\pi} L \longrightarrow 1,$$

donde la primera flecha es la inclusión canónica y $\pi\colon G \to L$ está definida por $\pi(hl) = l$ para todo $h \in H$ y $l \in L$. Es claro que la inclusión canónica de L en G es una sección de π. Así, por lo que hemos probado, la aplicación $\varphi\colon H \times_\phi L \to G$, dada por $\varphi(h,l) = hl$, donde $\phi\colon L \to \mathrm{Aut}(H)$ está definido por $\phi(l)(h) = lhl^{-1}$, es un isomorfismo de grupos que hace conmutativo al diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\iota_H} & H \times_\phi L & \xrightarrow{\pi_L} & L & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_H} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_L} & & \\ 1 & \longrightarrow & H & \longrightarrow & G & \xrightarrow{\pi} & L & \longrightarrow & 1 \end{array}$$

Ejemplo 2. Para cada n denotemos con C_n al grupo cíclico de orden n. Consideremos el morfismo

$$\phi\colon C_2 \to \mathrm{Aut}(C_n),$$

definido por $\phi(1)(b) = b$ y $\phi(a)(b) = b^{-1}$, donde a denota al generador de C_2. Es fácil ver que $C_n \times_\phi C_2$ es isomorfo al grupo diedral D_n. Una construcción análoga puede hacerse reemplazando C_n por un grupo abeliano arbitrario.

Ejemplo 3. Denotemos con $H = \langle a\rangle$ y $L = \langle b\rangle$ a dos grupos cíclicos de ordenes n y m respectivamente. Por la Observación 1.12.2, para cada r existe un morfismo $\phi_r\colon H \to H$, tal que $\phi_r(a) = a^r$. Afirmamos que $\mathrm{Ker}(\phi_r) = \langle a^{n/(r:n)}\rangle$, donde $(r : n)$ denota al máximo de los divisores comunes $(r : n)$ de r y n. En efecto esto se sigue claramente de que $a^{ir} = \phi_r(a^i)$ es 1 si y sólo si n divide a ir. En particular ϕ_r es un automorfismo si y sólo si r es coprimo con n. Notemos que $\phi_r^m(a) = a^{r^m}$, de manera de que $\phi_r^m = \mathrm{id}$ si y sólo si $r^m \equiv 1 \pmod n$, y que además esto implica que r y n son coprimos. Así, nuevamente por la Observación 1.12.2 hay un morfismo

$$\phi\colon L \to \mathrm{Aut}(H)$$

tal que $\phi(b) = \phi_r$ si y sólo si $r^m \equiv 1 \pmod n$. Ahora podemos considerar el producto semidirecto $H \times_\phi L$. Claramente $H \times_\phi L$ está generado por a y b y además $a^n = 1$, $b^m = 1$ y $ba = a^r b$. Notemos finalmente que todo esto se puede generalizar facilmente al caso caso en que H es un grupo abeliano finito de exponente n.

Ejemplo 4. Fijemos $m \in \mathbb{N}$. Afirmamos el grupo cuaterniónico H_{2^m} de orden 2^{m+2} no es producto semidirecto de subgrupos no triviales. En efecto, para probar esto bastará ver que que la intersección de dos subgrupos no triviales de H_{2^m} no se reduce nunca a $\{1\}$, lo cual se sigue inmediatamente de que, por teorema de Lagrange y la Observación 1.6.4, todo subgrupo no trivial de H_{2^m} tiene algún elemento de orden 2 y de que, como vimos en el Ejemplo 4 de la subsección 1.6, H_{2^m} tiene un único elemento de orden 2. Acabamos de ver más precisamente que la intersección de todos los subgrupos no triviales de H_{2^m} tiene orden 2. Notemos además que, por el ejemplo que precede al Ejercicio 11, el único subgrupo de orden 2 de H_{2^m} es $\mathrm{Z}(H_{2^m})$ y que, por lo tanto, es invariante. Por último de la Proposición 1.6.14 se sigue que los otros subgrupos de H_2 también son invariantes y así todos los subgrupos de H_2 lo son. Los grupos, que como H_2, satisfacen esta propiedad se denominan *Hamiltonianos.*

Observación 1.15.3. *Supongamos que $\phi_1\colon L_1 \to Aut(H)$ y $\phi_2\colon L_2 \to Aut(H)$ son dos morfismos de grupos. Si $\sigma\colon L_1 \to L_2$ es un isomorfismo de grupos que satisface $\phi_2 \circ \sigma = \phi_1$, entonces la aplicación $\tau\colon H \times_{\phi_1} L_1 \to H \times_{\phi_2} L_2$, definida por $\tau(h, l) = (h, \sigma(l))$, también es un isomorfismo de grupos.*

Demostración. Es claro que basta ver que τ es un morfismo de grupos. En efecto

$$\tau((h, l)(h', l')) = \tau(h\phi_1(l)(h'), ll') = (h\phi_1(l)(h'), \sigma(ll'))$$

y

$$\tau(h, l)\tau(h', l') = (h, \sigma(l))(h', \sigma(l')) = (h\phi_2(\sigma(l))(h'), \sigma(l)\sigma(l')),$$

que coinciden claramente. □

Observación 1.15.4. *Supongamos que tenemos una equivalencia de extensiones*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\iota_H} & H \times_\phi L & \xrightarrow{\pi_L} & L & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_H} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_L} & & \\ 1 & \longrightarrow & H & \xrightarrow{\iota_H} & H \times_\psi L & \xrightarrow{\pi_L} & L & \longrightarrow & 1 \end{array}$$

Por la conmutatividad del segundo cuadrado,

$$\pi_L(\varphi(1,l)) = \pi_L(1,l) = l$$

y así existe $f\colon L \to H$ tal que $\varphi(1,l) = (f(l),l)$. En consecuencia, dado que por la conmutatividad del primer cuadrado,

$$\varphi(h,1) = \varphi(\iota_H(h)) = \iota_H(h) = (h,1),$$

tenemos que

$$\varphi(h,l) = \varphi\big((h,1)(1,l)\big) = \varphi(h,1)\varphi(1,l) = (h,1)(f(l),l) = (hf(l),l).$$

Así

$$\varphi\big((h,l)(h',l')\big) = \varphi\big(h(l\cdot_\phi h'),ll'\big) = \big(h(l\cdot_\phi h')f(ll'),ll'\big)$$

y

$$\varphi(h,l)\varphi(h',l') = (hf(l),l)(h'f(l'),l') = \big(hf(l)(l\cdot_\psi (h'f(l'))),ll'\big).$$

Por lo tanto el hecho de que φ es un morfismo de grupos se traduce en que

$$(l\cdot_\phi h')f(ll') = f(l)(l\cdot_\psi (h'f(l'))).$$

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

$$f(ll') = f(l)(l\cdot_\psi f(l')) \qquad y \qquad (l\cdot_\phi h')f(l) = f(l)(l\cdot_\psi h'). \tag{2}$$

Notemos que lo primero implica que $f(1) = 1$, ya que tomando $l = l' = 1$ obtenemos $f(1) = f(1)(1\cdot_\psi f(1)) = f(1)f(1)$, y que la igualdad $f(1) = 1$ la hemos usado para obtener la segunda condición. Reciprocamente si (2) vale, entonces

$$(l\cdot_\phi h')f(ll') = (l\cdot_\phi h')f(l)(l\cdot_\psi f(l')) = f(l)(l\cdot_\psi h')(l\cdot_\psi f(l')) = f(l)(l\cdot_\psi (h'f(l'))).$$

Notemos por último que la segunda de las condiciones (2) se puede expresar como

$$\phi(l)(h') = f(l)\psi(l)(h')f(l)^{-1},$$

lo que dice que $\phi(l) = \Phi_{f(l)}\circ\psi(l)$, donde $\Phi_{f(l)}$ es el automorfismo interior de H asociado a $f(l)$.

2.Grupo de permutaciones

En esta sección vamos a estudiar el grupo de permutaciones S_n. Ya sabemos que el orden de este grupo es $n!$. Una manera usual de denotar una permutación σ es la siguiente:

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

Para abreviar vamos a denotar con X al conjunto $\{1, \dots, n\}$, de modo que $\mathrm{S}_n = \mathrm{S}_X$. Dado $\sigma \in \mathrm{S}_n$ y $x \in X$ decimos que σ *fija* x si $\sigma(x) = x$ y que lo *mueve* si $\sigma(x) \neq x$. Dos permutaciones σ y τ son disjuntas si cada $x \in X$ movida por una de ellas es dejado fijo por la otra. Es facil ver que dos permutaciones disjuntas conmutan entre si y que si una permutación σ se escribe como un producto $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$ de permutaciones disjuntas dos a dos, entonces el conjunto de los puntos movidos por σ es igual a la unión disjunta de los conjuntos de puntos movidos por cada σ_i.

2.1.Estructura cíclica. Una permutación σ es un r-ciclo si existen $i_1, \dots, i_r \in X$ distintos, tales que σ deja fijos los elementos de $X \setminus \{i_1, \dots, i_r\}$ y

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

A σ la vamos a denotar con el símbolo $(i_1, \dots, i_r)$. Notemos que

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

El número r que aparece en la definición anterior es claramente el orden de σ. En particular el único 1-ciclo es la identidad. A los 2-ciclos se los suele llamar también *transposiciones*. Es inmediato que la cantidad de r-ciclos es $n(n-1)\dots(n-r+1)/r$.

Teorema 2.1.1. *Toda permutación σ se escribe como un producto $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$ de ciclos disjuntos dos a dos (y que por lo tanto conmutan entre si). Además el orden de σ es el mínimo de los múltiplos comunes de los órdenes de los σ_i's y esta escritura es única, salvo el orden en que aparecen sus factores, si se pide que los ciclos que aparecen en ella sean distintos de la identidad.*

Demostración. Veamos la existencia. Hacemos inducción en la cantidad k de elementos de X que son movidos por σ. Si $k = 0$, entonces $\sigma = \mathrm{id}$, que es un 1-ciclo. Supongamos que $k > 0$ y que el resultado vale para permutaciones que mueven menos que k elementos. Tomemos $i_1 \in X$ tal que $\sigma(i_1) \neq i_1$ y definamos $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$, $i_4 = \sigma(i_3)$, etcetera. Denotemos con r al mínimo número natural tal que $i_{r+1} \in \{i_1, \dots, i_r\}$ (este r existe pues X es finito). Es claro que $i_{r+1} = i_1$, pues si fuera $i_{r+1} = i_j$ con $j > 1$, tendríamos que $\sigma(i_r) = i_{r+1} = i_j = \sigma(i_{j-1})$, lo que contradice la inyectividad de σ. denotemos con σ_1 al r-ciclo definido por

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

Es claro que el conjunto de los puntos fijados por $\sigma_1^{-1} \circ \sigma$ es la unión disjunta de $\{i_1, \dots, i_r\}$ con el conjunto de los puntos fijados por σ. Así, por hipótesis inductiva $\sigma_1^{-1} \circ \sigma = \sigma_2 \circ \cdots \circ \sigma_s$, donde $\sigma_2, \dots, \sigma_s$ son ciclos disjuntos. Como el conjunto de los puntos movidos por $\sigma_2 \circ \cdots \circ \sigma_s$ es igual a la unión disjunta de los conjuntos de puntos movidos por cada σ_i con $1 < i \leq s$, sabemos que $\{i_1, \dots, i_r\}$ es dejado fijo

por cada σ_i con $1 < i \leq s$ y así, $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$ es un producto de ciclos disjuntos dos a dos. Veamos ahora la unicidad. Supongamos que

$$\sigma_1 \circ \cdots \circ \sigma_s = \sigma = \sigma'_1 \circ \cdots \circ \sigma'_{s'}.$$

son dos productos de ciclos de ordenes mayores que 1 y disjuntos. Tomemos i_1 movido por σ_1. Entonces i_1 es movido también por algún σ'_i y, como los σ'_i conmutan entre si, podemos suponer que $i = 1$. Es fácil ver que $\sigma_1^k(i_1) = \sigma^k(i_1) = {\sigma'_1}^k(i_1)$ para todo $k \in \mathbb{N}$. Pero entonces $\sigma_1 = \sigma'_1$ y así, $\sigma_2 \circ \cdots \circ \sigma_s = \sigma'_2 \circ \cdots \circ \sigma'_{s'}$. Un argumento inductivo muestra ahora que $s' = s$ y que $\{\sigma_2, \ldots, \sigma_s\} = \{\sigma'_2, \ldots, \sigma'_{s'}\}$. Denotemos con r_j al orden de σ_j, con r' al de σ y con r al mínimo de los múltiplos comunes de los r_j's. Resta ver que $r = r'$. Dado que $\sigma^r = \sigma_1^r \circ \cdots \circ \sigma_s^r = \mathrm{id}$, tenemos que r' divide a r. Por otro lado, 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 $1 \leq j \leq s$ y así r divide a r'. □

Por ejemplo del teorema anterior se sigue que los elementos de S_4 que son un 2-ciclo o producto de dos 2-ciclos disjuntos tienen orden 2, los 3-ciclos tienen orden 3 y los 4-ciclos, orden 4, etcetera.

Escribamos una permutación σ 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 $r_1 \leq r_2 \leq \cdots \leq r_s$. Claramente $r_1 + \cdots + r_s \leq n$ y $n - r_1 - \cdots - r_s$ es la cantidad de puntos fijos de σ. Denotemos con α_1 a esta cantidad y con α_j, para $1 < j \leq n$, a la cantidad de j-ciclos que aparecen en $\{\sigma_1, \ldots, \sigma_s\}$. 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 $r_1 \leq r_2 \leq \cdots \leq r_s$ tales que $r_1 + \cdots + r_s \leq n$ y el de los $\alpha_1, \ldots, \alpha_n \geq 0$ tales que $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n$. A la sucesión $(\alpha_1, \ldots, \alpha_n)$ la vamos a denominar la *estructura cíclica* de σ. Vale lo siguiente:

Teorema 2.1.2. *Dos permutaciones son conjugadas en* S_n *si y sólo si tienen la misma estructura cíclica. Además si*

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

y τ *es una permutación arbitraria, entonces*

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

Demostración. Claramente si $(i_1, \ldots, i_r)$ es un r-ciclo y τ es una permutación arbitraria, entonces

$$\tau \circ (i_1, \ldots, i_r) \circ \tau^{-1} = (\tau(i_1), \ldots, \tau(i_r)).$$

Así, 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. Supongamos ahora que σ y σ' son dos permutaciones que tienen la misma estructura cíclica.

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

y

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

Es claro entonces que si $\tau \in \mathrm{S}_n$ está definida por $\tau(i_j) = i'_j$ para $1 \leq j \leq r_s$ y $\tau(i) = i$ si $i \in X \setminus \{i_1, \dots, i_s\}$, entonces $\tau \circ \sigma \circ \tau^{-1} = \sigma'$. $\square$

Por el teorema anterior cada clase de conjugación de S_n se corresponde con la estructura cíclica $(\alpha_1, \dots, \alpha_n)$ de cada uno de sus elementos σ y así la cantidad de clases de conjugación de S_n es igual a la cantidad de sucesiones $\alpha_1, \dots, \alpha_n \geq 0$ que satisfacen $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n$. Para $1 \leq j \leq n$, denotemos con μ_j a $\alpha_j + \cdots + \alpha_n$. Entonces $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n$ y $\mu_1 + \cdots + \mu_n = n$. Recíprocamente dada una sucesión $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n$ tal que $\mu_1 + \cdots + \mu_n = n$, podemos definir $\alpha_j = \mu_j - \mu_{j+1}$, para $1 \leq j < n$ y $\alpha_n = \mu_n$ y claramente $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = \mu_1 + \cdots + \mu_n = n$. Como estas asignaciones son inversa una de la otra obtenemos que la cantidad de de clases de conjugación de S_n es igual a la cantidad de particiones $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n$ de n. Como ejemplo consideremos S_5. Las particiones de 5 son $(1,1,1,1,1)$, $(2,1,1,1,0)$, $(2,2,1,0,0)$, $(3,1,1,0,0)$, $(3,2,0,0,0)$, $(4,1,0,0,0)$ y $(5,0,0,0,0)$ y así, S_5 tiene 7 clases de conjugación. Por último la cantidad de elementos que tiene la clase de conjugación de S_n correspondiente a la estructura cíclica $(\alpha_1, \dots, \alpha_n)$ es

$$\frac{n!}{1^{\alpha_1}\alpha_1!2^{\alpha_2}\alpha_2! \dots n^{\alpha_n}\alpha_n!}. \tag{3}$$

En efecto, esto se sigue de que cada j-ciclo se puede obtener de j formas distintas

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

y que si permutamos entre si los α_j ciclos de orden j obtenemos la misma permutación de S_n. La expresión (3) es conocida como fórmula de Cauchy.

Observación 2.1.3. *Podemos usar el Teorema 2.1.2 para probar que si un morfismo de grupos $f\colon N \to G$ no es sobreyectivo, entonces tampoco es un epimorfismo. Denotemos con H a la imagen de f y supongamos que H es un subgrupo propio de G. Debemos ver que hay un grupo N y morfismos distintos $g, h\colon G \to N$ tales que $g_{|H} = h_{|H}$. Tomemos como N a S_X, donde X es la familia de las coclases a izquierda de H junto con un elemento adicional $*$. Definamos $g(a)$ como $g(a)(*) = *$ y $g(a)(bH) = abH$ y a h como $\Phi_\tau \circ g$, donde Φ_τ es la conjugación por la transposición τ de X que intercambia H con $*$. Es facil ver que $*$ es un punto fijo de $g(a)$ para todo $a \in G$ mientras que H es un punto fijo de $g(a)$ si y sólo si $a \in H$. Por el Teorema 2.1.2 se sigue de esto que $h(a) = \Phi_\tau(g(a)) = g(a)$ si y sólo si $a \in H$, que es más que lo que necesitábamos probar.*

2.2.Generadores de S_n. Un cálculo directo muestra que

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

y

$$(1, i_1) \circ (1, i_j) \circ (1, i_1) = (i_1, i_j) \qquad \text{si } i_i, i_j \neq 1.$$

Como cada permutación es producto de ciclos se sigue de esto que S_n está generado por las transposiciones $(1,2),(1,3),\ldots,(1,n)$. Dado que además tenemos que

$$(i,i+1)\circ(1,i)\circ(i,i+1)=(1,i+1)\qquad \text{si } 1<i<n,$$

un argumento inductivo muestra que transposiciones $(1,2),(2,3),\ldots,(n-1,n)$ también generan a S_n. Por último usando la igualdad

$$(1,\ldots,n)^{i-1}\circ(1,2)\circ(1,\ldots,n)^{-i+1}=(i,i+1),$$

válida para $1\leq i<n$, obtenemos que S_n está generado por $(1,2)$ y $(1,\ldots,n)$.

2.3.Paridad de una permutación. Subgrupo alternado. Vamos a definir un morfismo sobreyectivo sg de S_n en el grupo cíclico con dos elementos $\{\pm 1\}$. Este morfismo sg se llama el *signo* y su núcleo es un subgrupo normal de índice 2 de S_n, que se llama el grupo *alternado* A_n. El orden de A_n es claramente $n!/2$.

Una factorización de una permutación σ de S_n como producto de ciclos disjuntos

$$\sigma=\sigma_1\circ\cdots\circ\sigma_s,$$

es *completa* si contiene un 1-ciclo por cada elemento de X fijado por sigma. Así, $s=\alpha_1+\cdots+\alpha_n$, donde $(\alpha_1,\ldots,\alpha_n)$ es la estructura cíclica de σ. Definimos el signo $\mathrm{sg}(\sigma)$ de σ como $(-1)^{n-s}$.

Lema 2.3.1. *Si $k,l\geq 0$, entonces*

$$(a,b)\circ(a,c_1,\ldots,c_k,b,d_1,\ldots,d_l)=(a,c_1,\ldots,c_k)\circ(b,d_1,\ldots,d_l)$$

Demostración. Sale por cálculo directo. □

Teorema 2.3.2. *La aplicación* $\mathrm{sg}\colon \mathrm{S}_n\to\{\pm 1\}$ *es un morfismo sobreyectivo de grupos.*

Demostración. Es claro que sg es sobreyectiva ya que $\mathrm{sg}(\mathrm{id})=1$ y $\mathrm{sg}(1,2)=-1$. Veamos que es un morfismo de grupos. Tomemos σ y τ en S_n y escribamos τ como un producto de transposiciones $\tau=\tau_1\circ\cdots\circ\tau_r$. Denotemos con $\sigma=\sigma_1\circ\cdots\circ\sigma_s$ a la factorización completa de σ como producto de ciclos disjuntos. Vamos a probar por inducción en r que $\mathrm{sg}(\tau\circ\sigma)=\mathrm{sg}(\tau)\,\mathrm{sg}(\sigma)$. El caso $r=0$ es trivial ya que significa que $\tau=\mathrm{id}$. Supongamos ahora que $r=1$ y que $\tau=(a,b)$. Si a,b aparecen en un ciclo σ_i, entonces podemos suponer que $i=1$, y del Lema 2.3.1 se sigue facilmente que $\tau\circ\sigma_1$ se escribe como producto de ciclos disjuntos en la forma $\tau\circ\sigma_1=\sigma_1'\circ\sigma_1''$ y que la factorización completa de $\tau\circ\sigma$ es $\sigma_1'\circ\sigma_1''\circ\sigma_2\circ\cdots\circ\sigma_s$. En consecuencia, en este caso, $\mathrm{sg}(\tau\circ\sigma)=(-1)^{n-s-1}=(-1)^{n-(n-1)}(-1)^{n-s}=\mathrm{sg}(\tau)\,\mathrm{sg}(\sigma)$. Similarmente si a,b aparecen en un ciclos distintos σ_i y σ_j, entonces podemos suponer que $i=1$ y $j=2$, y del Lema 2.3.1 se sigue facilmente que $\tau\circ\sigma_1\circ\sigma_2$ es un ciclo σ' y que la factorización completa de $\tau\circ\sigma$ es $\tau\circ\sigma=\sigma'\circ\sigma_3\circ\cdots\circ\sigma_s$. Por lo tanto, en este caso, $\mathrm{sg}(\tau\circ\sigma)=(-1)^{n-s+1}=(-1)^{n-(n-1)}(-1)^{n-s}=\mathrm{sg}(\tau)\,\mathrm{sg}(\sigma)$. Supongamos ahora que $r>1$ y que el resultado vale para permutaciones τ que se escriben como un producto de menos que r transposiciones. Entonces

$$\begin{aligned}\mathrm{sg}(\tau\circ\sigma)&=\mathrm{sg}(\tau_1\circ\cdots\circ\tau_r\circ\sigma)\\&=-\mathrm{sg}(\tau_2\circ\cdots\circ\tau_r\circ\sigma)\\&=-\mathrm{sg}(\tau_2\circ\cdots\circ\tau_r)\,\mathrm{sg}(\sigma)\\&=\mathrm{sg}(\tau_1\circ\cdots\circ\tau_r)\,\mathrm{sg}(\sigma)\\&=\mathrm{sg}(\tau)\,\mathrm{sg}(\sigma),\end{aligned}$$

donde la segunda y cuarta igualdad se siguen del caso $r = 1$ y la tercera de la hipótesis inductiva. □

Vamos a decir que una permutación es *par si su signo es* 1 *y que es impar si es* -1. *Así* A_n *es el subgrupo de* S_n *formado por las permutaciones pares. Notemos que por definición*

$$\mathrm{sg}(i_1, \ldots, i_r) = (-1)^{n-(n-r+1)} = (-1)^{r-1}$$

y, por lo tanto, un r*-ciclo está en* A_n *si y sólo si* r *es impar.*

Observación 2.3.3. *La aplicación* $\theta\colon \mathrm{S}_n \to A_{n+2}$*, 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 2.3.4. A_n *está generado por los cuadrados de los elementos de* S_n.

Demostración. Es claro que $\langle \sigma^2 : \sigma \in \mathrm{S}_n \rangle \subseteq A_n$ ya que $\mathrm{sg}(\sigma^2) = \mathrm{sg}(\sigma)^2 = 1$ para todo $\sigma \in \mathrm{S}_n$. Para ver la inclusión recíproca es suficiente probar que el producto de dos transposiciones es un cuadrado y esto se sigue de que

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

donde $a, b, c, d \in X$ son elementos distintos. □

Notese que hemos probado que A_n está generado por los cuadrados de 3-cíclos y de 4-cíclos. Dado que $(a, b, c)^2 = (a, c, b)$ se sigue del proximo teorema que A_n está generado por los cuadrados de $(1, 3, 2), (1, 4, 2), \ldots, (1, n, 2)$.

Teorema 2.3.5. A_n *está generado por* $(1, 2, 3), (1, 2, 4), \ldots, (1, 2, n)$.

Demostración. Si $n < 3$ el teorema es trivial. Supongamos que $n \geq 3$. Es claro que todos los 3-ciclos están en A_n. Veamos primero que A_n está generado por ellos. En efecto, esto se sigue de que

$$(a, b) \circ (a, c) = (a, c, b) \quad \text{y} \quad (a, b) \circ (c, d) = (a, b, c) \circ (b, c, d)$$

donde $a, b, c, d \in X$ son elementos distintos. Dado para cada terna $a, b, c \in X$ de elementos distintos de 1, tenemos que

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

para terminar la demostraciń es suficiente ver que cada 3-ciclo $(1, a, b)$ con $a \neq 2$ se expresa como un producto de 3-ciclos de la forma $(1, 2, i)$ con $3 \leq i \leq n$, y esto es así, ya que

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

para cada par $a, b \in X$ de elementos distintos de 1 y 2. □

Teorema 2.3.6. *A_n está generado por $\{(i,i+1)\circ(j,j+1) : 1 \leq i < j < n\}$.*

Demostración. Es claro que cada permutación de la forma $(i,i+1)\circ(j,j+1)$ está en A_n. Por el Teorema 2.3.5, es suficiente ver que cada 3-ciclo $(1,2,a)$, con $3 \leq a \leq n$, está en el subgrupo H de A_n generado por las permutaciones $(i,i+1)\circ(j,j+1)$, donde $1 \leq i < j < n$. La demostración de este hecho sale facilmente por inducción en n, usando que $(1,2,3) = (1,2)\circ(2,3)$ y

$$\big((1,2)\circ(n,n+1)\circ(1,2,n)\circ(1,2)\circ(n,n+1)\big)^2 = (1,n+1,2)^2 = (1,2,n+1),$$

para todo $n \geq 3$. □

Teorema 2.3.7. *A_n está generado por $\{(i,i+1)\circ(1,2) : 1 < i < n\}$.*

Demostración. Es claro que cada permutación de la forma $(i,i+1)\circ(1,2)$ está en A_n. El resultado se sigue de que

$$\begin{aligned}
&(1,2)\circ(2,3) = (2,3)\circ(1,2)\circ(2,3)\circ(1,2),\\
&(1,2)\circ(j,j+1) = (j,j+1)\circ(1,2) && \text{for } 2 < j < n,\\
&(i,i+1)\circ(j,j+1) = (i,i+1)\circ(1,2)\circ(j,j+1)\circ(1,2) && \text{for } 1 < i < j < n.
\end{aligned}$$

y del Teorema 2.3.6. □

Proposición 2.3.8. *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 de orden dos σ (es decir que la descomposición cíclica de σ es un producto de una cantidad impar de transposiciones disjuntas), entonces H es el producto semidirecto de $H \cap A_n$ y $\{\mathrm{id}, \sigma\}$ (en particular S_n es el producto semidirecto de A_n y $\{\mathrm{id}, (1,2)\}$).*

Demostración. Tomemos $\sigma \in H \setminus A_n$. Es claro que la aplicación de

$$\theta\colon H \cap A_n \to H \setminus A_n,$$

definida por $\theta(\tau) = \tau\circ\sigma$ es biyectiva. Así $H \cap A_n$ es un subgrupo de índice 2 de H que, por lo tanto, es normal. Supongamos ahora que σ es una permutación impar de orden dos. Como $(H \cap A_n) \cap \{\mathrm{id}, \sigma\} = \{\mathrm{id}\}$ y $(H \cap A_n)\{\mathrm{id}, \sigma\} = H$, sabemos que H es el producto semidirecto de $H \cap A_n$ y $\{\mathrm{id}, \sigma\}$. □

Proposición 2.3.9. *Vale lo siguiente:*

1) A_4 no tiene subgrupos de orden 6.

2) El único subgrupo de orden 12 de S_4 es A_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 $\tau \in A_n$. Dado que si τ es un 3-ciclo, $\tau = \tau^4 = (\tau^2)^2$ deducimos de esto que H contiene a todos los 3-ciclos de S_4, lo que es absurdo ya que hay 8 de ellos.

2) Supongamos que $H \neq A_4$ es un subgrupo de orden 12 de S_4. Entonces, por la Proposición 2.3.8, $H \cap A_4$ es un subgrupo de orden 6 de A_4, lo que se contradice con el item 1). □

2.4.El conmutador y el centro. En esta subsección calculamos el conmutador y el centro de S_n y A_n.

Proposición 2.4.1. *Vale lo siguiente:*

1) $[\mathrm{S}_n, \mathrm{S}_n] = A_n$.

2) Si $n \geq 5$, *entonces* $[A_n, A_n] = A_n$.

Demostración. 1) Claramente $[\mathrm{S}_n, \mathrm{S}_n] \subseteq A_n$, ya que $\mathrm{sg}(\sigma) = \mathrm{sg}(\sigma^{-1})$ para todo $\sigma \in \mathrm{S}_n$ y así $\mathrm{sg}([\sigma, \tau]) = \mathrm{sg}(\sigma)\,\mathrm{sg}(\tau)\,\mathrm{sg}(\sigma^{-1})\,\mathrm{sg}(\tau^{-1}) = 1$. Veamos la inclusión recíproca. Esto es trivial si $n < 3$. Supongamos que $n \geq 3$. Por el Teorema 2.3.5, es suficiente ver que todo 3-ciclo está en $[\mathrm{S}_n, \mathrm{S}_n]$, lo que se sigue inmediatamente de que

$$(a, b, c) = (a, b) \circ (a, c) \circ (a, b) \circ (a, c) = [(a, b), (a, c)].$$

para toda terna a, b, c de elementos distintos de X.
2) Claramente $[A_n, A_n] \subseteq A_n$. Veamos la inclusión recíproca. Fijemos un 3-ciclo (a, b, c). Como $n \geq 5$ existen $d, e \in X$ tales que a ,b, c, d y e son todos distintos. Para terminar la demostración es suficiente ver que

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

lo que sale por cálculo directo. □

Observación 2.4.2. *Como* A_3 *es abeliano,* $[A_3, A_3] = \{1\}$. *En cuanto a* $[A_4, A_4]$ *debido a que el subgrupo*

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

de A_4 *es normal y* A_4/H *es abeliano, tenemos que* $[A_4, A_4] \subseteq H$. *Afirmamos que* $[A_4, A_4] = H$. *En efecto, la inclusión que falta, sale de que*

$$(1, 2) \circ (3, 4) = [(1, 2, 3), (1, 3, 4)],$$
$$(1, 3) \circ (2, 4) = [(1, 3, 2), (1, 2, 4)],$$
$$(1, 4) \circ (2, 3) = [(1, 4, 2), (1, 2, 3)].$$

Proposición 2.4.3. *Vale lo siguiente:*

1) Si $n \geq 3$, *entonces* $\mathrm{Z}(\mathrm{S}_n) = \{1\}$.

2) Si $n \geq 4$, *entonces* $\mathrm{Z}(A_n) = \{1\}$.

Demostración. 1) Tomemos $\sigma \in \mathrm{S}_n$. Si en la descomposición cíclica de σ hay dos ciclos no triviales, $\sigma = (i_1, i_2, \dots) \circ (j_1, j_2, \dots) \circ \cdots$, entonces tomando $\tau = (i_1, j_1, j_2)$ obtenemos

$$\tau \circ \sigma \circ \tau^{-1} = (j_1, i_2, \dots) \circ (j_2, i_1, \dots) \circ \cdots \neq \sigma.$$

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

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

Finalmente si σ es una transposición (i_1, i_2), entonces existe $i_3 \in X$ distinto de i_1 e i_2 y tomando $\tau = (i_1, i_3)$ obtenemos

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

2) Tomemos $\sigma \in A_n$. Si en la descomposición cíclica de σ hay dos ciclos no triviales, entonces podemos proceder como en el item 1), pues la permutación τ que hemos tomado alli está en A_n. Si σ es un ciclo $(i_1, i_2, i_3, i_4 \dots)$ de longitud al menos 5, entonces tomando $\tau = (i_1, i_2) \circ (i_3, i_4)$ obtenemos

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

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 $\tau = (i_1, i_2) \circ (i_3, i_4)$ obtenemos

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

lo que termina la demostración. □

Notemos que $\mathrm{Z}(\mathrm{S}_2) = \mathrm{S}_2$ y $\mathrm{Z}(A_3) = A_3$, ya que estos grupos son conmutativos.

2.5.Simplicidad de A_n con $n \neq 4$. Claramente $\mathbb{Z}_p$ es simple para todo primo p. Esta es la familia más sencilla de grupos simples y estos son todos los grupos simples conmutativos. A continuación vamos a obtener otra familia de grupos simples. Vale lo siguiente:

Teorema 2.5.1. *A_n es simple para todo $n \geq 3$ y distinto de 4.*

Demostración. Es claro que A_3 es simple. Así podemos suponer que $n \geq 5$. Tomemos un subgrupo normal $H \neq \{1\}$ de A_n. Afirmamos que H tiene todos los 3-ciclos y que, por lo tanto, es igual a A_n. Para probar esto vamos a usar el argumento desarrollado en la demostración de la Proposición 2.4.3. Fijemos $\sigma \in H$ distinto de la identidad.

