TEORÍA DE GRUPOS

1. Definición y Propiedades Básicas

1.1.Monoides. 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 *monoide* es un conjunto A provisto de una operación interna. Usualmente hablaremos de un monoide A, mencionando sólo al conjunto subyacente y no a la operación. Esto es ambiguo, porque en 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 monoide 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. El *monoide opuesto* de un monoide A es el monoide 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 monoide 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 monoide A tienen una versión a izquierda y otra a derecha, de modo 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 monoide 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 monoide es *unitario* si tiene neutro. Es claro que A es unitario si y sólo si A^{op} lo es.

1.2.Semigrupos. Un *semigrupo* es un monoide unitario y asociativo. Es evidente que A es un semigrupo si y sólo A^{op} lo es. Un elemento a de un semigrupo 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 claro que a es inversible a izquierda (respectivamente derecha) si y sólo si l_a (respectivamente r_a) es sobreyectiva. Si a tiene inversa a izquierda y a derecha, entonces estas son únicas y coinciden. En efecto, supongamos que b y b' son inversas a izquierda y a derecha de a, respectivamente. Entonces $b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'$. 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 semigrupo no necesariamente conmutativo y usaremos la notación multiplicativa. También usaremos esta convención para monoides 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 cancelable a derecha. Si a y b son cancelable 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. 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 $n \in \mathbb{Z}$.

Supongamos que $a \in A$ es inversible y que la aplicación $n \mapsto a^n$ no es inyectiva. Tomemos $n < m$ 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 $0 \leq r \leq |a|$, 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 semigrupos.

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

Ejemplo 2. El conjunto $\mathrm{Fun}(X, X)$ de funciones de un conjunto X en si mismo con la composición como operación es un semigrupo no abeliano que tiene a la identidad de X como neutro.

1.3.Grupos. Un *grupo* G es un semigrupo 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 semigrupo 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. *Un monoide G cuya operación es asociativa, tiene un neutro a izquierda e, y satisface la propiedad de que para cada elemento $a \in G$ hay un elemento $a' \in G$ tal que $a'a = e$, es un grupo con neutro e.*

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

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

Ejemplo 1. El conjunto A^* de las unidades o elementos inversibles de un semigrupo 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, $\mathbb{Z}/n\mathbb{Z}$ de los enteros módulo n, y $k[X]$ de los polinomios con coeficientes en un anillo conmutativo k, son grupos via la suma usual. También lo son $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ y $(\mathbb{Z}/n\mathbb{Z})^*$ 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.

Decimos que un grupo G tiene *exponente finito* si existe $n \in \mathbb{N}$ tal que $g^n = 1$ para todo $g \in G$. En ese caso al mínimo n que satisface esta 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.

1.4.Submonoides. Un subconjunto B de un monoide A es un *submonoide* de A si es cerrado para el producto. Es evidente que entonces B es un monoide en si mismo. Cada monoide A tiene a A mismo como submonoide y, si A es unitario, entonces el conjunto $\{e\}$, que tiene como único elemento a la unidad de A, también es un submonoide de A. Estos son los llamados submonoides *triviales* de A. Un submonoide de A es *propio* si es distinto de A. Es fácil comprobar que la intersección de una familia arbitraria de submonoides de A es un submonoide de A. Por ejemplo, dado un subconjunto S de A, la intersección de los submonoides de A que incluyen a S es el mínimo submonoide $\langle S\rangle_s$ de A que contiene a S. Si $A = \langle S\rangle_s$, decimos que S *genera* a A. Siguiendo la práctica usual, si $S = \{x_1, \ldots, x_s\}$, escribiremos $\langle x_1, \ldots, x_s\rangle_s$, y no $\langle\{x_1, \ldots, x_s\}\rangle_s$. Esto se debe simplemente a una cuestión de estética. Un monoide 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 monoide asociativo, entonces todo submoniode de A también es asociativo y para