1) Si $\sigma = (i_1, i_2, \dots) \circ (j_1, j_2, \dots) \circ \cdots$ tiene dos ciclos no triviales en su descomposición cíclica, entonces tomando $\tau = (i_1, j_1, j_2)$, obtenemos

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

si el ciclo $(j_1, j_2, \dots)$ tiene más de dos elementos y

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

si tiene exactamente dos.

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

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

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

Así que tenemos tres casos: $\varrho = (i_1, i_2) \circ (i_3, i_4)$ es un producto de dos 2-ciclos, $\varrho = (i_1, i_2, i_3, i_4, i_5)$ es un 5-ciclo o $\varrho = (i_1, i_2, i_3)$ es un 3-ciclo. En el primer caso, existe $i_5 \notin \{i_1, i_2, i_3, i_4\}$ y tomando $u = (i_2, i_5, i_3)$, obtenemos

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

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

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

lo que nos lleva al tercer caso y así concluímos que H 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 2.1.2, existe $t \in \mathrm{S}_n$ tal que $(j_1, j_2, j_3) = t \circ (i_1, i_2, i_3) \circ t^{-1}$. Si $t \in A_n$ entonces $(j_1, j_2, j_3) \in H$ por definición. Si esto no es así, podemos tomar $k_1, k_2 \in X \setminus \{j_1, j_2, j_3\}$ distintos y, entonces

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

Como $t \notin A_n$ implica que $(k_1, k_2) \circ t \in A_n$, se sigue de esto que $(j_1, j_2, j_3) \in H$. □

Notemos que debido al hecho de que todo subgrupo de índice 2 de un grupo es invariante del teorema anterior se sigue en particular que A_n no tiene subgrupos de orden $n!/4$ para ningún $n \geq 5$. Esto prueba que el el item 1) de la Proposición 2.3.9 vale en general. La siguiente proposición prueba en particular que también vale el item 2).

Teorema 2.5.2. *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 así, por el Teorema 2.5.1, $H \cap A_n = A_n$ o $H \cap A_n = \{1\}$. Como A_n tiene índice 2, lo primero inplica que $H = A_n$. Para terminar la demostración, debemos ver que el caso $H \cap A_n = \{1\}$ es imposible. Por la Proposición 2.3.8, debe ser $H = \{\tau, \mathrm{id}\}$ con τ de orden 2. Pero entonces τ es un producto de 2-ciclos disjuntos y, por el Teorema 2.1.2, su clase de conjugación tiene claramente más de un elemento. Esto contradice el hecho de que $H = \{\tau, \mathrm{id}\}$ es normal, ya que entonces debe contener a toda la clase de conjugación de τ. □

2.6.Presentación por generadores y relaciones. A continuación vamos a dar presentaciones de S_n y A_n por generadores y relaciones.

Teorema 2.6.1. S_n *es el grupo generado por $s_1, \ldots, s_{n-1}$ sujeto a las relaciones*

$$\begin{aligned} &s_i^2 = 1, && \text{para } 1 \leq i < n, \\ &s_i s_j = s_j s_i, && \text{para } 1 < i+1 < j < n, \\ &s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, && \text{para } 1 \leq i < n-1, \end{aligned}$$

para todo $n \geq 2$.

Demostración. Supongamos que para algún n el resultado es falso y tomemos el mínimo para el que falla. Es claro que $n > 2$. Denotemos con G al grupo generado por $s_1, \ldots, s_{n-1}$ sujeto a las relaciones mencionadas arriba. Es inmediato que hay una aplicación $\phi\colon G \to \mathrm{S}_n$, que está definida por $\phi(s_i) = (i, i+1)$ y que esta aplicación es sobreyectiva. Para terminar la demostración debemos ver que también es inyectiva, lo que se seguirá si probamos que $|G| \leq n!$. Claramente el subgrupo G' de G generado por $s_1, \ldots, s_{n-2}$ es un cociente del grupo generado por $s_1, \ldots, s_{n-2}$ sujeto a relaciones similares a las de arriba, y así $|G'| \leq (n-1)!$ debido a la

definición de n. Consideremos ahora los subconjuntos $C_1, \ldots, C_n$ de G, definidos por $C_i = G's_{n-1}s_{n-2}\cdots s_{i+1}s_i$. Afirmamos que para cada $1 \leq i \leq n$ y $1 \leq j < n$ existe $1 \leq i' \leq n$ tal que $C_i s_j = C_{i'}$. En efecto

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

y

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

para $1 \leq j < n$. 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 anteúltima igualdad se sigue de que $s_j \in G'$ ya que $j < i-1 \leq n-1$. Finalmente, si $i < j$,

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

donde la anteúltima igualdad se sigue de que $s_{j-1} \in G'$ ya que $j-1 < n-1$. En consecuencia cualquiera sea $s \in G$, vale que para cada $1 \leq i \leq n$ existe $1 \leq i' \leq n$ tal que $C_i s = C_{i'}$, ya que s es producto de s_j's. En particular, dado que $1 \in G' = C_n$ obtenemos tomando $i = n$ y variando s que $G \subseteq \bigcup_{i=1}^{n} C_i$, de donde $|G| \leq \sum_{i=1}^{n} |C_i| = n|G'| \leq n!$. $\square$

Observación 2.6.2. *Claramente las relaciones que satisfacen $s_1, \ldots, s_{n-1}$ son equivalentes a*

$$\begin{aligned} &s_i^2 = 1, && \text{para } 1 \leq i < n, \\ &(s_i s_j)^2 = 1, && \text{para } 1 < i+1 < j < n, \\ &(s_i s_{i+1})^3 = 1, && \text{para } 1 \leq i < n-1. \end{aligned}$$

Teorema 2.6.3. *A_n es el grupo generado por $t_1, \ldots, t_{n-2}$ sujeto a las relaciones*

$$\begin{aligned} &t_1^3 = 1, \\ &t_i^2 = 1, && \text{para } 1 < i < n-1, \\ &(t_i t_j)^2 = 1, && \text{para } 1 < i+1 < j < n-1, \\ &(t_i t_{i+1})^3 = 1, && \text{para } 1 \leq i < n-2, \end{aligned}$$

para todo $n \geq 3$.

Demostración. Denotemos con G al grupo generado por $t_1, \ldots, t_{n-2}$ sujeto a las relaciones mencionadas arriba. Es fácil ver que hay un morfismo $\psi\colon G \to A_n$, que está definido por $\psi(t_i) = (i+1, i+2) \circ (1,2)$. Como, por el Teorema 2.3.7, este morfismo es sobreyectivo, para terminar la demostración es suficiente ver que $|G| \leq n!/2$. Denotemos con G' al grupo generado por $s_1, t_1, \ldots, t_{n-2}$, sujeto a las relaciones

$$\begin{aligned}
&s_1^2 = t_1^3 = 1, \\
&s_1 t_i s_1 = t_i^{-1}, && \text{para } 1 \leq i < n-1, \\
&t_i^2, && \text{para } 1 < i < n-1, \\
&(t_i t_j)^2 = 1, && \text{para } 1 < i+1 < j < n-1, \\
&(t_i t_{i+1})^3 = 1, && \text{para } 1 \leq i < n-2.
\end{aligned}$$

Escribamos $s_{i+1} = t_i s_1$ para $1 \leq i < n-1$. La relaciones mencionadas arriba para $s_1, t_1, \ldots, t_{n-2}$ son equivalentes a las relaciones mencionadas en la Observación 2.6.2 para $s_1, \ldots, s_{n-1}$. Así,

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

Claramente hay un morfismo $\phi\colon \mathbb{Z}_2 \to \mathrm{Aut}(G)$, que está definido por $\phi(1)(t_i) = t_i^{-1}$. Por ejemplo la relación $(t_1 t_2)^3 = 1$ se transforma por $\phi(1)$ en $(t_1^2 t_2)^3 = 1$, la cual vale ya que

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

Es fácil ver ahora que hay un morfismo de grupos $\varphi\colon G' \to G \times_\phi \mathbb{Z}_2$, que está definido por $\varphi(t_i) = (t_i, 0)$ y $\varphi(s_1) = (0,1)$, y que este morfismo es sobreyectivo. Por lo tanto $|G| \leq |G'|/2 = n!/2$. $\square$

2.7.Grupo de automorfismos de S_n. Supongamos que $n \geq 3$. Por la Proposición 2.4.3 el morfismo $\mathrm{S}_n \to \mathrm{Aut}(\mathrm{S}_n)$, que manda $\sigma \in \mathrm{S}_n$ en el automorfismo interior Φ_σ, es inyectivo. Vamos a probar a continuación que si $n \neq 6$, entonces también es sobreyectivo o, lo que es lo mismo, que $\mathrm{Aut}(\mathrm{S}_n) = \mathrm{Int}(\mathrm{S}_n)$.

Teorema 2.7.1. *Si $n \geq 3$ y $n \neq 6$, entonces todo automorfismo de S_n es interior*

Demostración. Tomemos un automorfismo φ de S_n. Como $(1,2,3)$ tiene orden 3, entonces el orden de $\varphi((1,2,3))$ también es 3 y así es un producto de una cantidad $r \geq 1$ de 3-ciclos disjuntos. Por otro lado como φ es un automorfismo, las clases de conjugación de $(1,2,3)$ y $\varphi((1,2,3))$ tienen la misma cantidad de elementos. Por la fórmula de Cauchy esto dice que

$$\frac{n!}{3(n-3)!} = \frac{n}{3^r r!(n-3r)!} \quad \text{o equivalentemente a} \quad \frac{r!3^{r-1}}{(3r-3)!} = \binom{n-3}{3r-3}.$$

Calculemos las posibles soluciones de esta igualdad. Si $r = 1$, entonces n puede ser cualquiera. Si $r = 2$, entonces la igualdad de arriba queda

$$1 = \binom{n-3}{3} = \frac{(n-3)(n-4)(n-5)}{6},$$

lo que implica que $n = 6$ (caso que hemos excluído). Supongamos ahora que $r \geq 3$. Entonces $3r - 3 \geq r + 2$ y así

$$\frac{r!3^{r-1}}{(3r-3)!} = \frac{3^{r-1}}{(3r-3)(3r-4)A}$$

donde A es un número natural. Como $(3r-3)(3r-4)$ es par esta fracción no es un número entero y, por lo tanto, no puede ser igual a $\binom{n-3}{3r-3}$. En consecuencia $\varphi((1,2,3))$ es un 3-ciclo. Escribamos $(a, b, c_3) = \varphi(1, 2, 3)$. Afirmamos que existen $c_4, \ldots, c_n \in \{1, \ldots, n\} \setminus \{a, b, c_3\}$, todos distintos, tales que

$$\varphi(1, 2, i) = (a, b, c_i) \qquad \text{para } 3 \leq i \leq n.$$

Tomemos $3 < i \leq n$ y escribamos $(a', b', c_i) = \varphi(1, 2, i)$. Como

$$(1, 2, 3) \circ (1, 2, i) = (1, 3) \circ (2, i)$$

tiene orden 2 también el orden de $(a, b, c_3) \circ (a', b', c_i) = \varphi((1, 2, 3) \circ (1, 2, i))$ debe ser 2. Si a, b, c_3, a', b', c_i son todos distintos, entonces $(a, b, c_3) \circ (a', b', c_i)$ tiene orden 3. Si en a, b, c_3, a', b', c_i hay un elemento en común, entonces podemos suponer que $a' = a$ y así $(a, b, c_3) \circ (a, b', c_i) = (a, b', c_i, b, c_3)$ tiene orden 5. Si en a, b, c_3, a', b', c_i hay dos elementos en común, entonces como antes podemos suponer que $a' = a$ y que $c_i = b$ o $b' = b$. En el primer caso $(a, b, c_3) \circ (a, b', b) = (a, b', c_3)$ tiene orden 3 y en el segundo $(a, b, c_3) \circ (a, b, c_i) = (b, c_i) \circ (a, c_3)$ tiene orden 2. Si en a, b, c_3, a', b', c_i hay tres elementos en común, entonces como antes podemos suponer que $a' = a$ y que $c_i = b$ y $b' = c_3$, o $b' = b$ y $c_i = c_3$. En el primer caso $(a, b, c_3) \circ (a, c_3, b) = \mathrm{id}$ tiene orden 1 y en el segundo $(a, b, c_3) \circ (a, b, c_3) = (a, c_3, b)$ tiene orden 3. En consecuencia el único caso posible es $a' = a$, $b' = b$ y $c_i \neq c_3$. Definamos $\sigma \in \mathrm{S}_n$ por $\sigma(1) = a$, $\sigma(2) = b$ y $\sigma(i) = c_i$ para $3 \leq i \leq n$. Afirmamos que $\varphi(\tau) = \sigma \circ \tau \circ \sigma^{-1}$ para todo $\sigma \in A_n$. Por el Teorema 3.2.5 basta ver que esto ocurre para $\tau = (1, 2, i)$ con $3 \leq i \leq n$, pero

$$\varphi((1, 2, i)) = (a, b, c_i) = (\sigma(1), \sigma(2), \sigma(i)) = \sigma \circ (1, 2, i) \circ \sigma^{-1}.$$

Como S_n est a generado por A_n y $(1, 2)$ para terminar la demostración es suficiente ver que $\varphi((1, 2)) = \sigma \circ (1, 2) \circ \sigma^{-1}$. Escribamos $\varsigma = \sigma^{-1} \circ \varphi((1, 2)) \circ \sigma$. Para todo $\tau \in A_n$ tenemos

$$\begin{aligned}
\varsigma \circ \tau \circ \varsigma^{-1} &= \sigma^{-1} \circ \varphi((1,2)) \circ \sigma \circ \tau \circ \sigma^{-1} \circ \varphi((1,2)) \circ \sigma \\
&= \sigma^{-1} \circ \varphi((1,2)) \circ \varphi(\tau) \circ \varphi((1,2)) \circ \sigma \\
&= \sigma^{-1} \circ \varphi((1,2) \circ \tau \circ (1,2)) \circ \sigma \\
&= (1,2) \circ \tau \circ (1,2),
\end{aligned}$$

donde la última igualdad se sigue de que $(1, 2) \circ \tau \circ (1, 2) \in A_n$. Tomando $\tau = (1, 2, i)$ obtenemos

$$\varsigma \circ (1, 2, i) \circ \varsigma^{-1} = (1, 2) \circ (1, 2, i) \circ (1, 2) = (2, 1, i).$$

Así $\varsigma(1) = 2$, $\varsigma(2) = 1$ y $\varsigma(i) = i$ para todo $3 \leq i \leq n$, de modo de que $\varsigma = (1, 2)$. Volviendo al definición de ς obtenemos de esto que $(1, 2) = \sigma^{-1} \circ \varphi((1, 2)) \circ \sigma$ o, equivalentemente, $\varphi((1, 2)) = \sigma \circ (1, 2) \circ \sigma^{-1}$. $\square$

3. Acciones de grupos sobre conjuntos

3.1. Acciones y G-conjuntos. Una *acción a izquierda* de un grupo G sobre un conjunto X es una función

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

que satisface:

1) $(ab)\cdot x = a\cdot(b\cdot x)$, para todo $a, b \in G$ y $x \in X$.
2) $1\cdot x = x$, para todo $x \in X$,

donde hemos escrito $a \cdot x$ en lugar de $\rho(a, x)$. Un *G-conjunto a izquierda* es un conjunto X provisto de una acción a izquieda de G en X.

Observación 3.1.1. *Tener una función $\rho\colon G\times X \to X$ es lo mismo que tener una función $\widetilde{\rho}\colon G \to Fun(X, X)$. En efecto dada ρ podemos definir $\widetilde{\rho}$ por $\widetilde{\rho}(a)(x) = \rho(a, x)$ y dada $\widetilde{\rho}$ podemos definir ρ por $\rho(a, x) = \widetilde{\rho}(a)(x)$ y evidentemente ambas construcciones son recíprocas una de la otra. Ahora la condición 1) dada arriba es claramente equivalente a que $\widetilde{\rho}(ab) = \widetilde{\rho}(a)\circ\widetilde{\rho}(b)$ y la 2) a que $\widetilde{\rho}(1) = \mathrm{id}$. De esto se sigue que $\widetilde{\rho}(a)$ es biyectiva para cada a, ya que $\widetilde{\rho}(a^{-1})\circ\widetilde{\rho}(a) = \widetilde{\rho}(1) = \mathrm{id}$ y así, la imagen de $\widetilde{\rho}$ está incluída en el grupo de permutaciones S_X de X. Recíprocamente si $\widetilde{\rho}\colon G \to \mathrm{S}_X$ satisface $\widetilde{\rho}(ab) = \widetilde{\rho}(a)\circ\widetilde{\rho}(b)$ entonces también tenemos $\widetilde{\rho}(1) = \mathrm{id}$ y así la aplicación $\rho\colon G \times X \to X$ asociada a $\widetilde{\rho}$ es una acción de G sobre X.*

Similarmente se define una *acción a derecha* de un grupo G sobre un conjunto X como una función $\rho\colon X \times G \to X$ que satisface:

1) $x\cdot(ab) = (x\cdot a)\cdot b$, para todo $a, b \in G$ y $x \in X$.
2) $x = x\cdot 1$, para todo $x \in X$,

donde $x\cdot a$ signfica $\rho(x, a)$ y un *G-conjunto a derecha* como un conjunto X provisto de una acción a derecha de G en X. Dada una función $\rho\colon X \times G \to X$ podemos definir $\rho^{\mathrm{op}}\colon G^{\mathrm{op}} \times X \to X$ por $\rho^{\mathrm{op}}(a, x) = \rho(x, a)$. Es fácil ver que ρ es una acción a derecha de G sobre X si y sólo si ρ^{op} es una acción a izquierda de G^{op} sobre X. Así tener un G-conjunto a derecha es lo mismo que tener un G^{op}-conjunto a izquierda. También es facil ver que tener una función $\rho\colon X\times G \to X$ es lo mismo que tener una función $\widetilde{\rho}\colon G \to Fun(X, X)$ y que ρ es una acción a derecha si y sólo si $\widetilde{\rho}(1) = \mathrm{id}$ y $\widetilde{\rho}(ab) = \widetilde{\rho}(b)\circ\widetilde{\rho}(a)$. Además en este caso la imagen de $\widetilde{\rho}$ está incluída en S_X. Notemos que las condiciones que acabamos de ver dicen que $\widetilde{\rho}$ es un morfismo de grupos de G^{op} en S_X (o, lo que es lo mismo, de G en $\mathrm{S}_X^{\mathrm{op}}$). Debido a todo esto salvo mención en contrario trabajaremos sólo con G-acciones y G-conjuntos a izquierda (nos referiremos a ellos simplemente como G-acciones y G-conjuntos) y dejaremos al lector la sencilla tarea de dar las definiciones y propiedades para G-conjuntos a derecha.

Núcleo de una acción y acciones fieles. El núcleo de una acción $\rho\colon G\times X \to X$ es $\mathrm{Ker}(\rho) = \{a \in G : a\cdot x = x \text{ para todo } x \in X\}$. Claramente este conjunto coincide con el núcleo del morfismo $\widetilde{\rho}\colon G \to \mathrm{S}_X$ asociado a ρ y, por lo tanto, es un subgrupo normal de G. Además es claro que queda definida una acción de $G/\mathrm{Ker}(\rho)$ sobre X poniendo $\overline{a}\cdot x = a\cdot x$, donde $\overline{a}$ denota a la clase de elemento $a \in G$ en $G/\mathrm{Ker}(\rho)$ (esta definición es correcta ya que si $b \in \mathrm{Ker}(\rho)$, entonces $(ab)\cdot x = a\cdot(b\cdot x) = a\cdot x$). Notemos que el núcleo de esta nueva acción es $\{1\}$. Una acción $\rho\colon G \times X \to X$ cuyo núcleo es $\{1\}$ es llamada *fiel*. En este caso el morfismo $\widetilde{\rho}\colon G \to \mathrm{S}_X$ es inyectivo y así G es isomorfo a un subgrupo de S_X. Veamos una aplicación de esto. Todo

grupo G actúa sobre el conjunto G/H de las coclases a izquierda de un subgrupo suyo H por la acción ρ dada traslaciones a izquierda, es decir que $a\cdot(bH) = abH$. El núcleo de esta acción es el máximo subgrupo $N = \bigcap_{a\in G} aHa^{-1}$ de H que es normal en G. En particular tomando $H = \{1\}$ obtenemos el siguiente

Teorema 3.1.2. *Supongamos que G es un grupo finito. La aplicación $\widetilde{\rho}\colon G \to \mathrm{S}_G$, definida por $\widetilde{\rho}(a)(b) = ab$, es un morfismo inyectivo de grupos.*

En particular, por la subsección 2.2, todo grupo finito es un subgrupo de un grupo generado por dos elementos y, por la Observación 2.3.3 y el Teorema 2.5.1, todo grupo finito es un subgrupo de un grupo simple. Este es el famoso teorema de Cayley que dice que todo grupo G es isomorfo a un subgrupo del grupo de permutaciones S_G. Veamos una aplicación de este resultado.

Proposición 3.1.3. *Supongamos que G tiene orden $n = 2^k m$ con $k \geq 1$ y $m \geq 1$ impar. Denotemos con $\widetilde{\rho}\colon G \to \mathrm{S}_n$ a la representación de Cayley. Para todo $a \in G$ vale que 2^k divide a $|a|$ si y sólo si $\widetilde{\rho}(a) \notin A_n$. En consecuencia si G tiene un elemento a tal que 2^k divide a $|a|$, entonces G tiene un subgrupo de índice 2.*

Demostración. Supongamos que $|a| = 2^{k'}m'$ con $0 \leq k' \leq k$ y m' un divisor positivo de m. Por su definición, $\widetilde{\rho}(a)$ es un producto de $2^{k-k'}m/m'$ ciclos disjuntos de longitud $2^{k'}m'$. Dado que estos ciclos son permutaciones impares si y sólo si $k' > 0$ y que $2^{k-k'}m/m'$ es impar si y sólo si $k' = k$, resulta que $\widetilde{\rho}(a) \notin A_n$ si y sólo si $k' = k$. Así, si G tiene un elemento a tal que 2^k divide a $|a|$, entonces por la Proposición 2.3.8, $\widetilde{\rho}(G)$ (y por lo tanto también G) tiene un subgrupo de índice 2. □

Ejercicio 20. *Pruebe que si G es un grupo simple de orden par y $|G| = 2^k m$ con m impar, entonces $k > 1$ y G no tiene ningún elemento a tal que 2^k divide a $|a|$.*

Volvamos al caso general en que H no necesariamente es $\{1\}$. Supongamos que su índice es n. Entonces el morfismo $\widetilde{\rho}\colon G \to \mathrm{S}_{G/H}$, asociado a ρ, induce una una inclusión de G/N en $\mathrm{S}_{G/H}$ y así el índice $|G : N|$ de N en G divide a $|\,\mathrm{S}_{G/H}\,| = n!$. Como también $n = |G : H|$ divide a $|G : N|$, tenemos el siguiente

Teorema 3.1.4. *Todo subgrupo H de índice n de un grupo G contiene un subgrupo normal N de G cuyo índice en G es nh con h un divisor de $(n-1)!$. Además la función $\widetilde{\rho}\colon G \to \mathrm{S}_{G/H} \simeq \mathrm{S}_n$ induce un isomorfismo de G/N en $\mathrm{Im}(\widetilde{\rho}) \subseteq \mathrm{S}_{G/H} \simeq \mathrm{S}_n$.*

Ejercicio 21. *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 $n = 4$.*

Notemos que el Teorema 3.1.4 generaliza al teorema de Cayley. Así, por ejemplo tenemos el siguiente

Corolario 3.1.5. *Si G es simple y tiene un subgrupo H de índice $n > 1$, entonces el morfismo $\widetilde{\rho}\colon G \to \mathrm{S}_{G/H} \simeq \mathrm{S}_n$ es inyectivo. Esto implica en particular que $|G| \leq n!$ y, en consecuencia, ningún grupo simple infinito tiene subgrupos propios de índice finito.*

Demostración. Pues $N = \mathrm{Ker}(\widetilde{\rho}) \subseteq H \subsetneq G$ y por lo tanto debe ser $\{1\}$ ya que G es simple. □

Para comparar el Teorema de Cayley con el Teorema 3.1.4 y su Corolario 3.1.5 podemos notar que el Teorema de Cayley dice que A_n es un subgrupo de $\mathrm{S}_{n!/2}$

(en realidad de $A_{n!/2}$ por la Proposición 3.1.3), mientras que por otra parte A_n tiene un subgrupo $H \simeq A_{n-1}$, de índice n, y así el Teorema 3.1.4 dice que hay un morfismo no nulo $\widetilde{\rho}\colon A_n \to \mathrm{S}_n$. Cuando $n \neq 4$ este morfismo es inyectivo, ya que A_n es simple. En el caso $n = 4$ tenemos que $\mathrm{Ker}(\widetilde{\rho}) \subseteq H \simeq A_3$ y así $\mathrm{Ker}(\widetilde{\rho}) = H$ o $\mathrm{Ker}(\widetilde{\rho}) = \{\mathrm{id}\}$, pero lo primero no puede pasar ya que H no es un subgrupo normal de A_4, pues por ejemplo $(2,3,4)\circ(1,2,3)\circ(2,3,4)^{-1} = (1,3,4)$ no pertenece a H. Nuevamente, usando la Proposición 3.1.3, podemos ver que la imagen de $\widetilde{\rho}$ está incluída en A_n.

Corolario 3.1.6. *Supongamos que G es un grupo finito y que $|G| = nm$. Todo subgrupo H de índice n de G contiene un subgrupo normal N de G cuyo índice en G es nh, con h un divisor de $\mathrm{mdc}((n-1)!, m)$, donde $\mathrm{mdc}((n-1)!, m)$ denota al máximo de los divisores comunes de $(n-1)!$ y m. En particular si todos los primos que aparecen en la factorización de m son mayores que el máximo primo que es menor o igual que $n-1$, entonces todo subgrupo H de orden m de G es normal.*

Demostración. Por el teorema anterior H contiene un subgrupo normal N de G cuyo índice es nh con h un divisor de $(n-1)!$. Como $|G : N|$ también divide a $|G| = nm$, tenemos h es un divisor de $\mathrm{mdc}((n-1)!, m)$. □

Corolario 3.1.7. *Supongamos que G es un grupo finito y denotemos con p al mínimo primo que divide a $|G|$. Todo subgrupo de G de índice p es normal.*

Subconjuntos estables y morfismos. Decimos que un subconjunto Y de un G-conjunto X es *estable por la acción de G* o simplemente *estable* si $a\cdot y \in Y$ para todo $a \in G$ e $y \in Y$. En este caso Y mismo es un G-conjunto con la misma acción que la de G sobre X. Decimos también que Y es un *G-subconjunto* de X. Un morfismo $f\colon X \to X'$, entre dos G conjuntos X y X' es una función f que satisface $f(a\cdot x) = a\cdot f(x)$ para todo $a \in G$ y $x \in X$. Por ejemplo la inclusión canónica de un G-subconjunto Y de un G-conjunto X en X es un morfismo de G-conjuntos y también la composición de dos morfismos de G-conjuntos lo es. Un *endomorfismo* de X es un morfismo con dominio y codominio X. Un ejemplo es la función identidad de X. Un morfismo $f\colon X \to X'$ es un *isomorfismo* si existe un morfismo $f^{-1}\colon X' \to X$, necesariamente único, llamado la *inversa* de f, tal que $f\circ f^{-1} = \mathrm{id}_{X'}$ y $f^{-1}\circ f = \mathrm{id}_X$. Es fácil ver que esto ocurre si y sólo si f es biyectiva. Un *automorfismo* de X es un endomorfismo de X que es un isomorfismo. Los símbolos $\mathrm{Hom}_G(X, X')$, $\mathrm{Iso}_G(X, X')$, $\mathrm{End}_G(X)$ y $\mathrm{Aut}_G(X)$ denotan respectivamente a los conjuntos de morfismos de X en X', isomorfismos de X en X', endomorfismos de X y automorfismos de X. Notemos que $\mathrm{End}_G(X)$, dotado de la operación dada por la composición de morfismos, es un monoide que tiene a la identidad de X como unidad, y que además $\mathrm{Aut}_G(X) = \mathrm{End}_G(X)^*$.

Algunos ejemplos. A continuación damos algunos ejemplos más de G-conjuntos.

Ejemplo 1. G actúa sobre todo conjunto X no vacío via $a\cdot x = x$ para todo $a \in G$ y todo $x \in X$. Esta acción es llamada la *acción trivial* de G sobre X y su núcleo es claramente G.

Ejemplo 2. G actúa sobre si mismo por conjugación, es decir que $a\cdot b = aba^{-1}$. El núcleo de esta acción es claramente el centro de G.

Ejemplo 3. G actúa sobre cada subgrupo normal H suyo por conjugación, es decir que $a{\cdot}b = aba^{-1}$. El núcleo de esta acción es claramente el centralizador $\mathrm{C}_G(H)$ de H en G. Cuando $H = G$ nos reducimos al Ejemplo 2.

Ejemplo 4. Si H y K son subgrupos de un grupo G y $H \subseteq \mathrm{N}_G(K)$, entonces K actúa sobre H por conjugación, es decir que $a{\cdot}b = aba^{-1}$. El núcleo de esta acción es claramente $K \cap \mathrm{C}_G(H)$. Cuando $K = G$ nos reducimos al Ejemplo 3.

Ejemplo 5. Todo subgrupo H de un grupo G actúa sobre G via $a \cdot b = ab$ para todo $a \in H$ y todo $b \in G$. Esta acción es llamada la *acción de H sobre G por traslaciones a izquierda* y es claramente fiel.

Ejemplo 6. G actúa sobre el conjunto $P(G)$ de los subconjuntos de G por conjugación, es decir que $a{\cdot}X = aXa^{-1}$. El núcleo de esta acción es el centro de G. El conjunto $S(G)$ de los subgrupos de G es claramente estable y así G también actúa sobre $S(G)$ por conjugación.

Ejemplo 7. G actúa sobre la clase de conjugación de un subgrupo suyo H por conjugación, es decir que $a \cdot bHb^{-1} = abHb^{-1}a^{-1}$. El núcleo de esta acción es $\bigcap_{a\in G} a\,\mathrm{N}_G(H)a^{-1}$.

Ejemplo 8. G actúa sobre el conjunto $P(G)$ de los subconjuntos de G por traslaciones a izquierda, es decir que $a{\cdot}X = aX$. Esta acción es claramente fiel.

Ejemplo 9. G actúa sobre el conjunto $G\backslash H$ de las coclases a derecha de un subgrupo suyo H via $a{\cdot}(Hb) = Hba^{-1}$. El núcleo de esta acción es el máximo subgrupo $N = \bigcap_{g\in G} gHg^{-1}$ de H que es normal en G.

Ejemplo 10. S_n actúa sobre el anillo de polinomios $k[X_1, \ldots, X_n]$ via

$$\sigma{\cdot}P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Esta acción es claramente fiel.

Ejemplo 11. $\mathrm{GL}(n, k)$ actúa sobre el espacio de matrices columna k^n, via $A{\cdot}x = Ax$. Esta acción se llama la *acción natural de* $\mathrm{GL}(n, k)$ y es claramente fiel. Más generalmente todo subgrupo de $\mathrm{GL}(n, k)$ actúa sobre k^n de la misma manera.

Ejemplo 12. El grupo ortogonal $O(n, k)$ actúa sobre la esfera

$$S^{n-1} = \{x \in k^n : \|x\| = 1\},$$

via $A{\cdot}x = Ax$. Es facil ver que esta acción también es fiel.

Ejemplo 13. S_X actúa sobre X, via $\sigma{\cdot}x = \sigma(x)$. Esta se llama la *acción natural de* S_X y es claramente fiel. Más generalmente todo subgrupo de S_X actúa sobre X de la misma manera.

Órbitas, puntos fijos y estabilizadores. Dos elementos x e y de un G-conjunto X son *conjugados con respecto a la acción de G sobre X* o simplemente *conjugados* si existe $a \in G$ tal que $a{\cdot}x = y$. Es facil ver que la relación definida por $x \sim y$ si x e y son conjugados es de equivalencia. Así X queda partido en clases llamadas *clases de conjugación* u *órbitas*. A la órbita que contiene a un elemento x la denotaremos $\mathcal{O}_x$. Por definición $\mathcal{O}_x = \{a{\cdot}x : a \in G\}$ y $\mathcal{O}_x = \mathcal{O}_y$ si y sólo si x e y son conjugados. Decimos que $x \in X$ es un *punto fijo* si $a \cdot x = a$ para todo $a \in G$, es decir si

$\mathcal{O}_x = \{x\}$. Cada orbita es claramente un G-subespacio de X. Denotemos con X' a un conjunto de representantes de las clases de conjugación de X (es decir que para cada $x \in X$ la intesección $X' \cap \mathcal{O}_x$ tiene exactamente un elemento). Notemos que el conjunto de los puntos fijos $\mathrm{PF}(X)$ de X está incluído en X'. Es claro que

$$\#(X) = \sum_{x \in X'} \#(\mathcal{O}_x) = \#(\mathrm{PF}(X)) + \sum_{x \in X' \setminus \mathrm{PF}(X)} \#(\mathcal{O}_x). \tag{4}$$

Decimos que la acción de un grupo G sobre un conjunto X es *transitiva* o que G *opera transitivamente* sobre X si tiene una sóla órbita. Por definición el *estabilizador* o *grupo de isotropía* de un elemento x de X es $G_x = \{a \in G : a{\cdot}x = x\}$. Es evidente que G_x es un subgrupo de G y que el núcleo de la acción de G sobre X es la intersección $\bigcap_{x \in X} G_x$ de los estabilizadores de todos los elementos de X.

Proposición 3.1.8. *Si $y = a{\cdot}x$, entonces $G_y = aG_xa^{-1}$. En particular si G_x es un subgrupo normal de G, entonces $G_y = G_x$.*

Demostración. Tomemos $b \in G_x$. Entonces

$$(aba^{-1}){\cdot}y = a{\cdot}(b{\cdot}(a^{-1}{\cdot}y)) = a{\cdot}(b{\cdot}x) = a{\cdot}x = y$$

y así $aG_xa^{-1} \subseteq G_y$. Por simetría $a^{-1}G_ya \subseteq G_x$, de donde $G_y \subseteq aG_xa^{-1}$. □

Corolario 3.1.9. *Si x e y estan en la misma órbita, entonces sus estabilizadores son isomorfos.*

Observación 3.1.10. *Supongamos que G actú a sobre un conjunto X. De la Proposición 3.1.8 se sigue que si H es conjugado a G_x, entonces existe $y \in \mathcal{O}_x$ tal que $G_y = H$. Así, por el comentario que precede a la Observación 1.13.6, $N = \bigcap_{y \in \mathcal{O}_x} G_y$ es el máximo subgrupo normal de G_x. Notemos que si G actúa transitivamente sobre X, entonces N coincide con el núcleo de la acción de G sobre X.*

Teorema 3.1.11. *Supongamos que X es un G-espacio y tomemos $x \in X$. Consideremos a G/G_x como G-espacio via $a{\cdot}bG_x = abG_x$. La aplicación $\Phi\colon G/G_x \to \mathcal{O}_x$, definida por $\Phi(aG_x) = a{\cdot}x$ es un isomorfismo de G-espacios.*

Demostración. Notemos en primer lugar que Φ está bien definida, ya que de la igualdad $aG_x = bG_x$ se sigue que existe $c \in G_x$ tal que $a = bc$ y, por tanto, $a{\cdot}x = b{\cdot}(c{\cdot}x) = b{\cdot}x$. Es evidente que Φ es un morfismo sobreyectivo de G-espacios. Resta ver que también es inyectivo, lo cual se sigue de que $a{\cdot}x = b{\cdot}x$ implica que $a^{-1}b \in G_x$ y así $aG_x = bG_x$. □

Corolario 3.1.12. *Para cada G-espacio X y cada $x \in X$ vale que*

$$\#(\mathcal{O}_x) = |G : G_x|.$$

En particular $x \in \mathrm{PF}(X)$ si y sólo si $G_x = G$.

Una aplicación de este resultado es la siguiente:

Proposición 3.1.13. *Si k es un cuerpo finito que tiene q elementos, entonces el orden de* $\mathrm{GL}(n,k)$ *es*

$$(q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q-1).$$

Demostración. Por inducción en n. Es claro que $\mathrm{GL}(1,k) = k^*$ tiene $q-1$ elementos. Supongamos que el resultado vale para n. Denotemos con 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 k^{n+1}. Dado que la acción natural de $\mathrm{GL}(n+1,k)$ sobre $k^{n+1}\setminus\{0\}$ es transitiva, tenemos

$$q^{n+1}-1 = \#(k^{n+1}\setminus\{0\}) = \frac{|\,\mathrm{GL}(n+1,k)|}{|\,\mathrm{GL}(n+1,k)_{e_1}|}.$$

Es facil ver que $\mathrm{GL}(n+1,k)_{e_1}$ es el conjunto de las matrices cuya primera columna es e_1 y así $|\,\mathrm{GL}(n+1,k)_{e_1}| = q^n|\,\mathrm{GL}(n,k)|$. En consecuencia por la 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 ver. □

Combinando el Corolario 3.1.12 con la fórmula (4) obtenemos que

$$\#(X) = \sum_{x\in X'} |G:G_x| = \#(\mathrm{PF}(X)) + \sum_{x\in X'\setminus \mathrm{PF}(X)} |G:G_x|, \tag{5}$$

donde X' es un conjunto de representantes de las clases de conjugación de X.

Veamos que nos dice todo esto en algunos de los ejemplos mencionados arriba:

1) En el caso en que G actúa sobre si mismo por conjugación, tenemos que $\mathrm{PF}(G) = \mathrm{Z}(G)$ y $G_a = \mathrm{C}_G(a)$ para todo $a\in G$, de manera de que el tamaño de la clase de conjugación de $a\in G$ es $|G:\mathrm{C}_G(a)|$ y así, si G es finito, divide al orden de G. Además la fórmula (5) queda

$$|G| = |\,\mathrm{Z}(G)| + \sum_{a\in X'\setminus \mathrm{Z}(G)} |G:\mathrm{C}_G(a)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de G. Esta es la llamada *ecuación de las clases.*

2) En el caso en que G actúa sobre uno de sus subgrupos normales H por conjugación, entonces $\mathrm{PF}(H) = H\cap \mathrm{Z}(G)$ y $G_a = \mathrm{C}_G(a)$ para todo $a\in H$, de manera de que el tamaño de la clase de conjugación de $a\in H$ es $|G:\mathrm{C}_G(a)|$ y así, si G es finito, divide al orden de G. Además la fórmula (5) queda

$$|H| = |H\cap \mathrm{Z}(G)| + \sum_{a\in X'\setminus (H\cap \mathrm{Z}(G))} |G:\mathrm{C}_G(a)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de G que están incluídas en H.

3) En el caso en que G actúa sobre el conjunto $S(G)$ de los subgrupos de G por conjugación, entonces $\mathrm{PF}(S(G))$ es el conjunto $S_N(G)$, de los subgrupos normales de G, y $G_H = \mathrm{N}_G(H)$ para todo subgrupo H de G, de manera de que el tamaño de la clase de conjugación de H es $|G : \mathrm{N}_G(H)|$ y así, si G es finito, divide al orden de G. Además la fórmula (5) queda

$$\#(S(G)) = \#(S_N(G)) + \sum_{H \in X' \setminus S_N(G)} |G : \mathrm{N}_G(H)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de $S(G)$.

4) En el caso en que G actúa sobre el conjunto $P(G)$ de los subconjuntos de G por conjugación, entonces $\mathrm{PF}(P(G))$ es el conjunto $P_N(G)$, de los subconjuntos S de G que satisfacen $aSa^{-1} = S$ para todo $a \in G$, y $G_S = \mathrm{N}_G(S)$ para todo subconjunto S de G, de manera de que el tamaño de la clase de conjugación de S es $|G : \mathrm{N}_G(S)|$ y así, si G es finito, divide al orden de G. Además la fórmula (5) queda

$$2^{|G|} = \#(P(G)) = \#(P_N(G)) + \sum_{S \in X' \setminus P_N(G)} |G : \mathrm{N}_G(S)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de $P(G)$.

5) La acción de G por traslaciones a izquierda sobre el conjunto G/H de las coclases a izquierda de un subgrupo H de G es transitiva. Así, si H es propio, entonces $\mathrm{PF}(G/H) = \emptyset$ y $G_{aH} = aHa^{-1}$ para toda coclase aH. La fórmula (5) en este caso es trivial.

A continuación damos otra aplicación del Corolario 3.1.12:

Observación 3.1.14. *Tomemos un elemento a de un grupo G. Es obvio que $\langle a \rangle \subseteq \mathrm{C}_G(a)$. Además, por el cálculo hecho en el item 1) de arriba, si G es finito, entonces $|\mathrm{C}_G(a)|$ es igual a $|G|$ dividido por el cardinal de la clase de conjugación de a. En consecuencia, $\langle a \rangle = \mathrm{C}_G(a)$ si y sólo si este cociente es igual al orden de a. Por ejemplo, por la fórmula de Cauchy obtenida en (3), para cada permutación $\sigma \in \mathrm{S}_n$, vale que $|\mathrm{C}_G(\sigma)| = 1^{\alpha_1}\alpha_1!2^{\alpha_2}\alpha_2! \dots n^{\alpha_n}\alpha_n!$, donde $(\alpha_1, \dots, \alpha_n)$ es la estructura cíclica de σ y así, por el Teorema 2.1.1, $\langle \sigma \rangle = \mathrm{C}_{\mathrm{S}_n}(\sigma)$ si y sólo si los órdenes de los ciclos que aparecen en la descomposición cíclica de σ son todos coprimos dos a dos (en particular tienen todos ordenes distintos).*

Ejercicio 22. *Pruebe que si G es un grupo simple infinito, entonces vale lo siguiente:*

1) Si $a \in G$ es distinto de 1, entonces la clase de conjugación de a tiene infinitos elementos.

2) Si H es un subgrupo no trivial de G, entonces la clase de conjugación de H tiene infinitos elementos.

Denotemos con k a un número natural. Decimos la acción de un grupo G sobre un conjunto X es *k-transitiva* o que G *opera k-transitivamente* sobre X si dados subconjuntos $\{x_1, \dots, x_k\}$ e $\{y_1, \dots, y_k\}$ de k elementos de X existe $a \in G$ tal que $a \cdot x_1 = y_1, \dots, a \cdot x_k = y_k$.

Ejemplo. La acción natural de S_n sobre $X = \{1, \ldots, n\}$ es n-transitiva. Afirmamos que la acción de A_n sobre X inducida por la acción natural de S_n es $n-2$ transitiva. En efecto si $\{x_1, \ldots, x_{n-2}\}$ e $\{y_1, \ldots, y_{n-2}\}$ son subconjuntos de X de $n-2$ elementos, entonce existe $\sigma \in \mathrm{S}_n$ tal que $\sigma(x_i) = y_i$ para $1 \leq i \leq n-2$. Si $\sigma \in A_n$ ya está. Si no tomando $z_1, z_2 \in X \setminus \{y_1, \ldots, y_{n-2}\}$ y considerando $\sigma' = (z_1, z_2) \circ \sigma$ obtenemos una permutatación par σ' que también satisface $\sigma'(x_i) = y_i$ para $1 \leq i \leq n-2$.

Proposición 3.1.15. *Supongamos que $k \in \mathbb{N}$ es mayor o igual que 2 y que X es un G-comjunto. Son equivalentes:*

1) *G opera k-transitivamente sobre X.*
2) *G opera transitivamente sobre X y la acción de cada estabilizador G_x sobre $X \setminus \{x\}$ es $(k-1)$-transitiva.*

Demostración. Veamos primero que 1) implica 2). Es claro que G opera transitivamente sobre X. Tomemos ahora $x \in X$. Por hipótesis, dados subconjuntos $\{x_1, \ldots, x_{k-1}\}$ e $\{y_1, \ldots, y_{k-1}\}$ de $k-1$ elementos de $X \setminus \{x\}$, existe $a \in G$ tal que $a \cdot x = x$ y $a \cdot x_1 = y_1, \ldots, a \cdot x_{k-1} = y_{k-1}$. Esto muestra que cada G_x opera $(k-1)$-transitivamente sobre $X \setminus \{x\}$. Veamos ahora que 2) implica 1). Tomemos subconjuntos $\{x_1, \ldots, x_k\}$ e $\{y_1, \ldots, y_k\}$ de k elementos de X. Como G opera transitivamente sobre X y G_{x_1} opera $(k-1)$-transitivamente sobre $X \setminus \{x_1\}$ existen $a \in G$ y $b \in G_{x_1}$ tales que $a \cdot y_1 = x_1$ y $b \cdot x_2 = a \cdot y_2, \ldots, b \cdot x_2 = a \cdot y_{k-1}$. Es claro ahora que $(a^{-1}b) \cdot x_1 = y_1, \ldots, (a^{-1}b) \cdot x_k = y_k$. $\square$

Contando órbitas. El siguiente resultado es conocido como lema de Burnside, pero es debido a Frobenius.

Teorema 3.1.16. *Para cada G-conjunto arbitrario N vale que*

$$N|G| = \sum_{a \in G} \#(\mathrm{PF}_a(X)),$$

donde $\mathrm{PF}_a(X) = \{x \in X : a \cdot x = x\}$ y N denota a la cantidad de órbitas de X.

Demostración. En $\sum_{a \in G} \#(\mathrm{PF}_a(X))$ cada $x \in X$ es contado $|G_x|$ veces (pues G_x consiste de todos los $a \in G$ tales que $x \in \mathrm{PF}_a(X)$). Dado que si x e y están en la misma órbita es $|G_x| = |G_y|$ y que la órbita de x tiene $|G : G_x|$ elementos, en la suma de arriba los elementos de $\mathcal{O}_x$ son contados en total $|G| = |G : G_x||G_x|$ veces. Recorriendo todas las órbitas de X obtenemos así que $\sum_{a \in G} \mathrm{PF}_a(X) = N|G|$. $\square$

Ejemplo. La cantidad c de clases de conjugación de un grupo finito G es

$$c = \frac{1}{|G|} \sum_{a \in G} |\,\mathrm{C}_G(a)|,$$

En efecto, para la acción de conjugación,

$$\mathrm{PF}_a(G) = \{b \in G : aba^{-1} = b\} = \{b \in G : b^{-1}ab = a\} = \mathrm{C}_G(a).$$

Corolario 3.1.17. *Si G es un grupo finito y X es un G-conjunto transitivo que tiene más de un elemento, entonces existe $a \in G$ tal que* $\mathrm{PF}_a(X) = \emptyset$.

Demostración. Dado que X es transitivo la cantidad de órbitas es 1. Así, por el Teorema 3.1.16, $|G| = \sum_{a\in G} \#(\mathrm{PF}_a(X))$ y, como $\#(\mathrm{PF}_1(X)) = \#(X) > 1$, debe existir $a \in G$ tal que $\mathrm{PF}_a(X) = \emptyset$. □

Lema 3.1.18. *Fijemos $n \geq 1$ y $q \in \mathbb{Q}$. Existe sólo una cantidad finita de n-uplas $(i_1, \ldots, i_n)$ de números naturales, tales que $q = \sum_{j=1}^{n} \frac{1}{i_j}$.*

Demostración. Demostraremos el lema mediante inducción en n. El caso $n = 1$ es trivial. Supongamos que el resultado vale para uplas de longitud $n-1$ y veamos que vale para uplas de longitud n. Claramente es suficiente ver que existe sólo una cantidad finita de n-uplas $(i_1, \ldots, i_n)$ de números naturales, tales que $i_1 \leq \cdots \leq i_n$ y $q = \sum_{j=1}^{n} \frac{1}{i_j}$. Para cada una de estas n-uplas claramente tenemos que $i_1 \leq n/q$. El resultado se sigue de que, por la hipótesis inductiva, para cada número natural $k \leq n/q$, sólo hay una cantidad finita de $(n-1)$-uplas $(i_2, \ldots, i_n)$ que satisfacen la igualdad $q - \frac{1}{k} = \sum_{j=2}^{n} \frac{1}{i_j}$. □

Teorema 3.1.19. *Para cada $n \geq 1$ sólo hay una cantidad finita de grupos finitos que tienen exactamente n clases de conjugación.*

Demostración. Supongamos que G es un grupo finito que tiene exactamente n clases de conjugación. Entonces la ecuación de las clases queda

$$|G| = \sum_{j=1}^{n} |G : C_G(a_j)|,$$

donde $\{a_1, \ldots, a_n\}$ es un conjunto de representantes de las clases de conjugación de G. De esto se sigue inmediatamente que

$$1 = \sum_{j=1}^{n} \frac{1}{i_j}, \quad \text{donde } i_j = |C_G(a_j)|.$$

Tomando j tal que $a_j \in \mathrm{Z}(G)$ obtenemos que el máximo i_j que aparece en esta suma es $|G|$. Por otra parte por el Lema 3.1.18 este máximo i_j está acotado por un $M > 0$. Esto muestra que $|G| \leq M$ y la demostración se termina usando el hecho obvio de que sólo hay una cantidad finita de grupos no isomorfos de un orden finito dado. □

Ejercicio 23. *Pruebe que si un grupo G contiene un elemento de orden $n > 1$ y dos clases de conjugación, entonces $|G| = 2$.*

3.2.Teoremas de Sylow. Denotemos con p a un número primo. 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 cuando no nos interese hablaremos también de *subgrupos de Sylow*. En esta sección vamos a probar tres importantes teoremas que aseguran entre otras cosas que el cardinal del conjunto de los p-subgrupo de Sylow de G es no vacío. Empezamos por los siguientes lemas.

Lema 3.2.1. *Si el orden de un grupo abeliano finito G es divisible por un primo p entonces G contiene un elemento de orden p.*

Demostración. Demostraremos el lema por inducción en $|G|/p$. El caso $|G|/p = 1$ es obvio. Para el paso inductivo tomemos $a \in G$ tal que $|a| > 1$. Si p divide a $|a|$, entonces $x^{|a|/p}$ tiene orden p. Si no, p divide a $|G/\langle a\rangle|$ y, por hipótesis inductiva, existe $b \in G$, tal que su clase $\overline{b}$ en $G/\langle a\rangle$ tiene orden p. Pero entonces el orden de b es múltiplo de p y $b^{|b|/p}$ tiene orden p. □

Lema 3.2.2. *Supongamos que P es un p-subgrupo de Sylow de G y que H un p-subgrupo de G. Si H está incluído en el normalizador $\mathrm{N}_G(P)$ de P en G, entonces H está incluído en P.*

Demostración. Por hipótesis HP es un subgrupo de $\mathrm{N}_G(P)$ y P es un subgrupo normal de HP. Por el teorema de Noether $|HP : P| = |H : P \cap H|$, que es una potencia de p, lo que implica que HP es un p-subgrupo de G. Como P es un p-subgrupo maximal de G, obtenemos de esto que $H \subseteq P$. □

Teorema 3.2.3 (Sylow). *Si G es un grupo finito y p es un primo que divide a $|G|$, entonces se satisfacen las siguientes propiedades:*

1) *La cantidad de p-subgrupos de Sylow de G es congruente a 1 módulo p.*
2) *Todos los p-subgrupos de Sylow de G son conjugados.*
3) *Todo p-subgrupo H de G está incluído en un p-subgrupo de Sylow de G. Además, la cantidad de p-subgrupos de Sylow de G que contienen a H es congruente a 1 módulo p.*

Demostración. Veamos primero que el conjunto de los p-subgrupos de Sylow de G no es vacío. Demostraremos esto por inducción en el orden de G. Si G tiene un subgrupo propio H cuyo índice es coprimo con p, entonces todo p-subgrupo de Sylow de H también lo será de G, y el resultado se sigue por inducción. Podemos suponer entonces que ningún subgrupo propio de G tiene índice coprimo con p. De la ecuación de las clases

$$|G| = |\,\mathrm{Z}(G)| + \sum_{a \in X' \setminus \mathrm{Z}(G)} |G : \mathrm{C}_G(a)|,$$

se sigue entonces que p divide a $|\,\mathrm{Z}(G)|$. Por el Lema 3.2.1 existe $a \in \mathrm{Z}(G)$ de orden p. Como $a \in \mathrm{Z}(G)$ el subgrupo $\langle a\rangle$ de G es normal. Tomemos un p-subgrupo de Sylow P' de $G/\langle a\rangle$ y escribamos $P = \pi^{-1}(P')$, donde $\pi\colon G \to G/\langle a\rangle$ es el epimorfismo canónico. Dado que $\langle a\rangle \subseteq P$ y que π aplica P sobre P' tenemos la sucesión exacta corta

$$1 \longrightarrow \langle a\rangle \longrightarrow P \xrightarrow{\pi} P' \longrightarrow 1$$

y así $|P| = p|P'|$, lo que 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. Denotemos con $\mathrm{PF}_H(X)$ al conjunto de los puntos fijos de X por esta acción. Por el Lema 3.2.2

$$\mathrm{PF}_H(X) = \{aPa^{-1} : H \subseteq \mathrm{N}_G(aPa^{-1})\} = \{aPa^{-1} : H \subseteq aPa^{-1}\},$$

y por otro lado,

$$\#(\mathrm{PF}_H(X)) \equiv \#(X) \pmod{p},$$

ya que $X \setminus \mathrm{PF}_H(X)$ es una unión disjunta de órbitas no triviales y que, por el Corolario 3.1.12, el cardinal de cada órbita no trivial de X es una potencia positiva de p. Así,

$$\#(\{aPa^{-1} : H \subseteq aPa^{-1}\}) \equiv \#(X) \pmod{p}.$$

Como $\{aPa^{-1} : P \subseteq aPa^{-1}\} = \{P\}$, tomando $H = P$ en esta igualdad, obtenemos que $\#(X) \equiv 1 \pmod{p}$ y, en consecuencia, que

$$\#(\{aPa^{-1} : H \subseteq aPa^{-1}\}) \equiv 1 \pmod{p}.$$

Aplicando esta fórmula con H un p-subgrupo de Sylow se obtiene el item 2). Considerando ahora H arbitrario se verifica que vale el item 3). Finalmente el item 1) se sigue del 3) tomando $H = \{1\}$. □

Corolario 3.2.4. *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 igual a $|G : \mathrm{N}_G(P)|$, dónde P es cualquier p-subgrupo de Sylow de G.*

Demostración. Denotemos con X al conjunto de los p-subgrupos de Sylow de G y consideremos la acción de G sobre X por conjugación. Como esta acción es transitiva el cardinal de X es $|G : \mathrm{N}_G(P)|$. □

Al conjunto de los p-subgrupos de Sylow de un grupo G lo vamos a denotar con $\mathrm{Syl}_p(G)$.

Corolario 3.2.5. *Si G es un grupo de orden $p^r m$ con p primo y m coprimo con p, entonces $\#(Syl_p(G))$ divide a m.*

Demostración. El resultado se sigue del corolario anterior y de que $|G : \mathrm{N}_G(P)|$ divide a $|G : P| = m$. □

Corolario 3.2.6. *Supongamos que P es un p-subgrupo de Sylow de un grupo finito G. Son equivalentes:*

1) P es un subgrupo completamante normal de G,

2) P es un subgrupo normal de G,

3) P es el único subgrupo de Sylow de G.

Demostración. 1) ⇒ 2). Es trivial.

2) ⇒ 3). Por el item 2) del Teorema 3.2.3.

3) ⇒ 1). Pues si G tiene sólo un p-subgrupo de Sylow P, entonces P es completamente normal en G, ya que la imagen de P por un endomorfismo de G, es un p-subgrupo de G que, por el item 3) del Teorema 3.2.3, está incluído en G. □

Proposición 3.2.7. *Si $(P_i)_{i\in I}$ es una familia que contiene un p-subgrupo de Sylow de un grupo finito G para cada primo p que divide a $|G|$, entonces G está generado por $\bigcup_{i\in I} P_i$.*

Demostración. Denotemos con G' al subgrupo de G generado por $\bigcup_{i\in I} P_i$. Como $P_i \subseteq G'$, sabemos que $|P_i|$ divide a $|G'|$ y así, como los $|P_i|$'s son coprimos dos a dos, su producto $\prod_{i\in I} |P_i|$ también divide a $|G'|$. Como este producto es igual a $|G|$, tenemos entonces $|G|$ divide a $|G'|$, de donde $G = G'$. □

Algunos ejemplos. A continuación calculamos los subgrupos de Sylow de algunos grupos.

Ejemplo 1. Consideremos el grupo simétrico S_3 cuyo orden es $3! = 2.3$. Es evidente que S_3 tiene un único 3-subgrupo de Sylow $\langle(1,2,3)\rangle$ y tres 2-subgrupos de Sylow $\langle(1,2)\rangle$, $\langle(1,3)\rangle$ y $\langle(2,3)\rangle$.

Ejemplo 2. Consideremos el grupo simétrico S_4 cuyo orden es $4! = 2^3.3$. Dado que los 3-cíclos son los únicos elementos de S_4 que tienen orden 3 y hay 8 de ellos, S_4 tiene cuatro 3-subgrupo de Sylow, $\langle(1,2,3)\rangle$, $\langle(1,2,4)\rangle$, $\langle(1,3,4)\rangle$ y $\langle(2,3,4)\rangle$. Calculemos ahora los 2-subgrupos de Sylow. Como (por ser unión de clases conjugadas) el subgrupo

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

de S_4 es invariante, H es un subgrupo de cada 2-subgrupo de Sylow de S_4. Así, los 2-subgrupo de Sylow de S_4 son los subgrupos de la forma $P_\sigma = \langle\sigma, H\rangle$, con $\sigma \in \mathrm{S}_4 \setminus H$ un elemento cuyo orden es una potencia de 2. Podemos tomar por ejemplo como σ a un 4-cíclo. Como los 3-subgrupos de Sylow de S_4 son conjugados, por el Teorema 2.1.2, todos serán de esta forma. Notemos ahora que $P_\sigma = P_{\sigma^3}$, ya que $\langle\sigma\rangle = \langle\sigma^3\rangle$, de manera de que S_4 tiene a lo sumo tres 2-subgrupos de Sylow, que son

$$P_1 = \langle(1,2,3,4), H\rangle, \qquad P_2 = \langle(1,2,4,3), H\rangle \qquad \text{y} \qquad P_3 = \langle(1,3,2,4), H\rangle.$$

Un cálculo directo muestra que

$$\begin{aligned} P_1 &= \{\mathrm{id}, (1,3), (2,4), (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3), (1,2,3,4), (1,4,2,3)\}, \\ P_2 &= \{\mathrm{id}, (1,4), (2,3), (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3), (1,2,4,3), (1,3,4,2)\}, \end{aligned}$$

y

$$P_3 = \{\mathrm{id}, (1,2), (3,4), (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3), (1,3,2,4), (1,4,2,3)\}.$$

Notemos por último que P_1 está generado por $\sigma = (1,2,3,4)$ e $\tau = (1,4)\circ(2,3)$ y que $\sigma^4 = \tau^2 = \mathrm{id}$ y $\tau\sigma\tau^{-1} = \sigma^{-1}$ y así P_1, P_2 y P_3 son isomorfos a D_4.

Ejemplo 3. Parte de los argumentos usados en el ejemplo anterior muestran que el grupo A_4, de orden $2^2.3$, tiene un único subgrupo de Sylow

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

de orden 4, que es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ y cuatro 3-subgrupo de Sylow, $\langle(1,2,3)\rangle$, $\langle(1,2,4)\rangle$, $\langle(1,3,4)\rangle$ y $\langle(2,3,4)\rangle$.

Ejemplo 4. Consideremos el grupo diedral D_n. Recordemos que D_n está generado por dos elementos a e b sujetos a las relaciones $a^n = 1$, $b^2 = 1$ y $bab^{-1}a = 1$ y que $D_n = \{1, \ldots, a^{n-1}, b, \ldots, a^{n-1}b\}$. Sabemos también que cualquiera sea r el subgrupo $\langle a^r\rangle$ de D_n es invariante. Escribamos $n = 2^m t$ con t impar, de manera de que $|D_n| = 2^{m+1}t$. Afirmamos que

1) La cantidad de 2-subgrupos de Sylow de D_n es t y cada uno de ellos es isomorfo a D_{2^m}.

2) Si p es un primo impar que divide a $2^{m+1}t$, entonces D_n tiene un único p-subgrupo de Sylow, que es cíclico.

Veamos primero el item 1). Como el subgrupo $\langle a^t\rangle$ de D_n es invariante y su orden es 2^m, está incluído en todos los 2-subgrupos de Sylow de D_n. Dado que si $a^i \in D_n \setminus \langle a^t\rangle$ su orden no es una potencia de 2, los 2-subgrupos de Sylow de D_n tienen la forma $K_i = \langle a^i b, a^t\rangle = \langle a^i b\rangle\langle a^t\rangle$, donde la última igualdad se sigue de que $\langle a^t\rangle$ es un subgrupo invariante de D_n. Además la igualdad

$$|\langle a^i b\rangle\langle a^t\rangle| = \frac{|\langle a^i b\rangle||\langle a^t\rangle|}{|\langle a^i b\rangle \cap \langle a^t\rangle|} = \frac{2.2^m}{1} = 2^{m+1}$$

muestra que cada uno de estos K_i es un 2-subgrupo de Sylow de D_n. Como

$$K_i = \langle a^i b, a^t\rangle = \{a^{tj+i}b, a^{tj} : 0 \leq j < 2^m\},$$

es claro que $K_i = K_{i'}$ si y sólo si $i' \equiv i \pmod t$ y así los 2-subgrupos de Sylow de D_n son exactamente $K_0, \ldots, K_{t-1}$. Por último los K_i's son diedrales ya que $a^i b$ y a^t son un conjunto de generadores de K_i que satisface $(a^t)^{2^m} = 1$, $(a^i b)^2 = 1$ y $(a^i b)a^t(a^i b)^{-1} = a^{-t}$. Veamos ahora el item 2). Notemos que si p es un primo impar y si p divide a $2^{m+1}t$, entonces p divide a t. Escribamos $t = p^u v$ con v coprimo con p. El subgrupo $\langle a^{2^m v}\rangle$ de D_n tiene orden p^u y es invariante y así es el único p-subgrupo de Sylow de D_n.

Ejemplo 5. Consideremos el grupo cuaterniónico H_n. Recordemos que H_n está generado por dos elementos a e b sujetos a las relaciones $a^n b^{-2} = 1$ y $bab^{-1}a = 1$ y que $H_n = \{1, \ldots, a^{2n-1}, b, \ldots, a^{2n-1}b\}$. Escribamos $n = 2^m t$ con t impar, de manera de que $|H_n| = 2^{m+2}t$. Afirmamos que

1) La cantidad de 2-subgrupos de Sylow de H_n es t y cada uno de ellos es isomorfo a H_{2^m} (aqui denotamos con H_1 a un grupo cíclico de orden 4).
2) Si p es un primo impar que divide a $2^{m+2}t$, entonces H_n tiene un único p-subgrupo de Sylow, que es cíclico.

Veamos primero el item 1). Como el subgrupo $\langle a^t\rangle$ de H_n es invariante y su orden es 2^{m+1}, está incluído en todos los 2-subgrupos de Sylow de H_n. Dado que si $a^i \in H_n \setminus \langle a^t\rangle$ su orden no es una potencia de 2, los 2-subgrupos de Sylow de H_n tienen la forma $K_i = \langle a^i b, a^t\rangle = \langle a^i b\rangle\langle a^t\rangle$, donde la última igualdad se sigue de que $\langle a^t\rangle$ es un subgrupo invariante de H_n. Notemos que $(a^i b)^2 = a^i b a^i b^{-1} b^2 = b^2 = a^n$ y así $\langle a^i b\rangle \cap \langle a^t\rangle = \{1, a^n\}$. En consecuencia

$$|\langle a^i b\rangle\langle a^t\rangle| = \frac{|\langle a^i b\rangle||\langle a^t\rangle|}{|\langle a^i b\rangle \cap \langle a^t\rangle|} = \frac{2.2^{m+1}}{2} = 2^{m+1},$$

lo que muestra que cada uno de estos K_i es un 2-subgrupos de Sylow de H_n. Como

$$K_i = \langle a^i b, a^t\rangle = \{a^{tj+i}b, a^{tj} : 0 \leq j < 2^{m+1}\},$$

es claro que $K_i = K_{i'}$ si y sólo si $i' \equiv i \pmod t$ y así los 2-subgrupos de Sylow de H_n son exactamente $K_0, \ldots, K_{t-1}$. Por último los K_i's son isomorfos a H_{2^m} ya que $a^i b$ y a^t son un conjunto de generadores de K_i que satisface $(a^t)^{2^m}(a^i b)^{-2} = 1$ y $(a^i b)a^t(a^i b)^{-1} = a^{-t}$. Veamos ahora el item 2). Notemos que si p es un primo impar y si p divide a $2^{m+2}t$, entonces p divide a t. Escribamos $t = p^u v$ con v coprimo con p. El subgrupo $\langle a^{2^{m+1} v}\rangle$ de H_n tiene orden p^u y es invariante y así es el único p-subgrupo de Sylow de H_n.

Ejemplo 6. Vamos a calcular los p-subgrupos de Sylow de S_p. Dado que $|\,\mathrm{S}_p\,| = p!$ y p es coprimo con $(p-1)!$, todo p-subgrupo de Sylow de S_p es cíclico de orden p. Como los elementos de orden p de S_p son los p-ciclos, por la fórmula de Cauchy, S_p tiene $(p-1)!$ de tales elementos. Así, dado que cada p-subgrupo de Sylow de S_p contiene $p-1$ generadores, hay exactamente

$$(p-2)! = \frac{(p-1)!}{p-1}$$

p-subgrupos de de Sylow. En particular obtenemos que $(p-2)! \equiv 1 \pmod{p}$ lo cual es el famoso teorema de Wilson.

Ejemplo 7. Vamos a encontrar uno de los p-subgrupos de Sylow de $\mathrm{GL}(n,k)$, donde k es un cuerpo finito de p^m elementos. Por la Proposición 3.1.13 el orden de $\mathrm{GL}(n,k)$ es $p^{mn(n-1)/2}(p^{mn}-1)(p^{m(n-1)}-1)\cdots(p^m-1)$ y claramente p es coprimo con $(p^{mn}-1)(p^{m(n-1)}-1)\cdots(p^m-1)$. Por otro lado el orden del subgrupo $\mathrm{UT}(n,k)$ de $\mathrm{GL}(n,k)$ formado por las matrices triangulares superiores con coeficientes en k, que tienen 1 en la diagonal principal, es $p^{mn(n-1)/2}$ y así $\mathrm{UT}(n,k)$ es un p-subgrupo de Sylow de $\mathrm{GL}(n,k)$.

Observación 3.2.8. *Supongamos que H es un subgrupo de un grupo finito G y denotemos con p a un primo que divide a $|H|$. Por el item 3) del Teorema 3.2.3 todo subgrupo de Sylow P_H de H está incluído en un subgrupo de Sylow P de G y así $P_H = P \cap H$. En particular la cantidad de subgrupos de Sylow de G es mayor que la de H. Supongamos ahora que P' es otro subgrupo de Sylow de G. Por el item 2) del mismo teorema, existe $g \in G$ tal que $P' = gPg^{-1}$ y así $gP_Hg^{-1} = P' \cap gHg^{-1}$. Por lo tanto, si H es normal, entonces $P' \cap H$ es un subgrupo de Sylow de H y, en consecuencia en este caso, todo subgrupo de Sylow de G corta a H en un subgrupo de Sylow (en particular todo p-subgrupo normal de G está incluído en todos los subgrupos de Sylow de G). Además, PH/H es un p-subgrupo de Sylow de G/H, ya que $|PH/H| = |P/(P \cap H)|$ y $|G/H : PH/H| = |G : PH|$. Usando que todos los subgrupos de Sylow de G/H son conjugados se sigue facilmente de esto que todos los subgrupos de Sylow de G/H son se esta forma.*

Proposición 3.2.9. *Si H es un subgrupo normal de un grupo finito G y p es un primo que divide a $|H|$, entonces $\#(\mathrm{Syl}_p(H))$ divide a $\#(\mathrm{Syl}_p(G))$. Además*

$$\frac{\#(\mathrm{Syl}_p(G))}{\#(\mathrm{Syl}_p(H))} = \frac{|\,\mathrm{N}_G(P_H)|}{|\,\mathrm{N}_G(P)|} = \frac{|G:H||\,\mathrm{N}_H(P_H)|}{|\,\mathrm{N}_G(P)|},$$

donde P es un p-subgrupo de G y P_H un p-subgrupo de H.

Demostración. G actúa sobre $\mathrm{Syl}_p(H)$ por conjugación, ya que si $P_H \in \mathrm{Syl}_p(H)$, entonces $gP_Hg^{-1} \subseteq gHg^{-1} = H$, para todo $g \in G$. Además esta acción es transitiva, puesto que lo es restringida a H. Como $\mathrm{N}_G(P_H)$ es el estabilizador de P_H con respecto a esta acción, $\#(\mathrm{Syl}_p(H)) = |G : \mathrm{N}_G(P_H)|$. Supongamos que $P \in \mathrm{Syl}_P(G)$ es tal que $P \cap H = P_H$. Claramente $\mathrm{N}_G(P) \subseteq \mathrm{N}_G(P_H)$, ya que si $g \in \mathrm{N}_G(P)$, entonces

$$gP_Hg^{-1} = g(P \cap H)g^{-1} = gPg^{-1} \cap gHg^{-1} = gPg^{-1} \cap H = P \cap H = P_H.$$

En consecuencia

$$\#(\mathrm{Syl}_p(H)) = |G : \mathrm{N}_G(P_H)| \quad \text{divide a} \quad |G : \mathrm{N}_G(P)| = \#(\mathrm{Syl}_p(G)).$$

Notemos también que de $|H : \mathrm{N}_H(P_H)| = \#(\mathrm{Syl}_p(H)) = |G : \mathrm{N}_G(P_H)|$ se sigue que

$$\frac{\#(\mathrm{Syl}_p(G))}{\#(\mathrm{Syl}_p(H))} = \frac{|\,\mathrm{N}_G(P_H)|}{|\,\mathrm{N}_G(P)|} = \frac{|G : H||\,\mathrm{N}_H(P_H)|}{|\,\mathrm{N}_G(P)|},$$

como queríamos. □

Proposición 3.2.10. *Si H es un subgrupo normal de un grupo finito G y p es un primo que divide a $|G/H|$, entonces $\#(\mathrm{Syl}_p(G/H))$ divide a $\#(\mathrm{Syl}_p(G))$.*

Demostración. G actúa sobre $\{PH/H : P \in \mathrm{Syl}_p(G)\}$ por conjugación y esta acción es claramente transitiva. Puesto que $\mathrm{N}_G(P)$ está claramente incluído en el estabilizador de PH/H y que, por la Observación 3.2.8,

$$\#(\mathrm{Syl}_p(G/H)) = \#(\{PH/H : P \in \mathrm{Syl}_p(G)\}),$$

tenemos que $\#(\mathrm{Syl}_p(G/H))$ divide a $|G : \mathrm{N}_G(P)| = \#(\mathrm{Syl}_p(G))$. □

Proposición 3.2.11 (Frattini). *Si H es un subgrupo normal de un grupo finito G y P es un p-subgrupo de Sylow de H, entonces $G = H\,\mathrm{N}_G(P)$. En particular, P es un subgrupo normal de H si y sólo si es un subgrupo normal de G.*

Demostración. Tomemos $a \in G$. Como H es normal, $aPa^{-1} \subseteq aHa^{-1} = H$ y así aPa^{-1} es un p-subgrupo de Sylow de H. Por el item 2) del Teorema 3.2.3, existe b en H tal que $baPa^{-1}b^{-1} = P$. Así $ba \in \mathrm{N}_G(P)$, de donde $a = b^{-1}(ba) \in H\,\mathrm{N}_G(P)$. □

Corolario 3.2.12. *Si H un subgrupo de un grupo finito G y H contiene al normalizador $\mathrm{N}_G(P)$ de un p-subgrupo de Sylow P de G, entonces $\mathrm{N}_G(H) = H$.*

Demostración. Como H es normal en $\mathrm{N}_G(H)$ y $P \subseteq H$ se sigue de la Proposición 3.2.11 que $\mathrm{N}_G(H) = H\,\mathrm{N}_{\mathrm{N}_G(H)}(P) \subseteq H\,\mathrm{N}_G(P) = H$. □

Terminamos esta subsección con el siguiente teorema probado por Cauchy en 1845.

Teorema 3.2.13 (Cauchy). *Si G es un grupo finito y p es un primo que divide a $|G|$, entonces G tiene elementos de orden p.*

Demostración. Tomemos $a \neq 1$ en P, donde P es un p-subgrupo de Sylow de G. Entonces $|a| = p^\alpha$ con $\alpha \geq 1$ y así $a^{p^{\alpha-1}}$ tiene orden p. □

Corolario 3.2.14. *Un grupo finito es un p-grupo si y sólo si el orden de cada uno de sus elementos es una potencia de p.*

3.3.p-grupos finitos. Denotemos con p a un número primo. En esta sección probaremos algunas propiedades básicas de los p-grupos finitos.

Teorema 3.3.1. *Denotemos con G a un p-grupo finito. Si H es un subgrupo normal no trivial de G, entonces $H \cap \mathrm{Z}(G)$ tampoco es trivial. En particular $\mathrm{Z}(G)$ no es trivial.*

Demostración. Consideremos la ecuación

$$|H| = |H \cap \mathrm{Z}(G)| + \sum_{a \in X' \setminus (H \cap \mathrm{Z}(G))} |G : \mathrm{C}_G(a)|,$$

donde X' es un conjunto de representantes de las clases de conjugación de G que están incluídas en H. Dado que tanto $|H|$ como cada $|G : \mathrm{C}_G(a)|$ son divisibles por p, también $|H \cap \mathrm{Z}(G)|$ lo es, de manera de que $H \cap \mathrm{Z}(G)$ no es trivial. □

Corolario 3.3.2. *Todo subgrupo normal de orden p de un p-grupo G está incluído en el centro de $|G|$.*

Corolario 3.3.3. *Si $|G| = p^n$, entones 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 $1 \leq i_1 < i_2 < \cdots < i_r < n$ 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 $1 \leq j \leq n$.

Demostración. Por inducción en α. Tomando $a \in \mathrm{Z}(G) \cap G_{i_1}$ de orden p obtenemos un subgrupo normal $G_1 = \langle a \rangle$ de orden p de G incluído en G_{i_1}. Supongamos ahora que el resultado vale para p-grupos de orden menor que p^n. Consideremos la sobreyección canónica $\pi \colon G \to G/\langle a \rangle$. Por hipótesis inductiva la cadena

$$0 = \overline{G}_0 \subseteq \overline{G}_{i_1 - 1} \subseteq \overline{G}_{i_2 - 1} \subseteq \cdots \subseteq \overline{G}_{i_r - 1} \subseteq \overline{G}_{n-1} = G,$$

donde $\overline{G}_{i_j - 1}$ denota a $\pi(G_{i_j})$ se puede extender a una cadena

$$0 = \overline{G}_0 \subseteq \overline{G}_1 \subseteq \overline{G}_2 \subseteq \cdots \subseteq \overline{G}_{n-1} \subseteq \overline{G}_n$$

con $|\overline{G}_j| = p^{j-1}$, para $1 \leq j \leq \alpha$. Es claro que la cadena

$$0 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$$

obtenida tomando $G_j = \pi^{-1}(\overline{G}_{j-1})$, para $1 \leq j \leq n$, satisface las condiciones pedidas en el enunciado. □

Corolario 3.3.4. *Todo grupo G de orden p^2 es abeliano. Además son equivalentes:*

1) G no es cíclico,

2) G tiene $p + 1$ subgrupos de orden p,

3) G tiene al menos dos subgrupos de orden p,

4) G es isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$,

Demostración. Supongamos que G no fuera abeliano. Debido a esto y al Teorema 3.3.1, $\mathrm{Z}(G)$ tendría orden p y así $G/\mathrm{Z}(G)$ tendría también orden p. Pero entonces sería cíclico, lo que contradeciría la Proposición 1.13.1. Veamos ahora las equivalencias. Si G no es cíclico, entonces tiene p^2-1 elementos de orden p y como los subgrupos de orden p de G tienen $p-1$ elementos de orden p y se intersecan trivialmente, hay $p+1=(p^2-1)/(p-1)$ subgrupos de orden p en G. Así 1) implica 2). Es claro que 2) implica 3) y 4) implica 1). Veamos que 3) implica 4). Si H_1 y H_2 son dos subgrupos distintos de orden p de G, entonces $H_1 \cap H_2 = \{1\}$ y así, por el Teorema 1.14.10, $G \simeq H_1 \times H_2 \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. □

Corolario 3.3.5. *Si G es un grupo no conmutativo de orden p^3, entonces*

$$\mathrm{Z}(G) = [G,G]$$

y tiene orden p y este es el único subgrupo invariante de G de orden p. Además $G/\mathrm{Z}(G)$ es abeliano y no cíclico.

Demostración. Por el Teorema 3.3.1, $\mathrm{Z}(G) \neq \{1\}$ y dado que G no es abeliano, $\mathrm{Z}(G) \neq G$. Además por la Proposición 1.13.1, $G/\mathrm{Z}(G)$ no es cíclico. Por lo tanto su orden es al menos p^2 y así $|\mathrm{Z}(G)| = p$. Como, por el Corolario 3.3.4, $G/\mathrm{Z}(G)$ es abeliano, tenemos que $[G,G] \subseteq \mathrm{Z}(G)$. Por otra parte no puede ser $[G,G] = \{1\}$ ya que esto significa que G es abeliano. Por último, por el Corolario 3.3.2, $\mathrm{Z}(G)$ es el único subgrupo invariante de G de orden p. □

Teorema 3.3.6. *Si H es un subgrupo propio de un p-grupo finito G, entonces $H \subsetneq \mathrm{N}_G(H)$.*

Demostración. Si H es normal es claro que $H \subsetneq \mathrm{N}_G(H)$ ya que $\mathrm{N}_G(H) = G$. Supongamos que H no es normal. Entonces el cardinal del conjunto X de los conjugados de H es $|G : \mathrm{N}_G(H)|$ lo que es una potencia de p mayor que 1. Ahora H actúa sobre X por conjugación y, dado que H es un p-grupo, el cardinal de cada una de sus órbitas es una potencia de p. Dado que la órbita de H es claramente $\{H\}$ que tiene tamaño 1, hay al menos $p-1$ elementos de X cuyas órbitas también tienen tamaño 1. Tomemos uno de estos elementos aHa^{-1}. Entonces para todo $b \in H$ vale que $baHa^{-1}b^{-1} = aHa^{-1}$, lo que implica que $a^{-1}ba \in \mathrm{N}_G(H)$. Pero como $aHa^{-1} \neq H$ algún $a^{-1}ba$ no está en H. □

Corolario 3.3.7. *Si H es un subgrupo propio maximal de un p-grupo finito G, entonces H es normal en G y su índice es p.*

Demostración. Por el Teorema 3.3.6 el subgrupo H de G es normal. Además por la Observación 1.11.7, G/H no tiene subgrupos no triviales y así, por el Corolario 3.3.3, $|G/H| = p$. □

Observación 3.3.8. *Supongamos que H es un subgrupo propio de un p-grupo finito G. Por el Teorema 3.3.6 existe una cadena*

$$H \subsetneq \mathrm{N}_G^1(H) \subsetneq \mathrm{N}_G^2(H) \subsetneq \cdots \subsetneq \mathrm{N}_G^{i-1}(H) \subsetneq \mathrm{N}_G^i(H) = G,$$

donde la sucesión $(\mathrm{N}_G^j(H))_{j\geq 0}$ está definida recursivamente por $\mathrm{N}_G^0(H) = \{1\}$ y $\mathrm{N}_G^{j+1}(H) = \mathrm{N}_G(\mathrm{N}_G^j(H))$. Para todo $0 \leq j \leq i$, denotemos con p^{α_j} al orden de $\mathrm{N}_G^j(H)$. Por el Corolario 3.3.3, para cada $0 \leq j < i$ existen cadenas

$$\mathrm{N}_G^j(H) = G_{\alpha_j} \subseteq G_{\alpha_j+1} \subseteq \cdots \subseteq G_{\alpha_{j+1}-1} \subseteq G_{\alpha_{j+1}} = \mathrm{N}_G^{j+1}(H),$$

tales que $H = G_l$ *para* $p^l = |H|$ *y* G_{α_j+l} *es un subgrupo normal de orden* p^{α_j+1} *de* $\mathrm{N}_G^{j+1}(H)$ *para cada* $0 \leq l \leq p^{\alpha_{j+1}} - p^{\alpha_j}$. *En particular* H *está incluído en un subgrupo de índice* p *de* G.

Teorema 3.3.9. *Denotemos con* H *a un* p*-subgrupo arbitrario de un grupo finito* G. *Si* $|H|$ *divide a* p^m *y* p^m *divide a* $|G|$, *entonces la cantidad de* p*-subgrupos de* G *de orden* p^m *que contienen 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 teorema se reduce al item 3) del Teorema 3.2.3. Supongamos ahora que $n > 0$ y que el teorema vale para subgrupos de G de orden p^{m+1}. Denotemos con $P_1, \ldots, P_u$ y con $Q_1, \ldots, Q_v$ a los subgrupos de orden p^{m+1} y p^m de G que contienen a H, respectivamente. Por hipótesis inductiva la cantidad a_j de los P_i's que contienen a un dado Q_j es congruente a 1 módulo p. Para terminar la demostración debemos ver que la cantidad b_i de los Q_j's que están contenidos en un dado P_i 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 contienen, se seguirá que $u \equiv v \pmod{p}$. Fijemos entonces P_i y supongamos que $Q_{j_1}, \ldots, Q_{j'_v}$ son los Q_j's que están contenidos en P_i. Debemos ver que $v' \equiv 1 \pmod{p}$. Por la Observación 3.3.8, $v' \geq 1$. Podemos suponer claramente que $v' > 1$. Por el Corolario 3.3.7 cada Q_{j_l} es normal en P_i y así, en particular, $Q_{j_1} Q_{j_2} = P_i$. Por la Proposición 1.6.8, se sigue de esto que $D_1 = Q_{j_1} \cap Q_{j_2}$ tiene orden p^{m-1}. Además D_1 es normal en P_i ya que es la intersección de dos subgrupos normales de P_i. Por el Corolario 3.3.4, P_i/D_1 es abeliano y tiene $p+1$ subgrupos de orden p. En consecuencia en el conjunto $\{Q_{j_1}, \ldots, Q_{j'_v}\}$ hay $p+1$ elementos que contienen a D_1. Si $v' = p+1$ esto termina la demostración. Supongamos que $v' > p+1$ y tomemos $Q_{j_{l_3}}$ tal que D_1 no está incluído en $Q_{j_{l_3}}$. Escribamos $D_2 = Q_{j_1} \cap Q_{j_{l_3}}$. Como antes podemos ver que en $\{Q_{j_1}, \ldots, Q_{j'_v}\}$ hay $p+1$ elementos que contienen a D_2. Claramente Q_{j_1} es el único elemento de $\{Q_{j_1}, \ldots, Q_{j'_v}\}$ que contiene a la vez a D_1 y a D_2, ya que si hubiera otro Q_{j_l}, entonces $Q_{j_1} \cap Q_{j_l}$ contendría a D_1 y a D_2 lo que es absurdo pues $|D_1| = |D_2| = |Q_{j_1} \cap Q_{j_l}| = p^{m-1}$ y $D_1 \neq D_2$. Así hay $2p+1$ elementos en $\{Q_{j_1}, \ldots, Q_{j'_v}\}$ que contienen a D_1 o a D_2. Si $v' = 2p+1$ la demostración se termina aquí. Supongamos entonces que $v' > 2p+1$ y tomemos $Q_{j_{l_4}}$ tal que ni D_1 ni D_2 están incluídos en $Q_{j_{l_4}}$ y escribamos $D_3 = Q_{j_1} \cap Q_{j_{l_4}}$. Como antes en $\{Q_{j_1}, \ldots, Q_{j'_v}\}$ hay $p+1$ elementos que contienen a D_3. Nuevamente Q_{j_1} es el único elemento de $\{Q_{j_1}, \ldots, Q_{j'_v}\}$ que contiene a la vez a D_1 y a D_3 y similarmente es el único elemento de $\{Q_{j_1}, \ldots, Q_{j'_v}\}$ que contiene a la vez a D_2 y a D_3. Así hay $3p+1$ elementos en $\{Q_{j_1}, \ldots, Q_{j'_v}\}$ que contienen a D_1, a D_2 o a D_3. Si $v' = 3p+1$ esto termina la demostracón y si no podemos continuar con este procedimiento hasta que todos los elementos de $\{Q_{j_1}, \ldots, Q_{j'_v}\}$ estén listados. □

Corolario 3.3.10. *Si* p^m *divide al orden de un grupo finito* G, *entonces la cantidad de subgrupos de* G *de orden* p^m *es congruente a* 1 *módulo* p.

Demostración. Por el teorema anterior aplicado al caso $H = \{1\}$. $\square$

Observación 3.3.11. *Supongamos que H es un subgrupo normal de un p-grupo finito G. Fijemos $m < n$ tales que $p^m \leq |H|$ y $p^n \leq |G|$ y denotemos con X al conjunto de los subgrupos de orden p^n de G que cortan a H en un subgrupo de orden p^m. El grupo G actúa por conjugación sobre X. Claramente el conjunto* $\mathrm{PF}(X)$ *de los puntos fijos de X por esta acción, consiste de los subgrupos normales de G que pertenecen a X. Además $\#(\mathrm{PF}(X)) \equiv \#(X) \pmod p$ ya que $X \setminus \mathrm{PF}(X)$ es una unión disjunta de órbitas no triviales y que, por el Corolario 3.1.12, el cardinal de cada órbita no trivial de X es una potencia positiva de p. Así*

$$\#(\{P \in X : P \text{ es un subgrupo normal de } G\}) \equiv \#(X) \pmod p$$

Por ejemplo, por el Teorema 3.3.9, si H un subgrupo normal de un p-grupo finito G y $|H| \leq p^n \leq |G|$, entonces la cantidad de subgrupos normales de G de orden p^n que contienen a H es congruente a 1 *módulo p y, por el Teorema 3.3.1, la cantidad de subgrupos de orden p^n, de un p-grupo finito G, que cortan al centro* $\mathrm{Z}(G)$ *de G trivialmente, es es congruente a* 0 *módulo p.*

Proposición 3.3.12 (Caracterización de grupos de orden p^3). *Supongamos que G es un grupo de orden p^3 con p primo. Vale lo siguente:*

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 a*

$$G_1 = \langle x, y : \ x^{p^2} = y^p = 1 \text{ e } yxy^{-1} = x^{1+p} \rangle$$

o

$$G_2 = \langle x, y, z : \ x^p = y^p = z^p = 1,\ xy = yx,\ xz = zx \text{ e } yz = xzy \rangle.$$

Demostración. Si G tiene elementos de orden p^3 entonces es cíclico. Supongamos ahora que G tiene elementos de orden p^2, pero no de orden p^3. Denotemos con x a uno de estos elementos y tomemos $y \in G \setminus \langle x \rangle$. Claramente G está generado por x e y. Además, dado que $|G : \langle x \rangle| = p$, por el Corolario 3.1.7, $\langle x \rangle$ es un subgrupo normal de G. En consecuencia $y^p \in \langle x \rangle$ y existe $1 \leq r < p^2$ tal que $yxy^{-1} = x^r$. Supongamos primero que $r = 1$ (es decir que G es conmutativo). Escribamos $y^p = x^j$ con $0 \leq j < p^2$. Como $1 = y^{p^2} = x^{pj}$ tenemos que p/j y así existe $0 \leq t < p$ tal que $j = pt$. Reemplazando y por yx^{-t} podemos suponer que $y^p = 1$, lo que implica que $\langle x \rangle \cap \langle y \rangle = \{1\}$. Por el Teorema 1.14.7 se sigue de esto que $G \simeq \langle x \rangle \times \langle y \rangle \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_p$. Supongamos ahora que $r > 1$. Un argumento inductivo prueba que $y^i x y^{-i} = x^{r^i}$ para todo $i \geq 1$. En particular $x = y^p x y^{-p} = x^{r^p}$, de donde $r^p \equiv 1 \pmod{p^2}$. Dado que $(1+p)^p \equiv 1 \pmod{p^2}$ y que $\mathbb{Z}_{p^2}^*$ tiene un único subgrupo de orden p (pues es cíclico), existe $0 < \alpha < p$ tal que $1 + p \equiv r^\alpha \pmod{p^2}$. Notemos que $y^\alpha \in G \setminus \langle x \rangle$ pues p no divide a α. Cambiando y por y^α podemos suponer que $r = 1 + p$, ya que $y^\alpha x y^{-\alpha} = x^{r^\alpha} = x^{1+p}$. Como antes existe $0 \leq t < p$ tal que $y^p = x^{tp}$. Dividimos la demostración ahora en los casos $p = 2$ y $p > 2$. En el primero las posibilidades para y^2 son 1 o x^2, ya que es imposible que sea $y^2 = x$ o $y^2 = x^3$, pues esto implicaría que $y^4 = x^2 \neq 1$. Si $y^2 = 1$, entonces G está generado

por dos elementos x e y que satisfacen $x^4 = y^2 = 1$ e $yxy^{-1} = x^3$ y así $G \simeq D_4$ y si $y^2 = x^2$, entonces G está generado por dos elementos x e y que satisfacen $x^4 = 1$, $y^2 = x^2$ e $yxy^{-1} = x^3$ y así $G \simeq H_2$. Pasemos al caso $p > 2$. Haciendo inducción primero en j y luego en i podemos ver que $y^i x^j = x^{j(1+p)^i} y^i$. Usando esto podemos ver ahora por inducción en l que

$$(x^{-t(1+p)}y)^l = x^{-t(1+p)(1+\cdots+(1+p)^{l-1})}y^l = x^{-t(1+p)\frac{(1+p)^l-1}{p}}y^l,$$

Como $p > 2$ tenemos que $(1+p)^p \equiv 1 + p^2 \pmod{p^3}$ y así la formula de arriba da en particular que

$$(x^{-t(1+p)}y)^p = x^{-t(1+p)\frac{(1+p)^p-1}{p}}y^p = x^{-t(1+p)p}y^p = x^{-tp}y^p = 1.$$

Dado que

$$(x^{-t(1+p)}y)x(x^{-t(1+p)}y)^{-1} = x^{-t(1+p)}yxy^{-1}x^{t(1+p)} = x^{-t(1+p)}x^{1+p}x^{t(1+p)} = x^{1+p},$$

obtenemos, reemplazando y por $x^{-t(1+p)}y$, que G está generado por dos elementos x e y que satisfacen $x^{p^2} = y^p = 1$ e $yxy^{-1} = x^{1+p}$ y así $G \simeq G_1$. Queda por considerar el caso en que todos los elementos de G tienen orden p. Supongamos primero que G es abeliano y tomemos $x \in G \setminus \{1\}$. Tomemos ahora $y, z \in G$ tales que sus clases en $G/\langle x\rangle$ generan $G/\langle x\rangle$. Esto implica en particular que $\langle y\rangle \cap \langle z\rangle = \{1\}$ y que $\langle x\rangle \cap \langle y, z\rangle = \{1\}$. Así, por Teorema 1.14.7, $G \simeq \langle x\rangle \times \langle y\rangle \times \langle z\rangle \simeq \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$. Supongamos ahora que G no es conmutativo. Entonces, por el Ejercicio 3), $p > 2$ y, por los Corolarios 3.3.4 y 3.3.5, $\mathrm{Z}(G) = [G, G]$ tiene orden p y $G/\mathrm{Z}(G) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Tomemos $y, z \in G$ tales que sus clases en $G/\mathrm{Z}(G)$ generen $G/\mathrm{Z}(G)$. El elemento $x = yzy^{-1}z^{-1} \in \mathrm{Z}(G)$ es distinto de 1, ya que en caso contrario $G = \langle y, z, \mathrm{Z}(G)\rangle$ sería abeliano. Por lo tanto G está generado por elementos x, y y z que satisfacen $x^p = y^p = z^p = 1$, $xy = yx$, $xz = zx$ e $yz = xzy$ y así $G \simeq G_2$. □

Con respecto a la proposición anterior queda por comprobar que existen grupos isomorfos a G_1 y G_2. Estos se pueden construír usando el producto semidirecto, lo que hacemos a continuación

Construcción de G_1. *Como $(1+p)^p \equiv 1 \pmod{p^2}$ la aplicación $f\colon \mathbb{Z}_{p^2} \to \mathbb{Z}_{p^2}$, definida por $f(x) = x(1+p)$ es un automorfismo de orden p. Así, podemos obtener un morfismo de grupos $\Phi\colon \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_{p^2})$ poniendo $\Phi(i) = f^i$. El producto semidirecto $\mathbb{Z}_{p^2} \times_\Phi \mathbb{Z}_p$ es un grupo no abeliano de orden p^3 que posee elementos de orden p^2 y así es isomorfo a G_1.*

Construcción de G_2. *La aplicación $f\colon \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p$, definida por la fórmula $f(x, y) = (x, x + y)$ es un automorfismo de orden p. Así, podemos obtener un morfismo de grupos $\Phi\colon \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p)$ poniendo $\Phi(i) = f^i$. El producto semidirecto $(\mathbb{Z}_p \times \mathbb{Z}_p) \times_\Phi \mathbb{Z}_p$ es un grupo no abeliano de orden p^3. Vamos a probar que si $p > 2$, entonces todos los elementos de $(\mathbb{Z}_p \times \mathbb{Z}_p) \times_\Phi \mathbb{Z}_p$ tienen orden p y así, $(\mathbb{Z}_p \times \mathbb{Z}_p) \times_\Phi \mathbb{Z}_p$ es isomorfo a G_2. Para ello es suficiente ver que*

$$((x, y), z)^m = \left(\left(mx, \frac{m(m-1)}{2}xz + my\right), mz\right) \qquad \textit{para todo } m \geq 1.$$

El caso $m = 1$ es trivial. Supongamos que la igualdad vale para m. Entonces

$$\begin{aligned}((x,y),z)^{m+1} &= ((x,y),z)\left(\left(mx, \frac{m(m-1)}{2}xz + my\right), mz\right)\\ &= \left((x,y) + f^z\left(mx, \frac{m(m-1)}{2}xz + my\right), (m+1)z\right)\\ &= \left((x,y) + \left(mx, \frac{m(m-1)}{2}xz + my + mxz\right), (m+1)z\right)\\ &= \left(\left((m+1)x, \frac{(m+1)m}{2}xz + (m+1)y\right), (m+1)z\right).\end{aligned}$$

Proposición 3.3.13. *Si H es un subgrupo abeliano y normal maximal de un p-grupo G, entonces $H = \mathrm{C}_G(H)$.*

Demostración. Como H es conmutativo, claramente $H \subseteq \mathrm{C}_G(H)$. Veamos la inclusión recíproca. Por el apartado que sigue a la Observación 1.13.6, el centro $\mathrm{C}_G(H)$ de H en G es un subgrupo normal de $\mathrm{N}_G(H)$. Como $H \subseteq G$ es normal, $\mathrm{N}_G(H) = G$ y así $\mathrm{C}_G(H)$ es un subgrupo normal de G. En consecuencia $\mathrm{C}_G(H)/H$ es un subgrupo normal del grupo nilpotente G/H. Por el Teorema 3.3.1, si $H \subsetneq \mathrm{C}_G(H)$, entonces existe $a \in \mathrm{C}_G(H) \setminus H$ tal que su clase en G/H pertenece a $\mathrm{Z}(G/H)$, de lo cual se sigue facilmente que $\langle H, a\rangle$ es un subgrupo normal y abeliano de G. □

3.4.Grupos de orden pequeño. Como aplicación del teorema de Cauchy vamos a caracterizar los grupos de orden pq con p y q primos distintos.

Proposición 3.4.1 (Caracterización de grupos de orden pq). *Supongamos que G es un grupo de orden pq con p y q primos y $q < p$. Vale lo siguiente:*

1) *Si G es abeliano, entonces $G \simeq \mathbb{Z}_{pq}$.*
2) *Si G no es abeliano, entonces q divide a $p-1$, el conjunto*

$$R = \{r : 1 < r < p \text{ y } r^q \equiv 1 \pmod p\}$$

no es vacío y G está generado por elementos x e y, de órdenes p y q respectivamente, que satisfacen $yxy^{-1} = x^{r_0}$, donde r_0 es el menor elemento de R.

Demostración. Por el Teorema 3.2.13 existen elementos $x, z \in G$ tales que $|x| = p$ y $|z| = q$. Por el Corolario 3.1.6, $\langle x\rangle$ es normal. Si $\langle z\rangle$ también lo es, entonces por el Corolario 1.14.11, $G \simeq \langle x\rangle \times \langle z\rangle \simeq \mathbb{Z}_{pq}$. Podemos suponer entonces que $\langle z\rangle$ no es normal. Como $\langle x\rangle$ es un subgrupo normal de G, existe $0 \leq r < p$ tal que $zxz^{-1} = x^r$. Además dado que la igualdad $zxz^{-1} = 1$ es imposible y que G no es conmutativo debe ser $r > 1$. Por último de $zxz^{-1} = x^r$ se sigue facilmente por inducción en i que $z^i x z^{-i} = x^{r^i}$ para todo $i > 1$, de donde $x^{r^q} = z^q x z^{-q} = x$, lo que implica que $r^q \equiv 1 \pmod p$. Como $1 < r < p$ y q es primo esto implica que q es el orden de r en $\mathbb{Z}_p^*$ y así, 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 r que satisfacen $1 < r < p$ y $r^q \equiv 1 \pmod p$. Tomemos $y = z^\alpha \neq 1$. Dado que $z = y^\beta$, donde $\beta \in \mathbb{Z}_q$ es el inverso multiplicativo de α, resulta que $G = \langle x, y\rangle$.

Para terminar la demostración basta observar que $y^q = (z^\alpha)^q = (z^q)^\alpha = 1$ e $yxy^{-1} = z^\alpha x z^{-\alpha} = x^{r^\alpha} = x^{r_0}$. $\square$

Supongamos ahora que p y q son primos y que q divide a $p-1$. Por el Teorema de Cauchy existe $r \in \mathbb{Z}_p^*$ de orden q. Se sigue del anteúltimo de los ejemplos que aparecen en la sección 1.15 que, para cada tal r, existe efectivamente un grupo de orden pq que está generado por elementos x e y, de órdenes p y q respectivamente, que satisfacen $yxy^{-1} = x^r$.

En lo que sigue de esta subsección denotaremos con n_p a la cantidad de p-subgrupos de Sylow de un grupo finito G.

Proposición 3.4.2. *Ningún grupo G de orden p^2q, donde p y q son dos números primos distintos, es simple (más precisamente, G tiene un subgrupo normal de orden p^2 o un subgrupo normal de orden q).*

Demostración. Por el Corolario 3.2.5, $n_q = 1$, $n_q = p$ o $n_q = p^2$. Si $n_q = 1$, entonces el único q-subgrupo de Sylow de G es normal. Si $n_q = p$, entonces por el item 1) del teorema de Sylow, $p \equiv 1 \pmod q$, de donde $p > q$. Dado que, por los mismos resultados mencionados arriba, $n_p \mid q$ y $n_p \equiv 1 \pmod p$, esto implica que $n_p = 1$ y así G tiene un único p-subgrupo de Sylow que, por lo tanto, es normal. Por último si $n_q = p^2$, 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, que es normal por la misma razón que antes. $\square$

Proposición 3.4.3. *Ningún grupo G de orden $2pq$, donde $p < q$ son dos primos impares, es simple (más precisamente, G tiene un subgrupo normal de orden p o un subgrupo normal de orden q).*

Demostración. Por el item 1) del teorema de Sylow, $n_p = h_p p + 1$ y $n_q = h_q q + 1$, con h_p y h_q enteros no negativos. 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, $h_p, h_q \geq 1$ y se tiene

$$\begin{aligned}
\#\big((G \setminus S) \cup \{1\}\big) &= 2pq - \big((h_p p + 1)(p-1) + (h_q q + 1)(q-1)\big) \\
&\leq 2pq - \big((p+1)(p-1) + (q+1)(q-1)\big) \\
&= 2pq - (p^2 - 1 + q^2 - 1) \\
&= -(q-p)^2 + 2 < 2,
\end{aligned}$$

lo cual es absurdo ya que todos los 2-subgrupos de Sylow de G están claramente incluídos en $(G \setminus S) \cup \{1\}$. $\square$

Otros ejemplos.

1) *No existen subgrupos simples G de orden $36 = 2^2 3^2$. En efecto, tomemos un 3-subgrupo de Sylow de G. Por el Corolario 3.1.6, P contiene un subgrupo normal P', cuyo índice en G divide a $4 \operatorname{mdc}(3!, 3^2) = 12 < 36$.*
2) *No existen subgrupos simples G de orden $48 = 2^4 3$. En efecto, tomemos un 2-subgrupo de Sylow de G. Por el Corolario 3.1.6, P contiene un subgrupo normal P', cuyo índice en G divide a $3 \operatorname{mdc}(2!, 2^4) = 6 < 48$.*
3) *No existen grupos simples G de orden $56 = 2^3.7$. En efecto, como $n_7 \equiv 1 \pmod 7$ y $n_7 \mid 8$ resulta que $n_7 = 1$ u $n_7 = 8$. En el primer caso G tiene un*

único 7-subgrupo de de Sylow que, por lo tanto, es normal y, en el segundo, G tiene $8.6 = 48$ elementos de orden 7 y los restantes 8 elementos sólo pueden formar un 3-subgrupo de Sylow de G, que es normal por la misma razón que antes.

4) *No existen grupos simples G de orden $80 = 2^4.5$. En efecto, tomemos un 2-subgrupo de Sylow de G. Por el Corolario 3.1.6, P contiene un subgrupo normal P', cuyo índice en G divide a $5 \operatorname{mdc}(4!, 2^4) = 40 < 80$. También se puede proceder de la siguiente manera: Como $n_5 \equiv 1 \pmod 5$ y $n_5 \mid 2^4$ tenemos que $n_5 = 1$ o $n_5 = 16$. En el primer caso G tiene un único 5-subgrupo de de Sylow que, por lo tanto, es normal y, en el segundo, G tiene $16.4 = 64$ elementos de orden 5 y los restantes 16 elementos sólo pueden formar un 2-subgrupo de Sylow de G, que es normal por la misma razón que antes.*

5) *No existen grupos simples G de orden $84 = 2^2.3.7$. En efecto, como $n_7 \equiv 1 \pmod 7$ y $n_7 \mid 12$ resulta que $n_7 = 1$ y así, G tiene un único 7-subgrupo de Sylow que, por lo tanto, es normal.*

6) *No existen subgrupos simples G de orden $96 = 2^5 3$. En efecto, tomemos un 2-subgrupo de Sylow de G. Por el Corolario 3.1.6, P contiene un subgrupo normal P', cuyo índice en G divide a $3 \operatorname{mdc}(2!, 2^5) = 6 < 96$.*

Proposición 3.4.4. *Si G es un grupo simple y $|G| = 2^m p^n$ con $0 \leq m \leq 3$, p primo impar y $n \geq 0$, entonces $m = 0$ y $n = 1$ o $m = 1$ y $n = 0$.*

Demostración. Los casos $m = 0$ u $n = 0$ se siguen del Corolario 3.3.3. Supongamos que $m, n > 0$ y que G es simple de manera que $n_p \neq 1$. Dado que n_p divide a 2^m, debe ser $n_p = 2$, $n_p = 4$ u $n_p = 8$. Además se debe satisfacer que $n_p \equiv 1 \pmod p$. De esto se sigue inmediatamente que $n_p \neq 2$; que si $n_p = 4$, entonces $p = 3$ y que si $n_p = 8$, entonces $p = 7$. Supongamos primero que $n_p = 4$ y $p = 3$. Tomemos un 3-subgrupo de Sylow P de G y escribamos $N = \mathrm{N}_G(P)$. Por el Corolario 3.2.4, $|G : N| = 4$ y así, por el Corolario 3.1.5, G es isomorfo a un subgrupo de S_4. Por lo tanto $n = 1$ y $|G| = 2^m 3$. Tomemos ahora un 2-subgrupo de Sylow Q de G. Como $|G : Q| = 3$ se sigue del Corolario 3.1.5 que G es isomorfo a un subgrupo de S_3 y así $|G|$ divide a 6, lo cual es absurdo por el teorema de caracterización de grupos de orden pq. Supongamos abora que $n_p = 8$ y $p = 7$. Tomemos como antes un 7-subgrupo de Sylow P de G y escribamos $N = \mathrm{N}_G(P)$. Nuevamente por el Corolario 3.2.4, $|G : N| = 8$ y así, por el Corolario 3.1.5, G es isomorfo a un subgrupo de S_8. Por lo tanto $n = 1$ y $|G| = 2^4 7 = 56$, caso que ya fué considerado antes. □

Proposición 3.4.5. *Todo grupo simple de orden $60 = 2^2.3.5$ es isomorfo a A_5.*

Demostración. Por el Corolario 3.1.15 es suficiente ver que si G es un grupo simple de orden 60, entonces G tiene un subgrupo H de índice 5. Por el item 1) del teorema de Sylow y el Corolario 3.2.5, sabemos que $n_2 \in \{1, 3, 5, 15\}$ y $n_5 \in \{1, 6\}$. Como G es simple, por el Corolario 3.2.6 no puede ser ni $n_2 = 1$ ni $n_5 = 1$ y por el Teorema 3.1.4 y el Corolario 3.2.4 tampoco puede ser $n_2 = 3$. En particular G tiene 24 elementos de orden 5. Si $n_2 = 5$, entonces por el Corolario 3.2.4 podemos tomar $H = \mathrm{N}_G(P)$ dónde P es un 2-subgrupo de Sylow arbitrario. Supongamos que $n_2 = 15$. Si cada par de 2-subgrupos de Sylow de G tuviera intersección trivial habría $15.3 + 1 = 46$ elementos de orden par, que sumados a los 24 de orden 5, daría 70 elementos, lo que es absurdo. Así, 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 $\langle P_1, P_2\rangle$. Como G es simple es imposible entonces que $\langle P_1, P_2\rangle$ sea igual a G. Dado que $4 = |P_1|$ divide propiamente a $|\langle P_1, P_2\rangle|$ y $|\langle P_1, P_2\rangle|$ a su vez divide propiamente a $|G| = 60$, debe ser $|\langle P_1, P_2\rangle| = 12$ o $|\langle P_1, P_2\rangle| = 20$, pero esto último es imposible por el Teorema 3.1.4. Así el índice de $\langle P_1, P_2\rangle$ en G es 5 y podemos tomes $H = \langle P_1, P_2\rangle$. □

3.5.Caracterización de los grupos de orden 12. Supongamos que G es un grupo de orden 12. Por la Proposición 3.4.2, sabemos que G tiene un subgrupo normal H de orden 3 o de orden 4. En el primer caso denotamos con K a un 2-subgrupo de Sylow y en el segundo a un 3-subgrupo de Sylow de G. Como 3 y 4 son coprimos $H \cap K = \{1\}$ y así existe $\phi\colon K \to \mathrm{Aut}(H)$ tal que $G \simeq H \times_\phi K$. Tenemos las siguientes posibilidades:

1) $H \simeq \mathbb{Z}_3$ y $K \simeq \mathbb{Z}_4$,
2) $H \simeq \mathbb{Z}_3$ y $K \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$,
3) $H \simeq \mathbb{Z}_4$ y $K \simeq \mathbb{Z}_3$,
4) $H \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$ y $K \simeq \mathbb{Z}_3$.

Caso 1: Como $\mathrm{Aut}(\mathbb{Z}_3) \simeq \mathbb{Z}_2$, sólo hay dos morfismos $\phi_i\colon \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3)$ $(i = 1, 2)$, que están definidos por

$$\phi_1(1)(x) = x \qquad \text{y} \qquad \phi_2(1)(x) = 2x,$$

respectivamente. Los grupos asociados

$$G_1 = \mathbb{Z}_3 \times_{\phi_1} \mathbb{Z}_4 = \mathbb{Z}_3 \times \mathbb{Z}_4 \qquad \text{y} \qquad G_2 = \mathbb{Z}_3 \times_{\phi_2} \mathbb{Z}_4$$

no son isomorfos ya que el primero es abeliano y el segundo no.

Caso 2: Hay cuatro morfismos $\phi_i\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ $(i = 1, 2, 3, 4)$, que están definidos por

$$\begin{aligned}
&\phi_1(1,0)(x) = x \qquad \text{y} \qquad \phi_1(0,1)(x) = x,\\
&\phi_2(1,0)(x) = x \qquad \text{y} \qquad \phi_2(0,1)(x) = 2x,\\
&\phi_3(1,0)(x) = 2x \qquad \text{y} \qquad \phi_3(0,1)(x) = x,\\
&\phi_4(1,0)(x) = 2x \qquad \text{y} \qquad \phi_4(0,1)(x) = 2x,
\end{aligned}$$

respectivamente. Los grupos asociados a los dos primeros

$$G_3 = \mathbb{Z}_3 \times_{\phi_1} (\mathbb{Z}_2 \times \mathbb{Z}_2) = \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \qquad \text{y} \qquad G_4 = \mathbb{Z}_3 \times_{\phi_2} (\mathbb{Z}_2 \times \mathbb{Z}_2)$$

no son isomorfos ya que el primero es abeliano y el segundo no y tampoco son isomorfos ni a G_1 ni a G_2 ya que tienen 2-subgrupos de Sylow no isomorfos a los de ellos. Por último claramente existen isomorfismos

$$\phi_{32}\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \qquad \text{y} \qquad \phi_{42}\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2,$$

tales que $\phi_3 = \phi_2 \circ \phi_{32}$ y $\phi_4 = \phi_2 \circ \phi_{42}$ y así, por la por la Observación 1.15.3, los grupos asociados a ϕ_3 y a ϕ_4 son isomorfos a G_4.

Caso 3: Como $\mathrm{Aut}(\mathbb{Z}_4) \simeq \mathbb{Z}_2$ el único morfismo $\phi_1 \colon \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_4)$ es el trivial y el grupo asociado $\mathbb{Z}_4 \times_{\phi_1} \mathbb{Z}_3 = \mathbb{Z}_4 \times \mathbb{Z}_3$ es isomorfo a G_1.

Caso 4: Por la Observación 1.14.14 sabemos que $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathrm{GL}_2(\mathbb{Z}_2)$. Así hay tres morfismos $\phi_i \colon \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ $(i = 1, 2, 3)$, que son los que mandan el 1 en la identidad y en los dos automorfismos de $\mathbb{Z}_2 \times \mathbb{Z}_2$ que tienen orden 3 respectivamente, y que están definidos por

$$\phi_1(1)(x, y) = (x, y), \quad \phi_2(1)(x, y) = (x + y, x) \quad \text{y} \quad \phi_3(1)(x, y) = (y, x + y).$$

El grupo $(\mathbb{Z}_2 \times \mathbb{Z}_2) \times_{\phi_1} \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, asociado a ϕ_1, es isomorfo a G_3, mientras que el grupo

$$G_5 = (\mathbb{Z}_2 \times \mathbb{Z}_2) \times_{\phi_2} \mathbb{Z}_3$$

no es isomorfo ni a G_1 ni a G_3 ya que no es abeliano, ni a G_2 ni a G_4 ya que los 2-subgrupos de Sylow de estos últimos no son invariantes y el de G_5 si. Por último el isomorfismo $\phi_{32} \colon \mathbb{Z}_3 \to \mathbb{Z}_3$, definido por $\phi_{21}(x) = 2x$, claramente satisface $\phi_3 = \phi_2 \circ \phi_{32}$ y así, por la por la Observación 1.15.3, el grupo asociados a ϕ_3 es isomorfo a G_5.

Hay en definitiva cinco grupos no isomorfos G_1, G_2, G_3, G_4 y G_5, de orden 12. Del item 1) del teorema de Sylow y del Corolario 3.2.5 se sigue facilmente que:

1) G_2 tiene un único 3-subgrupo de Sylow, isomorfo a $\mathbb{Z}_3$, y tres 2-subgrupos de Sylow, isomorfos a $\mathbb{Z}_4$,
2) G_4 tiene un único 3-subgrupo de Sylow, isomorfo a $\mathbb{Z}_3$, y tres 2-subgrupos de Sylow, isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_2$,
3) G_5 tiene un único 2-subgrupo de Sylow, que es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, y cuatro 3-subgrupos de Sylow, isomorfos a $\mathbb{Z}_3$.

Observación 3.5.1. *Por los Ejemplos 3, 4 y 5 que siguen al Corolario 3.2.6,*

$$A_4 \simeq G_5, \qquad D_6 \simeq G_4 \qquad y \qquad H_3 \simeq G_2.$$

En cierto sentido A_4 es el menos conmutativo de estos grupos, ya que su centro es trivial y su subgrupo conmutador tiene orden 4, mientras que los centros y subgrupos conmutadores de D_6 y H_3 tienen todos orden 2. Otra cosa que distinge a A_4 de D_6 y H_3 es que el primero no tiene subgrupos de orden 6 (Proposición 2.3.9) mientras que los otros si lo tienen. Más aún $(1, 2) \in G_2$ y $(1, (1, 0)) \in G_4$ son elementos de orden 6.

3.6.Otros resultados acerca de p-grupos finitos. A continuación probamos algunos resultados más acerca de p-grupos finitos.

Lema 3.6.1. *Si dos elementos a, b de un grupo G conmutan con $[a, b]$, entonces*

$$[a, b]^n = [a^n, b] = [a, b^n] \quad \forall n \in \mathbb{Z} \quad y \quad (ab)^n = [b, a]^{n(n-1)/2} a^n b^n \quad \forall n \in \mathbb{N}.$$

Demostración. Probemos la primera igualdad para $n \geq 0$ por inducción. Esta es clara para $n = 0$. Suponiendo que es cierto para $n \geq 0$, entonces

$$\begin{aligned}
[a, b]^n [a, b] &= a[a, b]^n b a^{-1} b^{-1} && \text{porque } a \text{ conmuta con } [a, b] \\
&= a[a^n, b] b a^{-1} b^{-1} && \text{por inducción} \\
&= a(a^n b a^{-n} b a^{-1}) b a^{-1} b^{-1} \\
&= [a^{n+1}, b].
\end{aligned}$$

Como

$$[a,b] = aba^{-1}b^{-1} = a^{-1}a[a,b] = a^{-1}[a,b]a = ba^{-1}b^{-1}a = [b,a^{-1}]$$

vale que $[a,b]^{-1} = [b,a^{-1}]^{-1} = [a^{-1},b]$, de donde

$$[a,b]^{-n} = [a^{-1},b]^n = [a^{-n},b] \quad \text{para todo } n \geq 0.$$

Por último

$$[a,b^n] = [b^n,a]^{-1} = [b,a]^{-n} = [a,b^n].$$

Probemos ahora la segunda igualdad por inducción en n. El caso $n = 0$ es trivial y suponiendo que la igualdad vale para $n \geq 0$,

$$\begin{aligned}
(ab)^n ab &= [b,a]^{n(n-1)/2} a^n b^n ab && \text{por inducción} \\
&= [b,a]^{n(n-1)/2} a^{n+1} [a^{-1},b^n] b^{n+1} \\
&= [b,a]^{n(n-1)/2} a^{n+1} [a,b]^{-n} b^{n+1} && \text{por la primera igualdad} \\
&= [b,a]^{n(n-1)/2} [a,b]^{-n} a^{n+1} b^{n+1} && \text{porque } a \text{ conmuta con } [a,b] \\
&= [b,a]^{n(n-1)/2} [b,a]^{n} a^{n+1} b^{n+1} \\
&= [b,a]^{(n+1)n/2} a^{n+1} b^{n+1},
\end{aligned}$$

como afirmamos. □

Para cada grupo G y cada entero n denotamos con G^n a $\{x^n : x \in G\}$ y con $G[n]$ a $\{x \in G : x^n = 1\}$.

Proposición 3.6.2. *Si G es un p-grupo finito y no cíclico y $\langle a\rangle \subseteq G$ es un subgrupo de índice p de G, entonces $\langle a\rangle$ es un subgrupo normal de G y $G^p = \langle a^p\rangle$. Además*

$$|G : G^p| = p^2, \quad [G,G] \subseteq G^p = \langle a\rangle \cap \langle b\rangle = \mathrm{Z}(G),$$

para cualquier $b \in G \setminus \langle a\rangle$ y vale lo siguiente:

1) *Si p es impar, entonces la aplicación $f\colon G \to G^p$, definida por $f(x) = x^p$ es un morfismo de grupos y su núcleo $G[p]$ es isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$.*
2) *Si $p = 2$, entonces la aplicación $f\colon G \to G^2$, definida por $f(x) = x^2$ no es un morfismo de grupos, pero si lo es la aplicación $g\colon G \to G^4$, definida por $g(x) = x^4$. Además su núcleo $G[4]$ tiene orden 8.*

Demostración. Por el Corolario 3.1.7, $\langle a\rangle$ es un subgrupo normal de G. Como $G/\langle a\rangle$ tiene orden p para cada $b \in G$ se satisface que $b^p = a^q$ para algún $q \in \mathbb{N}$. Si p y q son coprimos, entonces existen $r, s \in \mathbb{Z}$ tales que $1 = r|a| + sq$ y así, $a = a^{r|a|+sq} = a^{sq} = b^{sp}$, lo que implica que $\langle a\rangle \subseteq \langle b^p\rangle \subsetneq \langle b\rangle$, contradiciendo la hipótesis. Por lo tanto $G^p = \langle a^p\rangle \subsetneq \langle a\rangle$. Claramente G^p es un subgrupo normal de G. Como $|G : G^p| = |G : \langle a\rangle||\langle a\rangle : \langle a^p\rangle| = p^2$, el cociente G/G^p es abeliano y, en consecuencia, $[G,G] \subseteq G^p$. Tomemos $b \in G \setminus \langle a\rangle$. Evidentemente $G = \langle a\rangle\langle b\rangle$ de manera de que cada elemento de G se expresa como el producto de una potencia de a y una de b. Como los elementos de $\langle a\rangle \cap \langle b\rangle$ conmutan tanto con las potencias de a como con las de b, vale que $G^p \subseteq \langle a\rangle \cap \langle b\rangle \subseteq \mathrm{Z}(G)$. Por último no puede ser $G^p \subsetneq \mathrm{Z}(G)$, ya que en es caso $|G : \mathrm{Z}(G)| = p$ contradiciendo la Proposición 1.13.1.

En particular a y b conmutan con $[a,b]$. Por el Lema 3.6.1, $(ab)^p = [b,a]^{p(p-1)/2}a^pb^p$. Además $[b,a]^p = [b,a^p] = 1$ ya que $a^p \in \mathrm{Z}(G)$. Si p es impar, p divide a $p(p-1)/2$ y así, $(ab)^p = a^pb^p$. Claramente el núcleo de la aplicación $f\colon G \to G^p$, dado por $f(x) = x^p$ es $G[p] = \{x \in G : x^p = 1\}$ y $|G[p]| = |G : G^p| = p^2$, de donde $G[p]$ es isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$. Si $p = 2$, entonces $(ab)^2 = [b,a]a^2b^2$ y como G no es conmutativo $[b,a] \neq 1$. Así la aplicación $f\colon G \to G^p$, definida por $f(x) = x^2$ no es un morfismo de grupos, pero como $(ab)^4 = [b,a]^6a^4b^4$ y $[b,a]^6 = [b,a^6] = 1$, si lo es la aplicación $g\colon G \to G^4$. Finalmente $|G[4]| = |G : G^4| = |G : G^2||G^2 : G^4| = 8$, ya que $G^2 = \langle a^2\rangle$ implica $G^4 = \langle a^4\rangle$ y claramente $|\langle a^2\rangle : \langle a^4\rangle| = 2$. □

Teorema 3.6.3. *Si G es un p-grupo finito que tiene un único subgrupo de orden p y al menos dos subgrupos cíclicos de índice p, entonces $p = 2$ y $G \simeq H_2$.*

Demostración. Usamos libremente las notaciones y resultados de la proposición anterior. Por el item 1) de esa proposición $p = 2$ ya que en caso contrario $G[p]$ es un subgrupo de G que tiene más de un subgrupo de orden p. Si $G[4]$ no tiene al menos dos subgrupos cíclicos de orden 4, entonces debe tener más de un elemento de orden 2, lo que contradice la hipótesis. Así hay al menos dos subgrupos cíclicos $\langle x\rangle$ y $\langle y\rangle$ de orden 4 en $G[4]$. Afirmamos que $a^4 = 1$. En efecto, en caso contrario podríamos tomar $x \in \langle a^2\rangle = \mathrm{Z}(G)$ y entonces $\langle x\rangle\langle y\rangle$ sería abeliano, lo que contradice la hipótesis ya que en ese caso hay al menos dos elementos de orden dos en $G[4]$, pues $x^2 \neq y^2$ o $x^2 \neq xy^{-1}$. Así $|G| = |G : G^2||G^2| = |G : G^2||G^2| = |G : G^2|\langle a^2\rangle = 2^3$. El resultado se sigue ahora de la Proposición 3.6.12. En efecto $\mathbb{Z}_8$ queda descartado porque es cíclico y $\mathbb{Z}_4 \times \mathbb{Z}_2$ y $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ porque tienen más de un subgrupo de orden 2. Lo mismo pasa con D_4 ya que, por el Ejemplo 3 de la subsección 1.6, este grupo tiene 6 subgrupos de orden 2. Notemos por último que, por el Ejemplo 4 de la subsección 1.6, el grupo H_2 tiene 4 subgrupos cíclicos de índice 2 y sólo un subgrupo de orden 2.

Para lo que sigue necesitamos calcular el grupo de unidades $\mathbb{Z}_{2^r}^*$ del anillo $\mathbb{Z}_{2^r}$. Más generalmente calcularemos $\mathbb{Z}_{p^r}^*$ para todo primo p.

Proposición 3.6.4. *Se satisfacen:*

- *$(\mathbb{Z}/2^m\mathbb{Z})^*$ es cíclico si $m \leq 2$ e isomorfo a $\mathbb{Z}/2^{m-2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ si $m \geq 3$. Además, en este último caso $(\mathbb{Z}/2^m\mathbb{Z})^* = \{\pm 5^i : 0 \leq i < m-2\}$, donde las operaciones son realizadas en $\mathbb{Z}/2^m\mathbb{Z}$*
- *Si p es impar, $(\mathbb{Z}/p^m\mathbb{Z})^*$ es cíclico.*

Demostración. Cuando $m = 1$ todo esto se sigue de que el grupo de unidades de un cuerpo finito es cíclico. Así podemos suponer que $m > 1$. En la demostración de los dos items usaremos que que si $p = 2$ e $i > 1$ o $p > 2$ e $i \geq 1$, entonces

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

lo que se sigue de un cálculo sencillo. Para verificar que vale el segundo item será suficiente ver que $1 + p \in (\mathbb{Z}/p^m\mathbb{Z})^*$ tiene orden p^{m-1} y que existe $x \in (\mathbb{Z}/p^m\mathbb{Z})^*$ de orden $p-1$, ya que entonces $x(1+p)$ tendrá orden $(p-1)p^{m-1}$ en $(\mathbb{Z}/p^m\mathbb{Z})^*$. Usando $(*)$ es fácil ver, por inducción en i, que

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

lo que implica que el orden de $1+p$ en $(\mathbb{Z}/p^m\mathbb{Z})^*$ es p^{m-1}. Veamos la existencia del x mencionado arriba. Tomemos $z \in \mathbb{Z}/p^m\mathbb{Z}$ tal que $\pi(z) \in (\mathbb{Z}/p\mathbb{Z})^*$ tiene orden $p-1$, donde $\pi\colon \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ es la proyección canónica. Entonces $z \in (\mathbb{Z}/p^m\mathbb{Z})^*$ y tiene orden $(p-1)p^i$ con $0 \leq i < m$, lo que implica que el orden de $x = z^{p^i}$ en $(\mathbb{Z}/p^m\mathbb{Z})^*$ es $p-1$. Veamos ahora que vale el primer item. Es inmediato que el grupo de unidades de $\mathbb{Z}/2^m\mathbb{Z}$ es cíclico si $m = 2$. Supongamos ahora que $m \geq 3$. Como $5 = 1 + 2^2$, de la fórmula $(*)$ aplicada a $p = 2$, se sigue que

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

de donde 5 tiene orden 2^{m-2} en $(\mathbb{Z}/2^m\mathbb{Z})^*$. En consecuencia $\{5^i : 0 \leq i < m-2\}$ es un subgrupo cíclico de $(\mathbb{Z}/2^m\mathbb{Z})^*$ que tiene 2^{m-2} elementos. Además, por la fórmula de arriba, $5^{2^{m-3}}$ es congruente a $1+2^{m-1}$ módulo 2^m y, por lo tanto, distinto de -1 en $\mathbb{Z}/2^m\mathbb{Z}$. Dado que $5^{2^{m-3}}$ y -1 tienen ambos orden 2 en $(\mathbb{Z}/2^m\mathbb{Z})^*$, el subgrupo $\{\pm 5^i : 0 \leq i < m-2\}$ de $(\mathbb{Z}/2^m\mathbb{Z})^*$ no es cíclico. Por consiguiente contiene propiamente a $\{5^i : 0 \leq i < m-2\}$ y coincide así con $(\mathbb{Z}/2^m\mathbb{Z})^*$. Por último es fácil ver que $\{\pm 5^i : 0 \leq i < m-2\}$ es isomorfo a $\mathbb{Z}/2^{m-2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. □

Lema 3.6.5. *Si a y b son dos elementos de un grupo G que satisfacen $|a| = 2^m$ con $m \geq 3$, $b^2 = a^{2^r}$ con $0 \leq r < m$ y $bab^{-1} = a^t$, entonces*

$$t \equiv \pm 1 \pmod{2^m} \qquad o \qquad t \equiv \pm 1 + 2^{m-1} \pmod{2^m}.$$

Además, en los últimos dos casos G contiene al menos dos involuciones.

Demostración. Como $b^2 = a^{2^r}$ conmuta con a,

$$a = b^2ab^{-2} = ba^tb^{-1} = (bab^{-1})^t = (a^t)^t = a^{t^2},$$

de donde $t^2 \equiv 1 \pmod{2^m}$ y la clase de t en $\mathbb{Z}/2^m\mathbb{Z}$ es una involución. Por la Proposición 3.6.4, $t \equiv \pm 1 \pmod{2^m}$ o $t \equiv \pm 1 + 2^{m-1} \pmod{2^m}$. Resta ver que en los últimos dos casos G contiene al menos dos involuciones. Claramente una de ellas es $x^{2^{m-1}}$. Para cada entero k,

$$(a^kb)^2 = a^k(ba^kb^{-1})b^2 = a^k(bab^{-1})^kb^2 = a^k(a^t)^kb^2 = a^{k+tk+2^r},$$

Supongamos que $t \equiv 1 + 2^{m-1} \pmod{2^m}$. Entonces $(a^kb)^2 = a^{2s}$, donde

$$s \equiv k(1 + 2^{m-2}) + 2^{r-1} \pmod{2^{m-1}}.$$

Dado que $1 + 2^{m-2}$ es impar, existe k_0 tal que

$$s \equiv k_0(1 + 2^{m-2}) + 2^{r-1} \equiv 0 \pmod{2^{m-1}}.$$

En consecuencia, $(a^{k_0}b)^2 = a^{2s} = a^{2^m} = 1$ y $a^{k_0}b$ es otra involución, ya que de $bab^{-1} = a^t$ y $t \equiv 1 + 2^{m-1} \pmod{2^m}$ se sigue que $b \notin \langle a \rangle$. Supongamos ahora que $t \equiv -1 + 2^{m-1} \pmod{2^m}$. En ese caso $(a^kb)^2 = a^{2^r s}$, donde

$$s \equiv k2^{m-r-1} + 1 \pmod{2^{m-r}}.$$

Si tomamos k_0 tal que

$$s \equiv k_0 2^{m-r-1} + 1 \equiv 0 \pmod{2^{m-r}},$$

entonces $(a^{k_0}b)^2 = a^{2^r s} = aa^{2^m} = 1$ y $a^{k_0}b$ es otra involución. □

Lema 3.6.6. *Si un p-grupo abeliano tiene un único subgrupo de orden p, entonces es cíclico*

Demostración. Se sigue inmediatamente del teorema de caracterización de grupos abelianos finitos. □

Teorema 3.6.7. *Si G es un p-grupo finito que tiene un único subgrupo de orden p, entonces G es cíclico o $p = 2$ y $G \simeq H_{2^m}$ para algún m.*

Demostración. Probaremos el teorema por inducción en n, donde n es tal que $|G| = p^n$. El resultado es claro cuando $n = 1$. Supongamos ahora que $n > 1$ y que p es impar. Por el Corolario 3.3.3, G tiene un subgrupo H de índice p, que a su vez tiene un único subgrupo de orden p. En consecuencia, por hipótesis inductiva, H es cíclico. Así G es cíclico, ya que en caso contrario, por el item 1) de la Proposición 3.6.2, $G[p]$ es un subgrupo de G que tiene más de un subgrupo de orden p. Supongamos ahora que $p = 2$. Si G es abeliano, entonces por el Lema 3.3.6, G es cíclico. Consecuentemente podemos asumir que G no es abeliano. En particular $n \geq 3$. Escribamos $m = n-2$ y denotemos con H a un subgrupo abeliano maximal de G. Claramente H tiene un único subgrupo de orden 2 y así, por el Lema 3.6.6, $H = \langle a \rangle$. Afirmamos que H es un subgrupo de índice 2 de G. Supongamos por el contrario que $|G/H| \geq 4$. Si G/H no tiene exponente 2, entonces existe $b \in G \setminus H$ tal que $b^2 \notin H$. Consideremos $L = \langle a, b^2 \rangle \subsetneq \langle a, b \rangle \subseteq G$. Por la Proposición 3.3.13, el grupo L no es abeliano. Por lo tanto, debido a la hipótesis inductiva, debe ser isomorfo a $H_{2^{m'}}$, para algún $1 \leq m' < m$. Del Ejemplo 4), que aparece antes del Teorema 1.6.1, se sigue fácilmete que $b^2ab^{-2} = a^{-1}$. Como H es un subgrupo normal de G, existe $i \geq 1$ tal que $b^1ab^{-1} = a^i$ y así,

$$a^{-1} = b^2ab^{-2} = ba^ib^{-1} = (bab^{-1})^i = a^{i^2},$$

de donde $i^2 \equiv -1 \pmod{2^{m'+1}}$. Pero esta igualdad es imposible, ya que claramente no existe si $m' = 1$ y tampoco existe si $m' > 1$, ya que en ese caso, por la proposición 3.6.4, $(\mathbb{Z}/2^{m'+1}\mathbb{Z})^* = \{\pm 5^i : 0 \leq i < m' - 1\}$. En consecuencia el exponente de G/H debe ser 2 y así G/H tiene una copia de $\mathbb{Z}_2 \times \mathbb{Z}_2$. De esto se sigue que existen $b, c \in G \setminus H$, tales que

$$H \subsetneq \langle a, b \rangle \subsetneq G, \quad H \subsetneq \langle a, c \rangle \subsetneq G \quad \text{y} \quad H \subsetneq \langle a, b^{-1}c \rangle \subsetneq G.$$

Nuevamente por la Proposición 3.3.13 ninguno de estos grupos $\langle a, b \rangle$, $\langle a, c \rangle$ y $\langle a, b^{-1}c \rangle$ es abeliano y así todos ellos son isomorfos a $H_{2^{m'}}$, para algún $1 \leq m' < m$. Pero entonces $b^1ab^{-1} = a^{-1} = c^1ac^{-1} = a^{-1}$, de dónde $b^{-1}c \in \mathrm{C}_G(H)$, lo que es absurdo. De todo esto concluímos que el índice de H en G es 2. Tomemos $b \in G \setminus H$. Como $b^2 \in H$ existen $0 \leq r \leq m$ y $1 \leq s < 2^{m-r+1}$ impar, tales que $b^2 = a^{2^r s}$. Reemplazando, si es necesario, a por otro generador de H, podemos suponer que $s = 1$. Además $bab^{-1} = a^t$, para algún t, ya que H es normal en G. Como G tiene sólo una involución, por el Lema 3.6.5, debe ser $t = \pm 1$. El caso $p = 1$ está descartado, ya que estamos suponiendo que G no es abeliano. Resumiendo $G = \langle a, b \rangle$, donde

$$|a| = 2^{m+1}, \quad b^2 = a^{2^r} \text{ con } 0 \leq r \leq m \quad \text{y} \quad bab^{-1} = a^{-1}.$$

Para terminar la demostración debemos ver que $r = m$. Para ello, observemos que debido a que $a^{2^r} \in \langle b \rangle$, tenemos

$$a^{2^r} = ba^{2^r}b{-}1 = (bab^{-1})^{2^r} = (a^{-1})^{2^r} = a^{-2^r},$$

de dónde $2^r \equiv -2^r \pmod{2^{m+1}}$, lo que implica que $r = m$. □

4.El teorema de Jordan-Hölder, Grupos resolubles y nilpotentes

En lo que sigue con los símbolos $H \lhd G$ y $G \rhd H$ vamos a denotar que G es un grupo y que H es un subgrupo normal de G.

4.1.El teorema de Jordan-Hölder. Una *serie normal* de un grupo G es una sucesión de subgrupos

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G,$$

tal que $G_i \neq G_{i+1}$ para todo i. Los *grupos factores* de esta serie normal son los cocientes G_{i+1}/G_i. La *longitud* de la serie normal es la cantidad de grupos factores, o lo que es igual la cantidad de inclusiones. Una serie normal

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd M_m = G$$

es un *refinamiento* de otra $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ si $G_0, G_1, \ldots, G_n$ es una subsucesión de $H_0, H_1, \ldots, H_m$. Decimos que dos series normales de un grupo G son *equivalentes* si tienen los mismos grupos factores (no necesariamente en el mismo orden) y cada uno de ellos aparece la misma cantidad de veces en ambas.

Una serie normal de un grupo G es una *serie de composición* si cada uno de sus grupos factores es simple. Claramente cada grupo finito tiene una serie de composición.

Lema 4.1.1. *Si $A \lhd A'$ y $B \lhd B'$ son cuatro subgrupos de un grupo G, entonces*

$$A(A' \cap B) \lhd A(A' \cap B'), \quad (A \cap B')(A' \cap B) \lhd A' \cap B', \quad B(B' \cap A) \lhd B(B' \cap A'),$$

y hay isomorfismos

$$\frac{A(A' \cap B')}{A(A' \cap B)} \simeq \frac{A' \cap B'}{(A \cap B')(A' \cap B)} \simeq \frac{B(B' \cap A')}{B(B' \cap A)}.$$

Demostración. Escribamos $K = A(A' \cap B)$ y $L = A' \cap B'$. Como $A \lhd A'$, sabemos que K es un subgrupo de G. Además, $L \subseteq \mathrm{N}_G(K)$ y así, KL es un subgrupo de G, $(L \cap K) \lhd L$, $K \lhd KL$ y hay un isomorfismo $L/(L \cap K) \simeq KL/K$. Dado que claramente $KL = A(A' \cap B')$ y, por el item 1) de la Proposición 1.6.7, $L \cap K = (A \cap B')(A' \cap B)$ esto prueba que $(A \cap B')(A' \cap B) \lhd A' \cap B'$, $A(A' \cap B) \lhd A(A' \cap B')$ y vale el primer isomorfismo. El resto sale por simetría. □

Teorema 4.1.2 (Schreier). *Dos series normales de un grupo G tienen refinamientos equivalentes.*

Demostración. Supongamos que

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_m = G \quad \text{y} \quad \{1\} = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_n = G$$

son dos series normales de G. Escribamos

$$G_{ij} = G_{j-1}(H_i \cap G_j) \quad \text{para } 0 \leq i \leq n,\ 1 \leq j \leq m,$$

y

$$H_{ij} = H_{i-1}(H_i \cap G_j) \quad \text{para } 1 \leq i \leq n,\ 0 \leq j \leq m.$$

Por el Lema 4.1.1 tenemos las series normales

$$H_0 = H_{10} \lhd H_{11} \lhd \cdots \lhd H_{1m} = H_1 = H_{20} \lhd \cdots \lhd H_{nm} = H_n$$

y

$$G_0 = G_{01} \lhd G_{11} \lhd \cdots \lhd G_{n1} = G_1 = G_{02} \lhd \cdots \lhd G_{nm} = G_n,$$

donde no necesariamente las inclusiones son propias y

$$\frac{G_{ij}}{G_{i-1,j}} = \frac{G_{j-1}(H_i \cap G_j)}{G_{j-1}(H_{i-1} \cap G_j)} \simeq \frac{H_{i-1}(H_i \cap G_j)}{H_{i-1}(H_i \cap G_{j-1})} = \frac{H_{ij}}{H_{i,j-1}},$$

para todo $1 \leq i \leq n$ y $1 \leq j \leq m$. □

Teorema 4.1.3 (Jordan-Hölder). *Si un grupo G tiene una serie de composición, entonces todo serie normal de G tiene un refinamiento que es una serie de composición. Además, dos series de composición de G son equivalentes y por lo tanto tienen la misma longitud.*

Demostración. Es consecuencia inmediata del Teorema 4.1.2. □

A los grupos factores de una serie de composición de un grupo G se los denomina *factores de composición* de G. La *longitud* $l(G)$ de un grupo G es

$$l(G) = \begin{cases} n & \text{si } G \text{ tiene una serie de composición de longitud } n, \\ \infty & \text{en otro caso.} \end{cases}$$

Notemos que $l(\{1\}) = 0$.

Teorema 4.1.4. *Supongamos que H es un subgrupo normal de un grupo G. Entonces G tiene una serie de composición si y sólo si H y G/H la tienen y además $l(G) = l(H) + l(G/H)$.*

Demostración. Si G tiene una serie de composición, entonces por el Teorema 4.1.3 la serie normal $\{1\} \lhd H \lhd G$ se puede refinar a una serie de composición. De este hecho se sigue facilmente que H y G/H también tienen series de composición y $l(G) = l(H) + l(G/H)$. Que si H y G/H tienen series de composición, entonces G también la tiene es todavía más facil. □

Teorema 4.1.5 (de la dimensión). *Supongamos que H y L subgrupos de un grupo G y que H normaliza a L. Entonces $l(H)$ y $l(L)$ son finitos, si y sólo si $l(HL)$ y $l(H \cap L)$ lo son y además $l(HL) + l(H \cap L) = l(H) + l(L)$.*

Demostración. Se lo deduce facilmente aplicando el Teorema 4.1.4 a las sucesiones exactas

$$1 \longrightarrow H \cap L \longrightarrow H \longrightarrow \frac{H}{H \cap L} \longrightarrow 1$$

y

$$1 \longrightarrow L \longrightarrow HL \longrightarrow \frac{HL}{L} \longrightarrow 1,$$

y usando el hecho de que $H/(H \cap L) \simeq HL/L$. □

Observación 4.1.6. *Del teorema de Jorden-Hölder se sigue la parte de la unicidad del teorema fundamental de la aritmética. En efecto si $n = p_1 \dots p_n$ es una factorización de un número natural n y $\langle a \rangle$ es un grupo cíclico de orden n, entonces*

$$\{1\} \lhd \langle a^{p_2 \cdots p_n} \rangle \lhd \langle a^{p_3 \cdots p_n} \rangle \lhd \cdots \lhd \langle a^{p_{n-1} p_n} \rangle \lhd \langle a^{p_n} \rangle \lhd \langle a \rangle$$

es una serie de composición de $\langle a \rangle$. Como los grupos factores de esta serie tienen ordenes $p_1, \dots, p_n$, estos números dependen sólo de n.

4.2.Grupos resolubles. Una *serie resoluble* de un grupo G es una serie normal tal que sus grupos factores son conmutativos. Un grupo G es *resoluble* si tiene una serie resoluble. Claramente que todo grupo abeliano es resoluble. Notemos que un grupo simple es resoluble si y sólo si es isomorfo a $\mathbb{Z}_p$ con p primo y que un grupo resoluble tiene una serie de composición si y sólo si es finito. Esto último se sigue del Teorema 4.1.4 y de que lo mismo vale para grupos abelianos. A continuación damos un ejemplo no trivial de grupo resoluble

Ejemplo. Denotemos con V a un espacio vectorial sobre un cuerpo K. Fijemos una sucesión de subespacios

$$V = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_{n-1} \supsetneq V_n = \{0\}$$

tal que $\operatorname{codim}(V_i) = i$. Escribamos

$$G = \{ f \in \operatorname{End}(V) : f(V_i) \subseteq V_i \text{ para } 0 \leq i \leq n \}.$$

Vamos a ver que G es resoluble. Definimos una sucesión de subgrupos $(B_i)_{0 \leq i \leq n}$ de G poniendo

$$B_i = \{ f \in \operatorname{End}(V) : (f - \mathrm{id})(V_j) \subseteq V_{i+j} \text{ para } 0 \leq j \leq n - i \}.$$

Por ejemplo $B_0 = G$ y $B_n = \{0\}$. Afirmamos que $[B_j, B_k] \subseteq B_{j+k}$ para $0 \leq j, k \leq n$ con $0 \leq j + k \leq n$. En efecto, tomemos $f \in B_j$, $g \in B_k$ y $x \in V_i$. Por definición existen $u_{i+j} \in V_{i+j}$, $v_{i+k} \in V_{i+k}$ y $w_{i+j+k}, w'_{i+j+k} \in V_{i+j+k}$ tales que

$$\begin{aligned} f(x) &= x + u_{i+j}, \qquad & f(v_{i+k}) &= v_{i+k} + w'_{i+j+k}, \\ g(x) &= x + v_{i+k}, \qquad & g(u_{i+j}) &= u_{i+j} + w_{i+j+k}. \end{aligned}$$

Así

$$gf(x) = x + v_{i+k} + u_{i+j} + w_{i+j+k} \quad \text{y} \quad fg(x) = x + u_{i+j} + v_{i+k} + w'_{i+j+k}.$$

Por lo tanto $gf(x) = fg(x) \pmod{V_{i+j+k}}$, de donde

$$gfg^{-1}f^{-1}(x) = x \pmod{V_{i+j+k}}.$$

En particular

1) $[B_0, B_i] \subseteq B_i$ para $0 \leq i \leq n$, de donde cada B_i es normal en $B_0 = G$.
2) $[B_i, B_i] \subseteq B_{2i} \subseteq B_{i+1}$ para $1 \leq i < n$, de donde B_i/B_{i+1} es abeliano para $1 \leq i < n$.

Para terminar la demostración debemos ver que B_0/B_1 es abeliano, lo que se seguirá si probamos que $[B_0, B_0] \subseteq B_1$. Tomemos $f, g \in B_0$ y $x \in V_i \setminus V_{i+1}$. Como $V_i = Kx \oplus V_{i+1}$ y $f(V_i) + g(V_i) \subseteq V_i$ existen $\alpha, \beta \in K$ tal que $f(x) \in \alpha \cdot x + V_{i+1}$ y $g(x) \in \beta \cdot x + V_{i+1}$. Así, dado que además $f(V_{i+1}) + g(V_{i+1}) \subseteq V_{i+1}$, vale que

$$gf(x) \in \alpha \cdot g(x) + g(V_{i+1}) \subseteq \alpha\beta \cdot x + V_{i+1}$$

y similarmente

$$fg(x) \in \beta \cdot f(x) + f(V_{i+1}) \subseteq \beta\alpha \cdot x + V_{i+1}$$

Por lo tanto

$$gfg^{-1}f^{-1}(x) \in \alpha\beta\alpha^{-1}\beta^{-1} \cdot x + V_{i+1} = x + V_{i+1},$$

de donde $[g, f] \in B_1$. □

Teorema 4.2.1. *Cada subgrupo H de un grupo resoluble G es resoluble.*

Demostración. Tomemos una serie resoluble $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ de G y consideremos la serie $\{1\} = H_0 \subseteq H \cap G_1 \subseteq \cdots \subseteq H \cap G_n = H$. Para probar el teorema basta observar que $H \cap G_i \lhd H \cap G_{i+1}$ y

$$\frac{H \cap G_{i+1}}{H \cap G_i} = \frac{H \cap G_{i+1}}{(H \cap G_{i+1}) \cap G_i} \simeq \frac{G_i(H \cap G_{i+1})}{G_i} \subseteq \frac{G_{i+1}}{G_i},$$

para todo i. □

Teorema 4.2.2. *El grupo de permutaciones S_n no es resoluble para ningún $n \geq 5$.*

Demostración. Como el grupo alternado A_n es simple y no conmutativo no es resoluble. Así, por el Teorema 4.2.1, tampoco S_n lo es. □

Teorema 4.2.3. *Si*

$$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{\pi} L \longrightarrow 1$$

es una una sucesión exacta corta de grupos, entonces G es resoluble si y sólo si H y L lo son.

Demostración. Supongamos que G es resoluble. Por el teorema anterior sabemos que H lo es. Para comprobar que también lo es L, basta observar que, para cada serie resoluble $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ de G, tenemos que

$$\{1\} = \pi(G_0) \lhd \pi(G_1) \lhd \cdots \lhd \pi(G_n)$$

y

$$\frac{\pi(G_{i+1})}{\pi(G_i)} \simeq \frac{i(H)G_{i+1}}{i(H)G_i} = \frac{i(H)G_iG_{i+1}}{i(H)G_i} \simeq \frac{G_{i+1}}{i(H)G_i \cap G_{i+1}} \simeq \frac{G_{i+1}/G_i}{(i(H)G_i \cap G_{i+1})/G_i},$$

que es conmutativo. Reciprocamente, si $\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = H$ es una serie resoluble de H y $\{1\} = L_0 \lhd L_1 \lhd \cdots \lhd L_m = L$ es una serie resoluble de L, entonces

$$\{1\} = i(H_0) \lhd i(H_1) \lhd \cdots \lhd i(H_n) = H = \pi^{-1}(L_0) \lhd \pi^{-1}(L_1) \lhd \cdots \lhd \pi^{-1}(L_m) = G$$

es una serie resoluble de G. □

Corolario 4.2.4. *Si H y K son grupos resolubles, entonces también lo es cada producto semidirecto de H con K. En particular los grupos diedrales son resolubles.*

Teorema 4.2.5. *Supongamos que H y L son subgrupos de un grupo G y que H normaliza a L. Entonces H y L son resolubles, si y sólo si HL y $H \cap L$ lo son.*

Demostración. Se lo deduce facilmente aplicando el Teorema 4.2.3 a las sucesiones exactas

$$1 \longrightarrow H \cap L \longrightarrow H \longrightarrow \frac{H}{H \cap L} \longrightarrow 1$$

y

$$1 \longrightarrow L \longrightarrow HL \longrightarrow \frac{HL}{L} \longrightarrow 1,$$

y usando el hecho de que $H/(H \cap L) \simeq HL/L$. □

Observación 4.2.6. *Por el Teorema 4.2.5 todo grupo finito G tiene un máximo subgrupo normal y resoluble H. Además, por el teorema 4.2.3 ningún subgrupo no trivial de G/H es normal y resoluble.*

Definimos la *serie derivada*

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$$

de un grupo G, inductivamente por $G^{(0)} = G$ y $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.

Notemos que en la definición anterior se usa implicitamente el item 4) de la Proposición 1.13.4. En realidad por el item 2) de la misma proposición $G^{(i)}$ es un subgrupo completamente normal de $G^{(j)}$, para cada $i > j \geq 0$. Notemos también que $G^{(i)}/G^{(i+1)}$ es abeliano para todo $i \geq 0$.

Ejemplo 1. Por la Proposición 2.41 y la Observación 2.4.2, la serie derivada de S_n es

$$\mathrm{S}_2 \triangleright \{1\}, \quad \mathrm{S}_3 \triangleright A_3 \triangleright \{1\}, \quad \mathrm{S}_4 \triangleright A_4 \triangleright H \triangleright \{1\} \quad \text{y} \quad \mathrm{S}_n \triangleright A_n \triangleright A_n \triangleright \ldots, \text{ si } n \geq 5,$$

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

Ejemplo 2. Recordemos que D_n es el grupo generado por a, b sujeto a las relaciones $a^n = 1$, $b^2 = 1$ y $bab^{-1}a = 1$, y que H_n es el grupo generado por a, b sujeto a las relaciones $a^n b^{-2} = 1$ y $bab^{-1}a = 1$. Por el ejemplo que precede a la Proposición 1.13.4, las series derivadas de D_n (para $n > 2$) y H_n son

$$D_n \triangleright \langle a^2 \rangle \triangleright \{1\} \qquad \text{y} \qquad H_n \triangleright \langle a^2 \rangle \triangleright \{1\},$$

respectivamente.

Proposición 4.2.7. *Si los grupos factores de una sucesión*

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots$$

son todos conmutativos, entonces $G^{(i)} \subseteq G_i$ *para todo* i.

Demostración. Por inducción en i. El caso $i = 0$ es trivial. Supongamos que el resultado vale para i, de manera de que $G^{(i)} \subseteq G_i$. Dado que G_i/G_{i+1} es comutativo $[G_i, G_i] \subseteq G_{i+1}$ y así $G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G_i, G_i] \subseteq G_{i+1}$. □

Teorema 4.2.8. *Un grupo* G *es resoluble si y sólo si* $G^{(n)} = \{1\}$ *para algún* $n \geq 0$.

Demostración. Si $G^{(n)} = \{1\}$, entonces la serie derivada de G es una serie resoluble. Reciprocamente, si G tiene una serie resoluble $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$, entonces por el teorema anterior, $G^{(n)} \subseteq G_n = \{1\}$. □

Notemos que lo que el teorema anterior dice es que la serie derivada de un grupo G es una serie normal si y sólo si G es resoluble. Al mínimo n tal que $G^{(n)} = \{1\}$ se lo llama la *clase de resolubilidad de* G. Por ejemplo G es abeliano si y sólo su clase de resolubilidad es menor o igual que 1 (el único grupo que tiene clase de resolubilidad 0 es el trivial $\{1\}$). La S_3 de los grupos S_2, A_3, S_3, A_4 y S_4 es 1, 1, 2, 2 y 3 respectivamente. Por otra parte los grupos D_n con $n > 2$ y H_n tiene clase de resolubilidad 2.

Observación 4.2.9. *El Teorema 4.2.8 permite dar demostraciones alternativas de los Teorema 4.2.1 y 4.2.3. Para el primero basta observar que si* H *es un subgrupo de* G, *entonces claramente* $H^{(i)} \subseteq G^{(i)}$ *para todo* $i \geq 0$. *Del item 1) de la Proposición 1.13.4 se sigue por inducción que si* $\pi\colon G \to L$ *es un epimorfismo de grupos, entonces* $L^{(i)} = \pi(G^{(i)})$ *para todo* $i \geq 0$. *La primera parte del Teorema 4.2.3 es consecuencia inmediata de este hecho. Finalmente si* $H^{(m)} = \{1\}$, $L^{(n)} = \{1\}$ *y* G *es una extensión de* H *por* L, *entonces de* $\pi(G^{(n)}) = L^{(n)} = \{1\}$ *se sigue que* $G^{(n)} \subseteq H$ *y así* $G^{(n+m)} = (G^{(n)})^{(m)} \subseteq H^{(m)} = \{1\}$. *Notemos que de esta demostración se sigue que todo subgrupo y todo cociente de un grupo resoluble de clase* n *es resoluble de clase menor o igual que* n *y que si* G *es una extensión de un grupo resoluble* H *por otro* L, *entonces* G *es resoluble de clase menor o igual que la suma de las clases de* H *y* L.

Teorema 4.2.10. *Denotemos con* G *a un grupo arbitrario y con* n *a un número natural. Son equivalentes:*

1) G es resoluble de clase menor o igual que n.

2) Existe una sucesión

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n = \{1\}$$

de subgrupos completamente normales de G tal que G_i/G_{i+1} es abeliano para $0 \leq i < n$.

3) Existe una serie normal

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{n-1} \triangleright G_n = \{1\}$$

tal que G_i/G_{i+1} es abeliano para $0 \leq i < n$.

4) G tiene un subgrupo normal y abeliano H tal que G/H es resoluble de clase menor o igual que $n-1$.

Demostración. 1) $\Rightarrow$ 2). La serie derivada de G satisface lo pedido.

2) $\Rightarrow$ 3). Es trivial.

3) $\Rightarrow$ 1). Esto se sigue inmediatamente de la Proposición 4.2.7.

1) $\Rightarrow$ 4). Tomemos $H = G^{(n-1)}$. Del item 1) de la Proposición 1.13.4 se sigue facilmente que $(G/H)^{(i)} = G^{(i)}/H$ para $0 \leq i < n$. Así G/H es resoluble de clase menor o igual que $n-1$.

4) $\Rightarrow$ 3). Del item 1) de la Proposición 1.13.4 se sigue facilmente que

$$\left(\frac{G}{H}\right)^{(i)} = \frac{G^{(i)}H}{H} \quad \text{para } 0 \leq i < n.$$

En particular $G^{(i+1)}H$ es un subgrupo normal de $G^{(i)}H$ para $0 \leq i < n-1$ y

$$\frac{G^{(i)}H}{G^{(i+1)}H} = \frac{(G/H)^{(i)}}{(G/H)^{(i+1)}}$$

es abeliano para $0 \leq i < n-1$. Además, dado que por hipótesis $(G/H)^{(n-1)} = \{1\}$, también vale que $G^{(n-1)}H = H$. Así

$$G = G^{(0)}H \triangleright G^{(1)}H \triangleright G^{(2)}H \triangleright \cdots \triangleright G^{(n-1)}H \triangleright \{1\}$$

es una serie normal que satisface las condiciones del item 3). □

Ejercicio 24. *Pruebe que si G es un grupo que no es resoluble, entonces G tiene un subgrupo $H \neq \{1\}$ que es normal y satisface $H^{(1)} = H$. Pruebe además que si G es finito también vale la recíproca.*

Una serie *superresoluble* de un grupo G es una cadena

$$\{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_m = G$$

de subgrupos normales de G tal que los grupos factores son cíclicos. Un grupo G es *superresoluble* si tiene una serie superresoluble. Claramente toda serie superresoluble es resoluble y así todo grupo superresoluble es resoluble. No vale la recíproca. Por ejemplo S_4 es resoluble pero no superresoluble. En efecto, supongamos que

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq \mathrm{S}_4$$

es una cadena de subgrupos normales de G tal que los grupos factores son cíclicos. Entonces G_1 no puede ser par ya que entonces contendría una transposición y, por el Teorema 2.1.2, al subgrupo H de S_n formado por todas las transposiciones. Como este grupo no es cíclico esto no es posible. Por lo tanto $G_1 \simeq \mathbb{Z}_3$. Pero entonces G_1 contiene a un 3-ciclo y, por lo tanto, a todos los 3-ciclos, lo que es absurdo ya que hay 8 de ellos.

Teorema 4.2.11. *Vale lo siguiente:*

1) *Cada subgrupo H de un grupo superresoluble G es superresoluble.*
2) *Si $\pi\colon G \to L$ es un epimorfismo y G es superresoluble, entonces L también lo es.*
3) *Supongamos que*

$$1 \longrightarrow H \xrightarrow{\ i\ } G \xrightarrow{\ \pi\ } L \longrightarrow 1$$

es una sucesión exacta corta y que H es un subgrupo característico de G. Si H y L son superresolubles, entonces G también lo es.

Demostración. 1) Tomemos una serie superresoluble $\{1\} = G_0 \subseteq \cdots \subseteq G_n = G$ de G y consideremos la serie $\{1\} = H_0 \subseteq H \cap G_1 \subseteq \cdots \subseteq H \cap G_n = H$. Para probar el teorema basta observar que $H \cap G_i \lhd H \cap G = H$ y

$$\frac{H \cap G_{i+1}}{H \cap G_i} = \frac{H \cap G_{i+1}}{(H \cap G_{i+1}) \cap G_i} \simeq \frac{G_i(H \cap G_{i+1})}{G_i} \subseteq \frac{G_{i+1}}{G_i},$$

para todo i.

2) Basta observar que, para cada serie superresoluble $\{1\} = G_0 \subseteq \cdots \subseteq G_n = G$ de G, la cadena $\{1\} = \pi(G_0) \subseteq \pi(G_1) \subseteq \cdots \subseteq \pi(G_n) = L$ es una serie superresoluble de L ya que

$$\frac{\pi(G_{i+1})}{\pi(G_i)} \simeq \frac{HG_{i+1}}{HG_i} = \frac{HG_iG_{i+1}}{HG_i} \simeq \frac{G_{i+1}}{HG_i \cap G_{i+1}} \simeq \frac{G_{i+1}/G_i}{(HG_i \cap G_{i+1})/G_i},$$

donde H denota a el núcleo de π.

3) Si $\{1\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = H$ es una serie superresoluble de H y $\{1\} = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = L$ es una serie superresoluble de L, entonces, por la Observación 1.13.2,

$$\{1\} = i(H_0) \subseteq \cdots \subseteq i(H_n) = H = \pi^{-1}(L_0) \subseteq \pi^{-1}(L_1) \subseteq \cdots \subseteq \pi^{-1}(L_m) = G$$

es una serie superresoluble de G. □

4.3.Grupos nilpotentes. Definimos la *serie central descendente*

$$G = G^1 \triangleright G^2 \triangleright G^3 \triangleright \cdots$$

de un grupo G, inductivamente por $G^1 = G$ y $G^{i+1} = [G, G^i]$.

Notemos que en la definición anterior se usa implicitamente el item 4) de la Proposición 1.13.4. En realidad por el item 2) de la misma proposición G^i es un subgrupo completamente normal de G^j, para cada $i > j \geq 1$. Notemos también que, por la Observación 1.13.5, vale que $G^i/G^{i+1} \subseteq \mathrm{Z}(G/G^{i+1})$ para todo $i \geq 1$. Decimos que G es nilpotente si existe $n+1$ tal que $G^{n+1} = \{1\}$. Al mínimo n que satisface esta igualdad se lo denomina la *clase de nilpotencia de G*. Por ejemplo G es abeliano si y sólo su clase de nilpotencia es menor o igual que 1 (el único grupo que tiene clase de resolubilidad 0 es el trivial $\{1\}$). Un argumento inductivo simple muestra que $G^{(i)} \subseteq G^{i+1}$ para todo $i \geq 0$, de manera de que todo grupo nilpotente es resoluble.

Proposición 4.3.1. *La clase de grupos nilpotentes es cerrada para las operaciones de tomar subgrupos, cocientes y productos directos finitos.*

Demostración. Denotemos con H a un subgrupo de un grupo G. Un argumento inductivo simple muestra que $H^i \subseteq G^i$ para todo $i \geq 0$. De esto se sigue que si G es nilpotente, entonces H también lo es. Consideremos ahora un epimorfismo de grupos $\pi\colon G \to L$. Del item 1) de la Proposición 1.13.4 se sigue por inducción en que $L^i = \pi(G^i)$ para todo $i \geq 1$. Así, si G es nilpotente, entonces H también to es. Por último es fácil ver por inducción que para cada par H y L de grupos vale que $(H \times L)^i = H^i \times L^i$ para todo $i \geq 1$. Es claro ahora que si H y L son nilpotentes, entonces $H \times L$ también lo es.

Observación 4.3.2. *De la demostración anterior se sigue que las clases de nilpotencia de un subgrupo y de un cociente de un grupo son menores o igual que la del grupo, y que la clase de nilpotencia de en producto de dos grupos nilpotentes es igual al supremo de las clases de nilpotencia de sus factores.*

Una sucesión

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots$$

de subgrupos de un grupo G es *central* si $G_i/G_{i+1} \subseteq \mathrm{Z}(G/G_{i+1})$ para todo $i \geq 0$.

Proposición 4.3.3. *Si*

$$G = G_1 \triangleright G_2 \triangleright G_3 \triangleright \cdots$$

es una sucesión central de subgrupos de G, entonces $G^i \subseteq G_i$ para todo $i \geq 0$.

Demostración. Por inducción en i. El caso $i = 0$ es trivial. Supongamos que el resultado vale para i, de manera de que $G^i \subseteq G_i$. Como $G_i/G_{i+1} \subseteq \mathrm{Z}(G/G_{i+1})$ de la Observación 1.13.5 se sigue que $[G, G_i] \subseteq G_{i+1}$ y, en consecuencia,

$$G^{(i+1)} = [G, G^{(i)}] \subseteq [G, G_i] \subseteq G_{i+1}.$$

como afirmabamos. □

Teorema 4.3.4. *Denotemos con G a un grupo arbitrario y con n a un número natural. Son equivalentes:*

1) G es nilpotente de clase menor o igual que n.

2) Existe una sucesión

$$G = G_1 \supseteq G_2 \supseteq G_3 \supseteq \cdots \supseteq G_n \supseteq G_{n+1} = \{1\}$$

de subgrupos completamente normales de G tal que $G_i/G_{i+1} \subseteq \mathrm{Z}(G/G_{i+1})$ para $0 < i \leq n$.

3) Existe una serie normal

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{n-1} \triangleright G_n = \{1\}$$

que es central.

4) G tiene un subgrupo $H \subseteq \mathrm{Z}(G)$ (por lo tanto característico) tal que G/H es nilpotente de clase menor o igual que $n - 1$.

5) G tiene un subgrupo L que contiene a $[G, G]$ y que es nilpotente de clase menor o igual que $n - 1$.

Demostración. 1) $\Rightarrow$ 2). La serie central descendente de G satisface lo pedido.

2) $\Rightarrow$ 3). Es trivial.

3) $\Rightarrow$ 1). Esto se sigue inmediatamente de la Proposición 4.3.3.

1) $\Rightarrow$ 4). Tomemos $H = G^n$. Del item 1) de la Proposición 1.13.4 se sigue facilmente que $(G/H)^i = G^i/H$ para $1 \leq i \leq n$. Así G/H es nilpotente de clase menor o igual que $n-1$.

4) $\Rightarrow$ 3). Del item 1) de la Proposición 1.13.4 se sigue facilmente que

$$\left(\frac{G}{H}\right)^i = \frac{G^i H}{H} \quad \text{para } 1 \leq i \leq n.$$

En particular $G^{i+1}H$ es un subgrupo normal de G^iH para $1 \leq i < n$. Además

$$\frac{G^iH}{G^{i+1}H} \subseteq \mathrm{Z}\left(\frac{G}{G^{i+1}H}\right) \quad \text{ya que} \quad \frac{G^i}{G^{i+1}} \subseteq \mathrm{Z}\left(\frac{G}{G^{i+1}}\right).$$

Por último, dado que por hipótesis $(G/H)^n = \{1\}$, también vale que $G^nH = H$, y así

$$G = G^1H \triangleright G^2H \triangleright G^3H \triangleright \cdots \triangleright G^nH \triangleright \{1\},$$

satisface las condiciones del item 3).

1) $\Rightarrow$ 5). Basta tomar $L = [G, G]$.

5) $\Rightarrow$ 1). Por la Observación 4.3.2, $G^2 = [G, G] \subseteq L$ es nilpotente de clase menor o igual que $n-1$. Así, claramente G es nilpotente de clase menor o igual que n. $\square$

A continuación veremos que $[G^i, G^j] \subseteq G^{i+j}$ para todo $i, j \geq 1$. Para ello daremos dos versiones de un lema conocido como lema de los tres subgrupos. Cualquiera de estas versiones sirve para nuestros propositos.

Lema 4.3.5. *(de los tres subgrupos) Supongamos que K, H, L y G' son subgrupos de un grupo G.*

1) *Si K, H y L son normales en G y G' contiene a $[K,[H,L]][H,[L,K]]$, entonces también contiene a $[L,[K,H]]$.*
2) *Si G' es normal en G y contiene a $[K,[H,L]][H,[L,K]]$, entonces también contiene a $[L,[K,H]]$.*

Demostración. El item 1) se sigue inmediatamente de identidad de Hall

$$[cac^{-1},[b,c]][bcb^{-1},[a,b]][aba^{-1},[c,a]] = 1,$$

que se demuestra por cálculo directo y el 2) de identidad de Jacobi

$$b[a,[b^{-1},c]]b^{-1}c[b,[c^{-1},a]]c^{-1}a[c,[a^{-1},b]]a^{-1} = 1,$$

que también se demuestra por cálculo directo. $\square$

Proposición 4.3.6. *$[G^i, G^j] \subseteq G^{i+j}$ para todo $i, j \geq 1$.*

Demostración. Lo probamos por inducción en i. El caso $i = 1$ sale por definición y si suponemos que la igualdad vale para i y todo j, entonces

$$[G,[G^i,G^j]] \subseteq [G,G^{i+j}] = G^{i+j+1} \quad \text{y} \quad [G^i,[G^j,G]] = [G^i,G^{j+1}] \subseteq G^{i+j+1},$$

de donde, por el lema anterior, $[G^{i+1},G^j] = [[G,G^i],G^j] = [G^j,[G,G^i]]$ está incluído en G^{i+j+1}. $\square$

Corolario 4.3.7. *$G^{(i)} \subseteq G^{2^i}$ para todo $i \geq 0$.*

Demostración. Lo probamos por inducción en i. El caso $i = 0$ es trivial y si suponemos que vale para i, entonces por la Proposición 4.3.6,

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [G^{2^i}, G^{2^i}] \subseteq G^{2^{i+1}},$$

como queríamos. □

Se define la *serie central ascendente* de un grupo G

$$\{1\} = \mathrm{Z}_0(G) \subseteq \mathrm{Z}_1(G) \subseteq \mathrm{Z}_2(G) \subseteq \ldots,$$

recursivamente por $\mathrm{Z}_0(G) = \{1\}$ y $\mathrm{Z}_{n+1}(G)$ el único subgrupo de G que contiene a $\mathrm{Z}_n(G)$ y tal que $\mathrm{Z}_{n+1}(G)/\mathrm{Z}_n(G)$ es el centro de $G/\mathrm{Z}_n(G)$.

Una sucesión

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \ldots$$

de subgrupos de un grupo G es *central* si $G_{i+1}/G_i \subseteq \mathrm{Z}(G/G_i)$ para todo $i \geq 0$.

Proposición 4.3.8. *Si*

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \ldots$$

es una sucesión central de subgrupos de G, entonces $G_i \subseteq \mathrm{Z}_i(G)$ para todo $i \geq 0$.

Demostración. Por inducción en i. El caso $i = 0$ es trivial. Supongamos que el resultado vale para i. Como $G_{i+1}/G_i \subseteq \mathrm{Z}(G/G_i)$ se sigue de la inclusión $G_i \subseteq \mathrm{Z}_i(G)$ que

$$\frac{G_{i+1}\,\mathrm{Z}_i(G)}{\mathrm{Z}_i(G)} \subseteq Z\left(\frac{G}{\mathrm{Z}_i(G)}\right) = \frac{Z_{i+1}(G)}{Z_i(G)},$$

de donde, $G_{i+1} \subseteq G_{i+1}\,\mathrm{Z}_i(G) \subseteq Z_{i+1}(G)$. □

Teorema 4.3.9. *Para cada grupo G vale que $G^{n+1} = \{1\}$ si y sólo si $\mathrm{Z}_n(G) = G$. Además, en este caso $G^{i+1} \subseteq Z_{n-i}(G)$ para todo $0 \leq i \leq n$.*

Demostración. Supongamos que $\mathrm{Z}_n(G) = G$. Por la Proposición 4.3.3,

$$G^{i+1} \subseteq Z_{n-i}(G) \qquad \text{para } 0 \leq i \leq n.$$

En particular $G^{n+1} \subseteq Z_0(G) = \{1\}$. Supongamos ahora que $G^{n+1} = \{1\}$. Por la Proposición 4.3.8,

$$G^{i+1} \subseteq Z_{n-i}(G) \qquad \text{para } 0 \leq i \leq n.$$

En particular $G = G^1 \subseteq Z_n(G)$. □

Proposición 4.3.10. *Si $H \neq \{1\}$ es un subgrupo normal de un grupo nilpotente G, entonces $H \cap \mathrm{Z}(G) \neq \{1\}$.*

Demostración. Denotemos con i al mínimo número natural tal que $H \cap \mathrm{Z}_i(G) \neq \{1\}$. Como H es normal

$$[G, H \cap \mathrm{Z}_i(G)] \subseteq H \cap [G, \mathrm{Z}_i(G)] \subseteq H \cap \mathrm{Z}_{i+1}(G) = \{1\},$$

de dónde $H \cap \mathrm{Z}_i(G) \subseteq \mathrm{Z}(G)$. □

Proposición 4.3.11. *Si H es un subgrupo abeliano y normal maximal de un grupo nilpotente G, entonces $H = \mathrm{C}_G(H)$.*

Demostración. Como H es conmutativo, claramente $H \subseteq \mathrm{C}_G(H)$. Veamos la inclusión recíproca. Por el apartado que sigue a la Observación 1.13.6, el centro $\mathrm{C}_G(H)$ de H en G es un subgrupo normal de $\mathrm{N}_G(H)$. Como $H \subseteq G$ es normal, $\mathrm{N}_G(H) = G$ y así $\mathrm{C}_G(H)$ es un subgrupo normal de G. En consecuencia $\mathrm{C}_G(H)/H$ es un subgrupo normal del grupo nilpotente G/H. Por la Proposición 4.3.10, si $H \subsetneq \mathrm{C}_G(H)$, entonces existe $a \in \mathrm{C}_G(H) \setminus H$ tal que su clase en G/H pertenece a $\mathrm{Z}(G/H)$, de lo cual se sigue facilmente que $\langle H, a\rangle$ es un subgrupo normal y abeliano de G. □

Teorema 4.3.12. *Todo subgrupo propio de un grupo nilpotente está incluído propiamente en su normalizador.*

Demostración. Tomemos un subgrupo H de un grupo nilpotente G y consideremos la serie central ascendente

$$\{1\} = \mathrm{Z}_0(G) \subsetneq \mathrm{Z}_1(G) \subsetneq \cdots \subsetneq \mathrm{Z}_n(G) = G,$$

de G. Afirmamos que si i es el máximo índice tal que $\mathrm{Z}_i(G) \subseteq H$, entonces $\mathrm{Z}_{i+1}(G) \subseteq \mathrm{N}_G(H)$. En efecto, dado que $\mathrm{Z}_{i+1}(G)/\mathrm{Z}_i(G)$ es el centro de $G/\mathrm{Z}_i(G)$, para todo $x \in \mathrm{Z}_{i+1}(G)$, vale que

$$\overline{x}\frac{H}{\mathrm{Z}_i(G)}\overline{x}^{-1} = \frac{H}{\mathrm{Z}_i(G)},$$

donde $\overline{x}$ denota a la clase de x en $G/\mathrm{Z}_i(G)$. Así $xHx^{-1} = H$. □

Corolario 4.3.13. *Supongamos que G es un grupo nilpotente finito. Entonces vale lo siguiente:*

1) *Para todo subgrupo propio H de G existe una cadena*

$$H = G_1 \lhd G_2 \lhd \cdots \lhd G_m = G$$

de subgrupos de G tales que $|G_{i+1} : G_i|$ es primo para $1 \leq i < m$.

2) *Todo subgrupo propio H de G está incluído en un subgrupo normal L de G tal que $|G : L|$ es primo.*

3) *Todo subgrupo maximal de G es normal y tiene índice primo.*

Demostración. 1) Lo demostraremos por inducción en $|G : H|$. Si existe un subgrupo propio L de G que contiene propiamente a H, entonces por la hipótesis inductiva existen cadenas

$$H = G_1 \lhd G_2 \lhd \cdots \lhd G_i = L \quad \text{y} \quad L = G_i \lhd G_2 \lhd \cdots \lhd G_m = G$$

tales que $|G_{i+1} : G_i|$ es primo para $1 \leq i < m$, de donde el resultado se sigue inmediatamente. En caso contrario por el Teorema 4.3.12 sabemos que $\mathrm{N}_G(H) = G$. Así H es un subgrupo normal de G y el resultado se sigue de que G es resoluble, del Teorema 4.1.3 y del hecho de que cada factor de composición de un grupo resoluble es isomorfo a un $\mathbb{Z}_p$ con p primo.

2) Es consecuencia inmediata del item 1).

3) Es consecuencia inmediata dei item 2). □

Proposición 4.3.14. *Todo p-grupo finito es nilpotente.*

Demostración. Supongamos que P es un grupo de orden p^r y que el resultado vale para grupos de orden p^k con $k < r$. Entonces la serie central ascendente de $P/\operatorname{Z}(P)$ es

$$\frac{\operatorname{Z}_1(P)}{\operatorname{Z}_1(P)} \subsetneq \frac{\operatorname{Z}_2(P)}{\operatorname{Z}_1(P)} \subsetneq \cdots \subsetneq \frac{\operatorname{Z}_n(P)}{\operatorname{Z}_1(P)} = \frac{P}{\operatorname{Z}_1(P)}.$$

En consecuencia

$$\{1\} = \operatorname{Z}_0(P) \subsetneq \operatorname{Z}_1(P) \subsetneq \cdots \subsetneq \operatorname{Z}_n(P) = P,$$

es la serie central ascendente de P. □

Teorema 4.3.15. *Denotemos con G a un grupo finito. Son equivalentes:*

1) *G es un producto directo de p-grupos.*
2) *G es nilpotente.*
3) *Todo subgrupo propio de G está incluído propiamente en su normalizador.*
4) *Todo subgrupo maximal de G es normal.*
5) *Todos los subgrupos de Sylow de G son normales.*
6) *G es el producto directo de sus subgrupos de Sylow.*
7) *Dos elementos de G de ordenes coprimos entre si conmutan.*
8) *Si P es un p-subgrupo de Sylow de G y $q \neq p$ es un primo que divide a $|G|$, entonces existe un q-subgrupo de Sylow de G que normaliza a P.*

Demostración. 1) ⇒ 2). Se sigue inmediatamente de la Proposiciones 4.3.1 y 4.3.14.

2) ⇒ 3). Es consecuencia inmediata del Teorema 4.3.12.

3) ⇒ 4). Es trivial.

4) ⇒ 5). Denotemos con P un subgrupo de Sylow de G. Si P no fuera normal, entonces $\operatorname{N}_G(P)$ estaría incuído en un subgrupo maximal H de G. Por el Corolario 3.2.12, sabemos que $\operatorname{N}_G(H) = H$, lo que contradice la hipótesis.

5) ⇒ 6). Se sigue inmediatamente del Corolario 1.14.11.

6) ⇒ 1). Es trivial.

1) ⇒ 7). Es trivial.

7) ⇒ 8). Es trivial.

8) ⇒ 5). Tomemos un subgrupo de Sylow P de G. Claramente $P \subseteq \operatorname{N}_G(P)$ y por hipótesis para cada primo $q \neq p$ que divide a G hay un q-subgrupo de Sylow de G que está incluído en $\operatorname{N}_G(P)$. Así de la Proposición 3.2.7 se sigue que $\operatorname{N}_G(P) = G$. □

Un hecho trivial es que un grupo es conmutativo si y sólo si todos los subgrupos suyos, que están generados por dos elementos, lo son. Algo similar vale para los grupos nilpotente. En efecto, tenemos la siguiente proposición.

Proposición 4.3.16. *Un grupo finito es nilpotente si y sólo si todo subgrupo suyo generado por dos elementos, lo es.*

Demostración. Por la Proposición 4.3.1 si un grupo finito es nilpotente, entonces todos sus subgrupos generados por dos elementos, también lo son. La recíproca se sigue facilmente de la equivalencia entre los items 2) y 7) del Teorema 4.3.15. □

Teorema 4.3.17. *Cada grupo finito G contiene un máximo subgrupo normal nilpotente $\mathcal{F}(G)$. Además $\mathcal{F}(G)$ es un subgrupo característico de G.*

Demostración. Para ver lo primero es suficiente probar que si H y L son subgrupos normales y nilpotentes de G, entonces HL también lo es. De la Observación 1.6.13 se sigue que HL es normal en G. Consideremos el conjunto $p_1, \ldots, p_n$ de los primos positivos que dividen a $|H||L|$ y escribamos

$$P_i = \begin{cases} \text{El } p_i\text{-subgrupo de Sylow de } H & \text{si } p_i \text{ divide a } |H|, \\ \{1\} & \text{si } p_i \text{ no divide a } |H|. \end{cases}$$

y

$$Q_i = \begin{cases} \text{El } p_i\text{-subgrupo de Sylow de } L & \text{si } p_i \text{ divide a } |L|, \\ \{1\} & \text{si } p_i \text{ no divide a } |L|. \end{cases}$$

Por el Teorema 4.3.15 y la Proposición 3.2.11, los P_i y los Q_i son subgrupos normales de G. Así

$$HL = P_1 \ldots P_n Q_1 \ldots Q_n = P_1 Q_1 \ldots P_n Q_n.$$

Como $|P_iQ_i|$ es una potencia de p_i cada $|P_iQ_i|$ es coprimo con $|P_jQ_j|$ para $j \neq i$. Además por la Observación 1.6.13 los P_iQ_i's son subgrupos normales de G y por lo tanto también de HL. En consecuencia, por el Corolario 1.14.11

$$HL \simeq P_1Q_1 \times \cdots \times P_nQ_n,$$

de donde, por el Teorema 4.3.15, HL es nilpotente. Que $\mathcal{F}(G)$ es característico se sigue de la definición de $cf(G)$ y de que por la Proposioción 4.3.1, el subgrupo normal $f(\mathcal{F}(G))$ de G, es nilpotente, para cada automorfismo f de G. □

Al subgrupo $\mathcal{F}(G)$ de G se lo llama el subgrupo *de Fitting de* G.

Proposición 4.3.18. *Si $[G, G] = G$, entonces $\mathrm{Z}_2(G) = \mathrm{Z}_1(G)$.*

Demostración. Por el Lema 4.3.5, aplicado a $K = H = G$ y $L = \mathrm{Z}_2(G)$,

$$[\mathrm{Z}_2(G), [G, G]] \subseteq [G, [\mathrm{Z}_2(G), G]][G, [G, \mathrm{Z}_2(G)]] = [G, [G, \mathrm{Z}_2(G)]].$$

Dado que la hipótesis $[G, G] = G$ y por la Observación 1.13.5,

$$[G, [G, \mathrm{Z}_2(G)]] \subseteq [G, \mathrm{Z}_1(G)] \subseteq \{1\},$$

obtenemos que $[G, \mathrm{Z}_2(G)] = \{1\}$, de donde $\mathrm{Z}_2(G) = \mathrm{Z}_1(G)$. □

4.4.El subgrupo de Frattini. El *subgrupo de Frattini* $\Phi(G)$, de un grupo G, es la intersección de todos los subgrupos maximales de G. Claramente $\Phi(G)$ es un subgrupo característico de G. Es claro también que si $H \subseteq \Phi(G)$ es un subgrupo normal de G, entonces $\Phi(G) = \pi^{-1}(\Phi(G/H))$, donde $\pi\colon G \to G/H$ es la aplicación canónica.

Teorema 4.4.1. *Si para un subgrupo H de un grupo finito G se satisface $H\Phi(G) = G$, entonces $H = G$. En consecuencia la imagen de un subconjunto S de G en $G/\Phi(G)$ genera $G/\Phi(G)$ si y sólo si S genera G.*

Demostración. Si $H \neq G$, entonces existe un subgrupo maximal L de G que contiene a H. Como por definición $\Phi(G) \subseteq L$, tenemos que $H\Phi(G) \subseteq L$. □

Teorema 4.4.2. *Si G es un p-grupo finito, entonces vale lo siguiente:*

1) $\Phi(G) = [G,G]\langle G^p\rangle$, donde $G^p = \{x^p : x \in G\}$.

2) $\Phi(G)$ es el mínimo subgrupo normal H de G tal que G/H es un $\mathbb{Z}/p\mathbb{Z}$-espacio vectorial.

Demostración. 1) Por la Observación 3.3.8, cada subgrupo maximal H de G es normal y tiene índice p. En consecuencia G/H es abeliano y tiene exponente p, de donde $[G,G] \subseteq H$, y así $G^p \subseteq H$ y $[G,G]\langle G^p\rangle \subseteq \Phi(G)$. Para la inclusión recíproca notemos que $[G,G]\langle G^p\rangle$ es un subgrupo normal de G (en realidad es completamente normal) y que $G/[G,G]\langle G^p\rangle$ es un grupo abeliano de exponente p y, por lo tanto, un $\mathbb{Z}/p\mathbb{Z}$-espacio vectorial. De esto se sigue facilmente que $\Phi(G/[G,G]\langle G^p\rangle) = \{1\}$, lo que implica que $\Phi(G) = \pi^{-1}(\{1\}) = [G,G]\langle G^p\rangle$, donde $\pi\colon G \to G/[G,G]\langle G^p\rangle$ es la aplicación canónica.

2) Claramente G/H es un $\mathbb{Z}/p\mathbb{Z}$-espacio vectorial si y sólo si es abeliano y tiene exponente p, lo que es claramente equivalente a que $[G,G] \subseteq H$ y $G^p \subseteq H$. □

Un subconjunto S de un grupo G es un conjunto *minimal de generadores* de G si $\langle Srangle = G$ y ningún subconjunto propio de S genera a G. Se sigue del Teorema 4.4.1 que S es un conjunto minimal de generadores de G si y sólo si su imagen $\overline{S}$ en $G/\Phi(G)$ es un conjunto minimal de generadores de $G/\Phi(G)$. Por el teorema anterior cuando G es un p-grupo esto equivale a que $\overline{S}$ es una base de $G/\Phi(G)$ como $\mathbb{Z}/p\mathbb{Z}$-espacio vectorial. Así tenemos el siguiente resultado.

Teorema 4.4.3 (Burnside, 1912). *Un subconjunto $\{a_1,\dots,a_n\}$ de un p-grupo finito G es un conjunto minimal de generadores de G si y sólo las imágenes de sus elementos en $G/\Phi(G)$ forman una base de $G/\Phi(G)$ como $\mathbb{Z}/p\mathbb{Z}$-espacio vectorial. En conseccuencia todos los conjuntos minimales de generadores de G tienen el mismo cardinal y este coincide con $\dim_{\mathbb{Z}/p\mathbb{Z}}(G/\Phi(G))$ y cada $a \in G\setminus\Phi(G)$ pertenece a algún conjunto minimal de generadores de G.*

Teorema 4.4.4 (Frattini, 1885). *Si G es finito, entonces $\Phi(G)$ es un subgrupo nilpotente de G.*

Demostración. Por el Teorema 3.4.15, es suficiente demostrar que todos los subgrupos de Sylow de G son normales. Denotemos con P a uno de estos subgrupos. Debido a la Proposición 3.2.11, $G = \Phi(G)\,\mathrm{N}_G(P)$ y así del Teorema 4.4.1 se sigue que P es un subgrupo normal de G y, por lo tanto, también de $\Phi(G)$. □

Teorema 4.4.5 (Gaschütz, 1953). $[G,G] \cap \mathrm{Z}(G) \subseteq \Phi(G)$ *para cada grup G.*

Demostración. Escribamos $H = [G,G] \cap \mathrm{Z}(G)$. Si $H \nsubseteq \Phi(G)$, entonces existe un subgrupo maximal L de G tal que $H \nsubseteq L$ y así $G = HL$. Afirmamos que L es normal en G. En efecto, cada $\in G$ se escribe como $a = bc$ con $b \in H \subseteq \mathrm{Z}(G)$ y $c \in L$. Por lo tanto, $aLa^{-1} = bcLc^{-1}b^{-1} = bLb^{-1} = L$. Como G/L no tiene ningún subgrupo no trivial su orden es primo. En particular G/L es abeliano, lo que implica que $[G,G] \subseteq L$, contradiciendo que $H \nsubseteq L$. □

5. Complementos

5.1. Producto directo de familias arbitrarias de grupos. Si $(G_i)_{i\in I}$ es una familia de grupos, entonces sobre el producto cartesiano $\prod_{i\in I} G_i$ queda definida una estructura de grupo poniendo

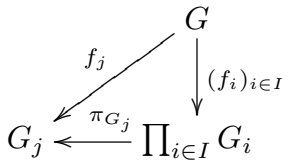
$$(g_i)_{i\in I}(g'_i)_{i\in I} = (g_i g'_i)_{i\in I}$$

Es claro que $(1_{G_i})_{i\in I}$ es el neutro de $\prod_{i\in I} G_i$ y que $(g_i)_{i\in I}^{-1} = (g_i^{-1})_{i\in I}$. Además las aplicaciones canónicas

$$\pi_{G_j}\colon \prod_{i\in I} G_i \to G_j$$

definidas por $\pi_{G_j}((g_i)_{i\in I}) = g_j$ son morfismos de grupos. A $\prod_{i\in I} G_i$, dotado de esta estructura de grupo, lo llamaremos *producto directo* de la familia $(G_i)_{i\in I}$ y a cada uno de los morfismos π_{G_j} lo llamaremos *proyección canónica* de $\prod_{i\in I} G_i$ en G_j. El producto $\prod_{i\in I} G_i$, junto con las proyecciones canónicas π_{G_j}, tiene la siguiente propiedad (que se denomina *propiedad universal del producto directo*):

Si $(f_i\colon G \to G_i)_{i\in I}$ es una familia de morfismos de grupos, entonces existe un único morfismo de grupos $(f_i)_{i\in I}\colon G \to \prod_{i\in I} G_i$ tal que los diagramas



conmutan. Es decir que $\pi_{G_j} \circ (f_i)_{i\in I} = f_j$.

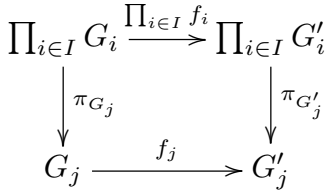
En efecto, estas igualdades fuerzan a que sea $(f_i)_{i\in I}(x) = (f_i(x))_{i\in I}$ y es claro que con esta definición $(f_i)_{i\in I}$ es un morfismo de grupos que satisface las igualdades mencionadas arriba. El claro también que $\operatorname{Ker}((f_i)_{i\in I}) = \bigcap_{i\in I} \operatorname{Ker}(f_i)$.

Notemos que propiedad universal del producto directo dice simplemente que para todo grupo G, la aplicación

$$\Psi\colon \operatorname{Hom}\Big(G, \prod_{i\in I} G_i\Big) \to \prod_{i\in I} \operatorname{Hom}(G, G_i),$$

definida por $\Psi(\varphi) = (\pi_{G_i} \circ \varphi)_{i\in I}$, es biyectiva.

Observación 5.1.1. *Si $(f_i\colon G_i \to G_i')_{i\in I}$ es una familia de morfismos de grupos, entonces por la propiedad universal del producto directo queda definido un único morfismo $\prod_{i\in I} f_i\colon \prod_{i\in I} G_i \to \prod_{i\in I} G_i'$ tal que $\pi_{G_j'} \circ \prod_{i\in I} f_i = f_j \circ \pi_{G_j}$ para todo $j \in I$. Estas igualdades se expresan también diciendo que los cuadrados*



conmutan. Es claro que $\left(\prod_{i\in I} f_i\right)((g_i)_{i\in I}) = (f_i(g_i))_{i\in I}$.

Observación 5.1.2. *Vale lo siguiente:*

1) $\prod_{i\in I} \mathrm{id}_{G_i} = \mathrm{id}_{\prod_{i\in I} G_i}$.
2) *Si $(f_i\colon G_i \to G_i')_{i\in I}$ y $(f_i'\colon G_i' \to G_i'')_{i\in I}$ son familias de morfismos de grupos, entonces $\left(\prod_{i\in I} f_i'\right) \circ \left(\prod_{i\in I} f_i\right) = \prod_{i\in I} (f_i' \circ f_i)$.*

Demostración. Se puede usar la propiedad universal del producto directo, pero también sale por cálculo directo. □

Observación 5.1.3. *Vale que*

$$\operatorname{Ker}\Big(\prod_{i\in I} f_i\Big) = \prod_{i\in I} \operatorname{Ker}(f_i) \quad e \quad \operatorname{Im}\Big(\prod_{i\in I} f_i\Big) = \prod_{i\in I} \operatorname{Im}(f_i).$$

Demostración. Sale por cálculo directo. □

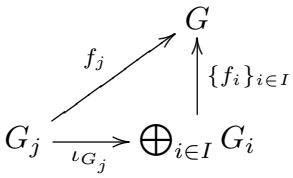
Observación 5.1.4. *Supongamos que $(G_i)_{i\in I}$ es una famila de grupos y que para cada $i \in I$ tenemos un subgrupo normal H_i de G_i. Denotemos con $\pi_i\colon G_i \to G_i/H_i$ a la sobreyección canónica. Por la Observación 5.1.3, el morfismo*

$$\prod_{i\in I} \pi_i\colon \prod_{i\in I} G_i \to \prod_{i\in I} \frac{G_i}{H_i}$$

es sobreyectivo y su núcleo es $\prod_{i\in I} H_i$ y, en consecuencia, induce un isomorfismo

$$\overline{\prod_{i\in I} \pi_i}\colon \frac{\prod_{i\in I} G_i}{\prod_{i\in I} H_i} \to \prod_{i\in I} \frac{G_i}{H_i}.$$

5.2.Suma directa de familias arbitrarias de grupos. Dada una familia de grupos $(G_i)_{i\in I}$, denotamos con $\bigoplus_{i\in I} G_i$ al subgrupo normal de $\prod_{i\in I} G_i$ formado por las familias $(g_i)_{i\in I}$ que satisfacen la propiedad de que el conjunto $\{i \in I : g_i \neq 1\}$ es finito. Al grupo $\bigoplus_{i\in I} G_i$ lo llamaremos *suma directa* de la familia $(G_i)_{i\in I}$. Para cada $j \in I$ hay un morfismo $\iota_{G_j}\colon G_j \to \bigoplus_{i\in I} G_i$, definido por $\iota_{G_j}(g_j) = (g_i')_{i\in I}$, donde $g_j' = g_j$ y $g_i' = 1$ si $i \neq j$. A cada uno de los morfismos ι_{G_j} lo llamaremos la *inyección canónica* de G_j en $\bigoplus_{i\in I} G_i$. La familia $(\iota_{G_j})_{j\in I}$ satisface la propiedad de que $\iota_{G_j}(g)\iota_{G_{j'}}(g') = \iota_{G_{j'}}(g')\iota_{G_j}(g)$ para todo $j, j' \in I$ distintos y todo $g \in G_j$ y $g' \in G_{j'}$. La suma directa $\bigoplus_{i\in I} G_i$, junto con las inyecciones canónicas ι_{G_j}, satisface la siguiente propiedad (que se denomina *propiedad universal de la suma directa*):

> Si $(f_i\colon G_i \to G)_{i\in I}$ es una familia de morfismos de grupos que satisface la propiedad de que $f_i(g)f_{i'}(g') = f_{i'}(g')f_i(g)$ para todo $i \neq i'$ en I y todo $g \in G_i$ y $g' \in G_{i'}$, entonces existe un único morfismo de grupos $\{f_i\}_{i\in I}\colon \bigoplus_{i\in I} G_i \to G$ tal que los diagramas
>
> 
>
>
> conmutan para todo $j \in I$. Es decir que $\{f_i\}_{i\in I} \circ \iota_{G_j} = f_j$.

En efecto, estas igualdades fuerzan a que sea

$$\begin{aligned}\{f_i\}_{i\in I}\big(\iota_{G_{i_1}}(g_{i_1}) \cdots \iota_{G_{i_n}}(g_{i_n})\big) &= \{f_i\}_{i\in I}(\iota_{G_{i_1}}(g_{i_1})) \cdots \{f_i\}_{i\in I}(\iota_{G_{i_n}}(g_{i_n})) \\ &= f_{i_1}(g_{i_1}) \cdots f_{i_n}(g_{i_n}),\end{aligned}$$

donde $i_1, \ldots, i_n$ es una subfamilia arbitraria de elementos de I y g_{i_j} pertenece a G_{i_j} para todo $1 \leq j \leq n$. Veamos que la aplicación $\{f_i\}_{i\in I}$, definida así, es un morfismo

de grupos: Supongamos que $g = \iota_{G_{i_1}}(g_{i_1}) \cdots \iota_{G_{i_n}}(g_{i_n})$ y $g' = \iota_{G_{i_1}}(g'_{i_1}) \cdots \iota_{G_{i_n}}(g'_{i_n})$. Entonces,

$$\begin{aligned}
\{f_i\}_{i\in I}(gg') &= \{f_i\}_{i\in I}\big(\iota_{G_{i_1}}(g_{i_1}g'_{i_1}) \cdots \iota_{G_{i_n}}(g_{i_n}g'_{i_n})\big) \\
&= f_{i_1}(g_{i_1}g'_{i_1}) \cdots f_{i_n}(g_{i_n}g'_{i_n}) \\
&= f_{i_1}(g_{i_1})f_{i_1}(g'_{i_1}) \cdots f_{i_n}(g_{i_n})f_{i_n}(g'_{i_n}) \\
&= f_{i_1}(g_{i_1}) \cdots f_{i_n}(g_{i_n})f_{i_1}(g'_{i_1}) \cdots f_{i_n}(g'_{i_n}) \\
&= \{f_i\}_{i\in I}(g)\{f_i\}_{i\in I}(g').
\end{aligned}$$

Es claro que $\{f_i\}_{i\in I}$ satisface las igualdades mencionadas arriba.

Observación 5.2.1. *Si $(f_i\colon G_i \to G'_i)_{i\in I}$ es una familia de morfismos de grupos, entonces por la propiedad universal de la suma directa queda definido un único morfismo $\bigoplus_{i\in I} f_i\colon \bigoplus_{i\in I} G_i \to \bigoplus_{i\in I} G'_i$ tal que $\big(\bigoplus_{i\in I} f_i\big)\circ\iota_{G_j} = \iota_{G'_j}\circ f_j$ para todo $j \in I$. Estas igualdades se expresan también diciendo que los cuadrados*

$$\begin{array}{ccc}
G_j & \xrightarrow{\quad f_j \quad} & G'_j \\
\Big\downarrow{\scriptstyle \iota_{G_j}} & & \Big\downarrow{\scriptstyle \iota_{G'_j}} \\
\bigoplus_{i\in I} G_i & \xrightarrow{\bigoplus_{i\in I} f_i} & \bigoplus_{i\in I} G'_i
\end{array}$$

conmutan. Es claro que $\big(\bigoplus_{i\in I} f_i\big)\,((g_i)_{i\in I}) = (f_i(g_i))_{i\in I}$.

Observación 5.2.2. *Vale lo siguiente:*

1) $\bigoplus_{i\in I} \mathrm{id}_{G_i} = \mathrm{id}_{\bigoplus_{i\in I} G_i}$.
2) *Si $(f_i\colon G_i \to G'_i)_{i\in I}$ y $(f'_i\colon G'_i \to G''_i)_{i\in I}$ son familias de morfismos de grupos, entonces $\big(\bigoplus_{i\in I} f'_i\big)\circ\big(\bigoplus_{i\in I} f_i\big) = \bigoplus_{i\in I}(f'_i\circ f_i)$.*

Demostración. Se puede usar la propiedad universal de la suma directa, pero también sale por cálculo directo. □

Observación 5.2.3. *Vale que*

$$\mathrm{Ker}\Big(\bigoplus_{i\in I} f_i\Big) = \bigoplus_{i\in I} \mathrm{Ker}(f_i) \quad e \quad \mathrm{Im}\Big(\bigoplus_{i\in I} f_i\Big) = \bigoplus_{i\in I} \mathrm{Im}(f_i).$$

Demostración. Sale por cálculo directo. □

Observación 5.2.4. *Supongamos que $(G_i)_{i\in I}$ es una famila de grupos y que para cada $i \in I$ tenemos un subgrupo normal H_i de G_i. Denotemos con $\pi_i\colon G_i \to G_i/H_i$ a la sobreyección canónica. Por la Observación 5.2.3, el morfismo*

$$\bigoplus_{i\in I} \pi_i\colon \bigoplus_{i\in I} G_i \to \bigoplus_{i\in I} \frac{G_i}{H_i}$$

es sobreyectivo y su núcleo es $\bigoplus_{i\in I} H_i$ y, en consecuencia, induce un isomorfismo

$$\overline{\bigoplus_{i\in I} \pi_i}\colon \frac{\bigoplus_{i\in I} G_i}{\bigoplus_{i\in I} H_i} \to \bigoplus_{i\in I} \frac{G_i}{H_i}.$$

Observación 5.2.5. *Supongamos que $(H_i)_{i\in I}$ es una familia de subgrupos de un grupo G y que los elementos de H_i conmutan con los de $H_{i'}$ para todo $i' \in I \setminus \{i\}$. Por la propiedad universal de la suma directa existe un morfismo $\varphi\colon \bigoplus_{i\in I} H_i \to G$ que está definido por $\varphi((h_i)_{i\in I}) = \prod_{i\in I} h_i$ (donde el producto tomado en G, tiene sentido ya que los h_i son iguales a 1 salvo una cantidad finita de ellos y no importa el orden en que se los multiplican ya que conmutan entre si). Es evidente que la imagen de φ es el conjunto de los elementos de G que se escriben como $h_{i_1}\cdots h_{i_n}$, donde $i_1,\dots,i_n$ es una subfamilia arbitraria de elementos de I y h_{i_j} pertenece a H_{i_j} para todo $1 \le j \le n$. Notemos que cada H_i es normal en la imagen de φ. Esto se sigue facilmente de que los elementos de H_i conmutan con los de $H_{i'}$ para todo $i' \in I \setminus \{i\}$. Además son equivalentes:*

1) *φ es inyectiva.*
2) *Cada elemento de la imagen de φ se escribe de una única manera como un producto $h_{i_1}\cdots h_{i_n}$, donde $i_1,\dots,i_n$ es una subfamilia arbitraria de elementos de I y h_{i_j} pertenece a $H_{i_j}\setminus\{1\}$ para todo $1 \le j \le n$.*
3) *El 1 de G (que claramente está en la imagen de φ) satisface la propiedad mencionada en el item 2)*
4) *Para cada $i \in I$ vale que $H_i \cap \prod_{j\neq i} H_j = \{1\}$, donde $\prod_{j\neq i} H_j$ denota al subgrupo de G consistente de los elementos que se escriben como $h_{i_1}\cdots h_{i_n}$, con $i_1,\dots,i_n$ una subfamilia arbitraria de elementos de $I\setminus\{j\}$ y h_{i_j} pertenece a H_{i_j} para todo $1 \le j \le n$.*

Es claro por definición que los items 1) y 2) son equivalentes y que el 3) es equivalente a que $\ker(\varphi) = \{1\}$. Veamos que 3) implica 4). Si existieran $h_i \neq 1$ en H_i y $h_{i_1} \in H_{i_1},\dots,h_{i_n} \in H_{i_n}$ con $i \notin \{i_1,\dots,i_n\}$ tales que $h_i = h_{i_1}\cdots h_{i_n}$, entonces tendríamos que $1 = h_i^{-1}h_{i_1}\cdots h_{i_n}$, contradiciendo la hipótesis. La demostración de que 4) implica 3) es similar. En efecto, si $1 = h_{i_1}\cdots h_{i_n}$, donde $n \ge 1$ e $i_1,\dots,i_n$ es una subfamilia arbitraria de elementos de I y $h_{i_j} \neq 1$ pertenece a H_{i_j} para todo $1 \le j \le n$, entonces claramente $n \ge 2$ y $h_{i_1}^{-1} = h_{i_2}\cdots h_{i_n}$ está en $H_{i_1} \cap \prod_{j\neq i_1} H_j$. Notemos que si I está totalmente ordenado, entonces el item 4) puede ser reemplazado por el pedido de que para cada $i \in I$ valga $H_i \cap \prod_{j<i} H_j = \{1\}$. Dejamos al lector comprobar esto. Notemos también que si cada H_i es un subgrupo normal de G, entonces de la condición 4) se sigue que $H_i \cap H_{i'} = \{1\}$ para todo $i \neq i'$ en I, lo que por el Teorema 1.14.7 implica que los elementos de H_i conmutan con los de $H_{i'}$ para cada par i, i' de elementos distintos de I. Así, en este caso, esta última condición es redundante.

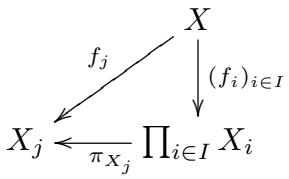
5.3.Producto directo de G-conjuntos. Si $(X_i)_{i\in I}$ es una familia de G-conjuntos, entonces sobre el producto cartesiano $\prod_{i\in I} X_i$ queda definida una estructura de G-conjunto poniendo $g\cdot(x_i)_{i\in I} = (g\cdot x_i)_{i\in I}$. Además las aplicaciones canónicas

$$\pi_{X_j}\colon \prod_{i\in I} X_i \to X_j$$

definidas por $\pi_{X_j}((x_i)_{i\in I}) = x_j$ son morfismos de G-conjuntos. Claramente el núcleo de la acción de G sobre $\prod_{i\in I} X_i$ es la intersección de los núcleos de la acciones de G sobre cada X_i, el estabilizador de $(x_i)_{i\in I}$ es la intesección $\bigcap_{i\in I} G_{x_i}$ de los estabilizadores de cada x_i y $\mathrm{PF}\big(\prod_{i\in I} X_i\big) = \prod_{i\in I} \mathrm{PF}(X_i)$. A $\prod_{i\in I} X_i$, dotado de esta acción, lo llamaremos *producto directo* de la familia $(X_i)_{i\in I}$ y a cada

uno de los morfismos π_{X_j} lo llamaremos *proyección canónica* de $\prod_{i\in I} X_i$ en X_j. El producto $\prod_{i\in I} X_i$, junto con las proyecciones canónicas π_{X_j}, tiene la siguiente propiedad (que se denomina *propiedad universal del producto directo*):

Si $(f_i\colon X \to X_i)_{i\in I}$ es una familia de morfismos de G-conjuntos, entonces existe un único morfismo de G-conjuntos $(f_i)_{i\in I}\colon X \to \prod_{i\in I} X_i$ tal que los diagramas



conmutan. Es decir que $\pi_{X_j}\circ(f_i)_{i\in I} = f_j$.

En efecto, estas igualdades fuerzan a que sea $(f_i)_{i\in I}(x) = (f_i(x))_{i\in I}$ y es claro que con esta definición $(f_i)_{i\in I}$ es un morfismo de G-conjuntos que satisface las igualdades mencionadas arriba.

Notemos que lo que la propiedad universal del producto directo dice es simplemente que para todo G-conjunto X, la aplicación

$$\Psi\colon \operatorname{Hom}_G\Big(X, \prod_{i\in I} X_i\Big) \to \prod_{i\in I} \operatorname{Hom}_G(X, X_i),$$

definida por $\Psi(\varphi) = (\pi_{X_i}\circ\varphi)_{i\in I}$, es biyectiva.

Observación 5.3.1. *Si $(f_i\colon X_i \to X_i')_{i\in I}$ es una familia de morfismos de G-conjuntos, entonces por la propiedad universal del producto directo queda definido un único morfismo $\prod_{i\in I} f_i\colon \prod_{i\in I} X_i \to \prod_{i\in I} X_i'$ tal que $\pi_{X_j'}\circ\prod_{i\in I} f_i = f_j\circ\pi_{X_j}$ para todo $j \in I$. Estas igualdades se expresan también diciendo que los cuadrados*

$$\begin{array}{ccc} \prod_{i\in I} X_i & \xrightarrow{\prod_{i\in I} f_i} & \prod_{i\in I} X_i' \\ \downarrow{\scriptstyle \pi_{X_j}} & & \downarrow{\scriptstyle \pi_{X_j'}} \\ X_j & \xrightarrow{\quad f_j \quad} & X_j' \end{array}$$

conmutan. Es claro que $\big(\prod_{i\in I} f_i\big)\,((x_i)_{i\in I}) = (f_i(x_i))_{i\in I}$.

Observación 5.3.2. *Vale lo siguiente:*

1) $\prod_{i\in I} \mathrm{id}_{X_i} = \mathrm{id}_{\prod_{i\in I} X_i}$.
2) *Si $(f_i\colon X_i \to X_i')_{i\in I}$ y $(f_i'\colon X_i' \to X_i'')_{i\in I}$ son familias de morfismos de G-conjuntos, entonces $\big(\prod_{i\in I} f_i'\big)\circ\big(\prod_{i\in I} f_i\big) = \prod_{i\in I}(f_i'\circ f_i)$.*

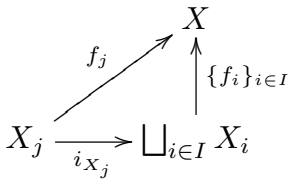
Demostración. Se puede usar la propiedad universal del producto directo, pero también sale por cálculo directo. □

5.4.Unión disjunta o coproducto de G-conjuntos. Si $(X_i)_{i\in I}$ es una familia de G-conjuntos, entonces sobre la unión disjunta $\bigsqcup_{i\in I} X_i$ de los X_i's queda naturalmente definida una única estructura de G-conjunto tal que las inclusiones canónicas

$$i_{X_j}\colon X_j \to \bigsqcup_{i\in I} X_i$$

son morfismos de G-conjuntos. A $\bigsqcup_{i\in I} X_i$, dotado de esta acción, lo llamaremos *unión disjunta* o *coproducto* de la familia $(X_i)_{i\in I}$ y a cada uno de los morfismos i_{X_j} lo llamaremos *inclusión canónica* de X_j en $\bigsqcup_{i\in I} X_i$. El coproducto $\bigsqcup_{i\in I} X_i$, junto con las inclusiones canónicas i_{X_j}, tiene la siguiente propiedad (que se denomina *propiedad universal del coproducto*):

Si $(f_i\colon X_i \to X)_{i\in I}$ es una familia de morfismos de G-conjuntos, entonces existe un único morfismo de G-conjuntos $\{f_i\}_{i\in I}\colon \bigsqcup_{i\in I} X_i \to X$ tal que los diagramas



conmutan. Es decir que $\{f_i\}_{i\in I}\circ i_{X_j} = f_j$.

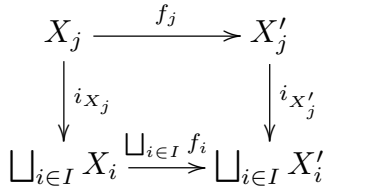
En efecto, estas igualdades fuerzan a que sea $\{f_i\}_{i\in I}(x) = f_i(x)$ para $x \in X_i$ y es claro que con esta definición $\{f_i\}_{i\in I}$ es un morfismo de G-conjuntos que satisface las igualdades mencionadas arriba.

Notemos que lo que la propiedad universal del coproducto dice es simplemente que para todo G-conjunto X, la aplicación

$$\Psi\colon \operatorname{Hom}_G\Big(\bigsqcup_{i\in I} X_i, X\Big) \to \prod_{i\in I} \operatorname{Hom}_G(X_i, X),$$

definida por $\Psi(\varphi) = (\varphi\circ\pi_{X_i})_{i\in I}$, es biyectiva.

Observación 5.4.1. *Si $(f_i\colon X_i \to X_i')_{i\in I}$ es una familia de morfismos de G-conjuntos, entonces por la propiedad universal del coproducto queda definido un único morfismo $\bigsqcup_{i\in I} f_i\colon \bigsqcup_{i\in I} X_i \to \bigsqcup_{i\in I} X_i'$ tal que $\big(\bigsqcup_{i\in I} f_i\big)\circ i_{X_j} = i_{X_j'}\circ f_j$ para todo $j \in I$. Estas igualdades se expresan también diciendo que los cuadrados*



conmutan. Es claro que $\big(\bigsqcup_{i\in I} f_i\big)(x) = f_i(x)$ para todo $x \in X_i$.

Observación 5.4.2. *Vale lo siguiente:*

1) $\bigsqcup_{i\in I} \mathrm{id}_{X_i} = \mathrm{id}_{\bigsqcup_{i\in I} X_i}$.
2) *Si $(f_i\colon X_i \to X_i')_{i\in I}$ y $(f_i'\colon X_i' \to X_i'')_{i\in I}$ son familias de morfismos de G-conjuntos, entonces $\big(\bigsqcup_{i\in I} f_i'\big)\circ\big(\bigsqcup_{i\in I} f_i\big) = \bigsqcup_{i\in I}(f_i'\circ f_i)$.*

Demostración. Se puede usar la propiedad universal del coproducto, pero también sale por cálculo directo. □

5.5.Complementos a los teoremas de Sylow. Dados un subgrupo H de un grupo finito G, un primo p que divide a $|H|$, un p-subgrupo de Sylow P_H de H y un divisor m de $|G|$ tal que $|P_H|$ divide a m, denotemos con $S_m(G, H, P_H)$ al conjunto de los subgrupos Q de orden m de G tales que $Q \cap H = P_H$.

Proposición 5.5.1. *Supongamos que H y H' son subgrupos de un grupo finito G y que p es un primo que divide a $|H| = |H'|$. Denotemos con P_H y con $P_{H'}$ a dos p-subgrupos de Sylow de H y H' respectivamente y con m a un divisor de $|G|$ tal que $|P_H|$ divide a m. Si existe un automorfismo f de G tal que $f(H) = H'$, entonces $\#(S_m(G, H, P_H)) = \#(S_m(G, H', P_{H'}))$.*

Demostración. Claramente $f(P_H)$ es un p-subgrupo de Sylow de H'. Por el item 2) del Teorema 2.2.2, existe un elemento h de H' tal que $hf(P_H)h^{-1} = P_{H'}$. Notemos que si $Q \cap H = P_H$, entonces

$$hf(Q)h^{-1} \cap H' = hf(Q)h^{-1} \cap hf(H)h^{-1} = hf(Q \cap H)h^{-1} = hf(P_H)h^{-1} = P_{H'},$$

de manera de que queda definida una aplicación

$$\theta\colon S_m(G, H, P_H) \to S_m(G, H', P_{H'})$$

poniendo $\theta(Q) = hf(Q)h^{-1}$. Es facil ver que esta aplicación es biyectiva y así $\#(S_m(G, H, P_H)) = \#(S_m(G, H', P_{H'}))$. □

Notemos que la proposición de arriba se aplica en particular cuando H y H' son conjugados y además muestra que $\#(S_m(G, H, P_H))$ no depende del subgrupo de Sylow P_H de H elejido. Así,

$$\#(\{Q \in \mathrm{Sub}(G) : |Q| = m \text{ y } Q \cap H \in \mathrm{Syl}_p(H)\}) = \#(\mathrm{Syl}_p(H))\#(S_m(G, H, P_H)),$$

donde $\mathrm{Sub}(G)$ denota al conjunto de los subgrupos de G. Dado que, por la Observación 2.2.7, vale que si H es normal y si $m = p^r$ donde $r > 0$ es tal que $|G| = p^r n$ con p y n coprimos, entonces

$$\mathrm{Syl}_p(G) = \#(\{Q \in \mathrm{Sub}(G) : |Q| = p^r \text{ y } Q \cap H \in \mathrm{Syl}_p(H)\}),$$

obtenemos así otra demostración de la primera parte de la Proposición 2.2.8.

5.6.Subgrupos normales minimales. Un subgrupo normal H de un grupo G es *normal minimal* si $H \neq \{1\}$ y no existe ningún subgrupo normal N de G tal que $H \subsetneq N \subsetneq G$. Es claro que todo grupo finito tiene subgrupos normales minimales. Vamos a caracterizar estos subgrupos. Para ello conviene estudiar primero los grupos *característicamente simples*, que son por definición los grupos que no tienen subgrupos característicos distintos de $\{1\}$ y G.

Lema 5.6.1. *Si H es un subgrupo normal de un grupo G y $\varphi \in \mathrm{Aut}(G)$, entonces $\varphi(H)$ también es un subgrupo normal de G.*

Demostración. Tomemos $x \in G$. Como φ es sobreyectiva existe $y \in G$ tal que $\varphi(y) = x$ y así, $x\varphi(H)x^{-1} = \varphi(yHy^{-1}) = \varphi(H)$. □

Teorema 5.6.2. *Si un grupo finito es característicamente simple, entonces es un producto directo de grupos simples isomorfos.*

Demostración. Elijamos un subgrupo normal $H \neq \{1\}$ de G con orden mínimo. En particular H es normal minimal. Entre todos los subgrupos de G de la forma $H_1 \times \cdots \times H_m$, con cada H_i normal e isomorfo a H, tomemos uno con m máximo. Afirmamos que $G = H_1 \times \cdots \times H_m$. Como G es característicamente simple, para probar esto será suficiente ver que $\varphi(H_i) \subseteq H_1 \times \cdots \times H_m$ para todo $1 \leq i \leq m$ y todo $\varphi \in \mathrm{Aut}(G)$. Es claro que $\varphi(H_i) \simeq H$ y que, por el Lema 5.6.1, $\varphi(H_i)$ es un subgrupo normal de G. Supongamos que $\varphi(H_i)$ no está incluído en $H_1 \times \cdots \times H_m$. Entonces por la minimalidad de $|H|$, debe ser $\varphi(H_i) \cap (H_1 \times \cdots \times H_m) = \{1\}$, pero esto implica que $\langle H_1 \times \cdots \times H_m, \varphi(H_i)\rangle \simeq H_1 \times \cdots \times H_m \times \varphi(H_i)$, lo que contradice la maximalidad de m. □

Teorema 5.6.3. *Todo subgrupo normal minimal H de un grupo finito G es característicamente simple y, por lo tanto, isomorfo a un producto directo de grupos simples isomorfos.*

Demostración. Se sigue de que, por la Observación 1.13.2, todo un subgrupo característico de H es un subgrupo normal de G. □

Un grupo es *elemental abeliano* si es isomorfo a un producto finito de $\mathbb{Z}_p$ con p-primo. Por los Teoremas 4.2.1 y 5.6.3 todo subgrupo normal minimal de un grupo finito es característicamente simple y resoluble, y por los Teoremas 4.2.1 y 5.6.2, todo grupo finito, característicamente simple y resoluble, es elemental abeliano.

Respuesta a los ejercicios

Ejercicio 1. *Pruebe que son equivalentes:*

1) a es inversible a izquierda y cancelable a derecha,

2) a es inversible a derecha y cancelable a izquierda,

3) a es inversible.

Solución. Es claro que 3) implica 1). Veamos que 1) implica 3). Por hipótesis existe $b \in A$ tal que $ba = 1$. Debemos ver que $ab = 1$, lo que se sigue de que $(ab)a = a(ba) = a1 = a = 1a$ y de que a es cancelable a derecha. La equivalencia entre 2) y 3) es similar a la equivalencia entre 1) y 3). □

Ejercicio 2. *Pruebe que vale lo siguiente:*

1) Si a es inversible, entonces a conmuta con b si y sólo si a^{-1} lo hace.

2) Si a y b conmutan entre si, entonces a^m y b^n también lo hacen, para todo $n, m \geq 0$.

3) Si a y b conmutan entre si, entonces $(ab)^n = a^n b^n$, para todo $n \geq 0$.

4) Si a y b son inversibles y conmutan entre si, entonces $(ab)^n = a^n b^n$, para todo $n \in \mathbb{Z}$.

5) Si a es inversible, entonces $a^{-n} = (a^n)^{-1}$, para todo $n \in \mathbb{Z}$.

6) $a^n a^m = a^{n+m}$, para todo $n, m \geq 0$.

7) Si a es inversible, entonces $a^n a^m = a^{n+m}$, para todo $n, m \in \mathbb{Z}$.

8) $(a^n)^m = a^{nm}$, para todo $n, m \geq 0$.

9) Si a es inversible, entonces $(a^n)^m = a^{nm}$, para todo $n, m \in \mathbb{Z}$.

Solución. 1) En efecto es claro que

$$ab = ba \Leftrightarrow b = a^{-1}ba \Leftrightarrow ba^{-1} = a^{-1}b.$$

como afirmamos.

2) Veamos primero que a^m conmuta con b para todo $m \geq 0$. Para $m = 0$ esto es trivial. Supongamos por hipótesis inductiva que a^m conmuta con b. Entonces,

$$a^{m+1}b = a^m ab = a^m ba = ba^m a = ba^{m+1},$$

y así a^m conmuta con b para todo $m \geq 0$. Ahora fijemos $m \geq 0$ y veamos que a^m conmuta con b^n para todo $n \geq 0$. Esto es trivial cuando $n = 0$. Supongamos por hipótesis inductiva que a^m conmuta con b^n. Entonces,

$$a^m b^{n+1} = a^m b^n b = b^n a^m b = b^n ba^m = b^{n+1}a^n$$

y, por lo tanto, a^m y b^n conmutan entre si para todo $n, m \geq 0$.

3) Para $n = 0$ esto es trivial. Supongamos por hipótesis inductiva que $(ab)^n = a^n b^n$. Entonces,

$$(ab)^{n+1} = (ab)^n ab = a^n b^n ab = a^n ab^n b = a^{n+1} b^{n+1},$$

y así $(ab)^n = a^n b^n$, para todo $n \geq 0$.

4) Ya sabemos que esto es cierto cuando $n \geq 0$. Para $n < 0$ tenemos

$$(ab)^n = ((ab)^{-1})^{-n} = (a^{-1}b^{-1})^{-n} = (a^{-1})^{-n}(b^{-1})^{-n} = a^n b^n.$$

5) Como a y a^{-1} conmutan entre si, $a^n(a^{-1})^n = (aa^{-1})^n = 1^n = 1$.

6) Para $m = 0$ esto es trivial. Supongamos ahora por hipótesis inductiva que $a^{n+m} = a^n a^m$. Entonces,

$$a^n a^{m+1} = a^n a^m a = a^{n+m} a = a^{n+m+1},$$

como dijimos.

7) Ya sabemos que esto vale cuando $n, m \geq 0$. Si $n \geq 0$, $m < 0$ y $n + m \geq 0$, entonces se sigue de que

$$a^n a^m = a^{n+m} \Leftrightarrow a^n = a^{n+m} a^{-m}.$$

Si $n \geq 0$, $m < 0$ y $n + m < 0$, de que

$$a^n a^m = a^{n+m} \Leftrightarrow a^{-(n+m)} a^n = a^{-m}$$

y si $n, m < 0$, de que

$$a^n a^m = a^{n+m} \Leftrightarrow a^{-(n+m)} = a^{-m} a^{-n}.$$

8) Para $m = 0$ esto es trivial. Supongamos ahora por hipótesis inductiva que $(a^n)^m = a^{nm}$. Entonces,

$$(a^n)^{m+1} = (a^n)^m a^n = a^{nm} a^n = a^{nm+n}$$

y así $(a^n)^m = a^{nm}$, para todo $n, m \geq 0$.

9) Si $n \geq 0$ y $m < 0$, entonces

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

Finalmente si $n < 0$ y $m \in \mathbb{Z}$,

$$(a^n)^m = ((a^{-1})^{-n})^m = (a^{-1})^{-nm} = a^{nm},$$

como afirmamos. □

Ejercicio 3. *Pruebe que si un grupo G tiene exponente 2, entonces es abeliano.*

Solución. Se sigue de que

$$abab = (ab)^2 = 1 = a^2 b^2 = aabb,$$

para todo $a, b \in G$. □

Ejercicio 4. *Pruebe que vale lo siguiente:*

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 $G = \langle G \setminus H \rangle$.

Solución. 1) Tomemos $a \in H \setminus L$ e $b \in L \setminus H$. Entonces ab no puede pertenecer a H, ya que en caso contrario $b = a^{-1}(ab)$ también pertenecería a H. Similarmente ab tampoco puede pertenecer a L y así $G \neq H \cap L$.

2) Dado que $G = \langle G \setminus H \rangle \cup H$ y que $H \neq G$, por el item 1) debe ser $G = \langle G \setminus H \rangle$. □

Ejercicio 5. *Pruebe que cada elemento de un cuerpo finito es suma de dos cuadrados.*

Solución. Supongamos que F es un cuerpo finito y denotemos con F^2 al conjunto de los cuadrados de F. Afirmamos que $2\#(F^2) > \#(F)$. En efecto esto se sigue de que $a^2 = b^2$ implica $(a+b)(a-b) = 0$ y así $a = b$ o $a = -b$. En consecuencia, por la Proposición 1.6.6, $F = F^2 + F^2$. □

Ejercicio 6. *Pruebe que un subgrupo H de G es invariante si y sólo si $ab \in H$ implica que $ba \in H$.*

Solución. Si H es normal y $ab \in H$, entonces $ba = a^{-1}(ab)a \in H$. Recíprocamente supongamos que $ab \in H$ implica que $ba \in H$ y tomemos $h \in H$. Entonces $(ha^{-1})a = h \in H$ y así $aha^{-1} \in H$, cualquiera sea $a \in G$. □

Ejercicio 7. *Supongamos que $f\colon A \to B$ es un morfismo sobreyectivo de magmas. Pruebe que:*

1) Si A es asociativo, entonces B también lo es.

2) Si A es conmutativo, entonces B también lo es.

3) Si e es unidad a izquierda de A, entonces $f(e)$ es unidad a izquierda de B.

Solución. El item 1) Se sigue de que

$$f(a)(f(b)f(c)) = f(a(bc)) = f((ab)c) = (f(a)f(b))f(c),$$

el 2) de que

$$f(a)f(b) = f(ab) = f(ba) = f(b)f(a)$$

y el 3) de que

$$f(e)f(a) = f(ea) = f(a) \quad \text{para todo } a \in A. \quad \square$$

Ejercicio 8. *Denotemos con $f\colon G \to G'$ a un morfismo de grupos y con K y L a dos subconjuntos de G'.*

1) Pruebe que $f^{-1}(K^{-1}) = f^{-1}(K)^{-1}$.

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

Solución. 1) Es consecuencia inmediata de que

$$a \in f^{-1}(K^{-1}) \Leftrightarrow f(a) \in K^{-1} \Leftrightarrow f(a)^{-1} \in K \Leftrightarrow f(a^{-1}) \in K \Leftrightarrow a^{-1} \in f^{-1}(K).$$

2) Es claro que $f^{-1}(K)f^{-1}(L) \subseteq f^{-1}(KL)$ (para esto no se usa que f sea sobreyectivo). Supongamos que $a \in f^{-1}(KL)$ de manera de que $f(a) = kl$ con $k \in K$ y $l \in L$. Como f es sobreyectivo existe $b \in K$ tal que $f(b) = k$. Entonces $f(b^{-1}a) = f(b)^{-1}f(a) = k^{-1}kl = l$ y así $a = b(b^{-1}a) \in f^{-1}(K)f^{-1}(L)$. □

Ejercicio 9. *Pruebe que si $\pi\colon G \to G'$ es un morfismo sobreyectivo de grupos y H es un subgrupo normal de G, entonces $\pi(H)$ es un subgrupo normal de G' y $G/(H\operatorname{Ker}(\pi)) \simeq G'/\pi(H)$.*

Solución. Como π es sobreyectiva, $\pi(H)$ es un subgrupo normal de G'. El resto se sigue inmediatamente de la propiedad universal del cociente aplicado al caso en que f está reemplazado por $\pi_H \circ \pi$, donde $\pi_H\colon G' \to G'/\pi(H)$ es la proyección canónica, y de que $\pi_H \circ \pi$ es sobreyectiva y $\operatorname{Ker}(\pi_H \circ \pi) = \pi^{-1}(H) = H\operatorname{Ker}(\pi)$. □

Ejercicio 10. *Pruebe que si $f\colon G \to G'$ es un morfismo de grupos y H' es un subgrupo normal de G', entonces $f^{-1}(H')$ es un subgrupo normal de G y existe un único morfismo inyectivo $\overline{f}\colon G/f^{-1}(H') \to G'/H'$ de grupos, tal que el diagrama*

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

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

Solución. Es claro que $f^{-1}(H')$ es un subgrupo normal de G. El resto se sigue inmediatamente de los comentarios que preceden a la Observación 1.11.9. □

Ejercicio 11. *Muestre que si $g\colon G \to G$ es un endomorfismo de grupos, entonces no necesariamente $g(\mathrm{Z}(G)) \subseteq \mathrm{Z}(G)$.*

Solución. Denotemos con H al grupo cuaterniónico $\{1, -1, i, -i, j, -j, k, -k\}$ y con K a $\{1, -1, i, -i\}$. Claramente K es un subgrupo de H y el conjunto $K \times H$ con la multiplicación definida coordenada a coordenada es un grupo. Es fácil ver que $\mathrm{Z}(K \times H) = K \times \{1, -1\}$ y así el endomorfismo $f\colon K \times H \to K \times H$, definido por $f(k, h) = (1, k)$, no satisface $f(\mathrm{Z}(K \times H)) \subseteq \mathrm{Z}(K \times H)$. □

Ejercicio 12. *Pruebe que si $g\colon G \to G'$ es un morfismo sobreyectivo de grupos, entonces $g(\mathrm{Z}(G)) \subseteq \mathrm{Z}(G')$.*

Solución. Tomemos $a \in \mathrm{Z}(G)$ y $b' \in G'$ arbitrario. Como g es sobreyectivo existe $b \in G$ tal que $b' = g(b)$ y así, $b'g(a) = g(ba) = g(ab) = g(a)b'$. □

Ejercicio 13. *Pruebe que si H es un subgrupo normal de un grupo finito G y $|H|$ y $|G : H|$ son coprimos, entonces H es un subgrupo completamente normal de G.*

Solución. Consideremos un endomorfismo $f\colon G \to G$. Como $|f(H)|$ divide a H, se sigue de la hipótesis que $|f(H)|$ es coprimo con $|G/H|$ y así, por la Observación 1.11.6, el morfismo canónico

$$f(H) \hookrightarrow G \to \frac{G}{H}$$

es trivial, lo que implica que $f(H) \subseteq H$. □

Ejercicio 14. *Supongamos que $H \subseteq L$ son subgrupos de un grupo G y que H es característico en G. Pruebe que L/H es característico en G/H, entonces L es característico en G.*

Solución. Consideremos un automorfismo $f\colon G \to G$. Como H es característico en G vale que $f(H) = H$. En consecuencia f induce un automorfismo $\overline{f}\colon G/H \to G/H$. Por hipótesis $f(L)/H = \overline{f}(L/H) = L/H$ y así $f(L) = L$. □

Ejercicio 15. *Supongamos que $H \subseteq L$ son subgrupos de un grupo G y que H es completamente normal en G. Pruebe que L/H es completamente normal en G/H, entonces L es completamente normal en G.*

Solución. Consideremos un endomorfismo $f\colon G \to G$. Como H es completamente normal en G vale que $f(H) \subseteq H$. En consecuencia f induce un endomorfismo $\overline{f}\colon G/H \to G/H$. Por hipótesis $f(L)H/H = \overline{f}(L/H) \subseteq L/H$ y así $f(L) \subseteq L$. □

Ejercicio 16. *Demuestre que el conmutador $[\ ,\ ]\colon G \times G \to G$ satisface las siguientes propiedades.*

1) $[a, bc] = [a, b]b[a, c]b^{-1}$ *y* $[ab, c] = a[b, c]a^{-1}[a, c]$.

2) $[cac^{-1}, [b, c]][bcb^{-1}, [a, b]][aba^{-1}, [c, a]] = 1$ *(identidad de Hall).*

3) $b[a, [b^{-1}, c]]b^{-1}c[b, [c^{-1}, a]]c^{-1}a[c, [a^{-1}, b]]a^{-1} = 1$ *(identidad de Jacobi).*

Solución. Sale por cálculo directo. □

Ejercicio 17. *Supongamos que H y L son subgrupos de un grupo G y que L está incluído es $\mathrm{N}_G(H)$. Pruebe que si K es un subgrupo normal de L, entonces HK es un subgrupo normal de HL.*

Solución. Claramente basta ver que $lKl^{-1} \subseteq HK$ y $hKh^{-1} \subseteq HK$ para todo $l \in L$ y todo $h \in H$ y que $lHl^{-1} \subseteq HK$ para todo $l \in L$. Lo primero se sigue de que K es un subgrupo normal de L y lo último de que $L \subseteq \mathrm{N}_G(H)$. Veamos lo segundo. Como $K \subseteq L \subseteq \mathrm{N}_G(H)$, para todo $h \in H$ y todo $k \in K$, vale que $hkh^{-1}k^{-1} = h' \in H$, de dónde $hkh^{-1} = h'k \in HK$. □

Ejercicio 18. *Pruebe que si N es un subgrupo normal de $H \times L$ y*

$$N \cap (H \times \{1\}) = N \cap (\{1\} \times L) = \{(1, 1)\},$$

entonces $N \subseteq \mathrm{Z}(H \times L)$.

Solución. Supongamos que existe $(h, l) \in N \setminus \mathrm{Z}(H \times L)$ y tomemos (h', l') en $H \times L$ tal que $(h', l')(h, l) \neq (h, l)(h', l')$. Esto es claramente equivalente a que $h'h \neq hh'$ o $l'l \neq ll'$. Supongamos que vale lo primero. Entonces

$$(h'hh'^{-1}, l) = (h', 1)(h, l)(h', 1)^{-1} \in N \quad \text{y} \quad h'hh'^{-1} \neq h.$$

Así $(h'hh'^{-1}h^{-1}, 1) = (h'hh'^{-1}, l)(h, l)^{-1} \in N$ y es distinto de $(1, 1)$. Similarmente, si $l'l \neq ll'$, entonces N corta a $\{1\} \times L$ no trivialmente. □

Ejercicio 19. *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 $G = H \times L$.*

Solución. Como H es simple y $L \neq H$, debe ser $H \cap L = \{1\}$, lo que implica que $H \subsetneq HL$ y así $HL = G$. Por el Teorema 1.14.7, esto muestra que $G = H \times L$. Finalmente, dado que $L \simeq G/H$, obtenemos que $|L| = 2$. □

Ejercicio 20. *Pruebe que si G es un grupo simple de orden par y $|G| = 2^k m$ con m impar, entonces $k > 1$ y G no tiene ningún elemento a tal que 2^k divide a $|a|$.*

Solución. Por la Proposiciones 1.6.14 y 3.1.3, G no tiene ningún elemento a tal que 2^k divide a $|a|$. Por la Observación 1.6.4, se sigue de esto que $k > 1$. □

Ejercicio 21. *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 $n = 4$.*

Solución. Si n es igual a 2 o 3 no hay nada que probar. Supongamos que $n \geq 5$. Por el Teorema 3.1.4, si S_n tiene un subgrupo de índice t, entonces también tiene un subgrupo normal de índice th con h un divisor de $(t-1)!$. Por el Teorema 2.5.2 esto implica que $t \in \{1, 2\}$ o $t \geq n$. Resta considerar el caso $n = 4$. Consideremos el subgrupo normal $N = \{\mathrm{id}, (1,2)\circ(3,4), (1,3)\circ(2,4), (1,4)\circ(2,3)\}$ de S_n. Por la Proposición 1.6.8 y la Observación 1.6.13, $\{\mathrm{id}, (1,2)\}N$ es un subgrupo de orden 8 de S_4. □

Ejercicio 22. *Pruebe que si G es un grupo simple infinito, entonces vale lo siguiente:*

1) *Si $a \in G$ es distinto de 1, entonces la clase de conjugación de a tiene infinitos elementos.*
2) *Si H es un subgrupo no trivial de G, entonces la clase de conjugación de H tiene infinitos elementos.*

Solución. 1) Como G es simple e infinito no puede ser abeliano (es facil ver que si un grupo abeliano es simple, entonces es cíclico de orden primo). Dado que el centro de G es un subgrupo característico debe ser igual a $\{1\}$. En consecuencia si $a \neq 1$, entonces $\mathrm{C}_G(a) \subsetneq G$ y así, por el Corolario 3.1.5, se sigue de esto que $\#(\{bab^{-1} : b \in G\}) = |G : \mathrm{C}_G(a)| = \infty$.

2) Supongamos que H es un subgrupo no trivial de G. Como G es simple, H no puede ser normal y así, $\mathrm{N}_G(H) \subsetneq G$. Por el Corolario 3.1.5 se sigue de esto que $\#(\{gHg^{-1} : g \in G\}) = |G : \mathrm{N}_G(H)| = \infty$. □

Ejercicio 23. *Pruebe que si un grupo G contiene un elemento de orden $n > 1$ y dos clases de conjugación, entonces $|G| = 2$.*

Solución. Tomemos $a \in G$ tal que $a^n = 1$ y $a^i \neq 1$ para todo $1 \leq i < n$. Es claro que si p es un primo que divide a n, entonces el orden de $a^{n/p}$ es p. Como por hipótesis todos los elementos distintos de 1 de G son conjugados, todos tienen el mismo orden y así $n = p$. Afirmamos que $n = 2$. En efecto de lo contrario existiría $b \in G$ tal que $bab^{-1} = a^2$, pero entonces $b^k a b^{-k} = a^{2^k}$, de donde $a = b^p a b^{-p} = a^{2^p} = a^2$, lo cual es absurdo. Por el Ejercicio 3) se sigue de esto que G es abeliano, lo que dado que G tiene sólo dos clases de conjugación, implica que $|G| = 2$. □

Ejercicio 24. *Pruebe que si G es un grupo que no es resoluble, entonces G tiene un subgrupo $H \neq \{1\}$ que es normal y satisface $H^{(1)} = H$. Pruebe además que si G es finito también vale la recíproca.*

Solución. Si $H \neq \{1\}$ es un subgrupo normmal de G que $H^{(1)} = H$, entonces por el Teorema 4.2.8, H no es resoluble y así, por el Teorema 4.2.1, tampoco G lo es. Supongamos ahora que G es finito. Entonces existe n tal que $G^{(n+1)} = G^{(n)}$. Si G no es resoluble, no puede ser $G^{(n)} \neq \{1\}$ y podemos tomar así $H = G^{(n)}$. □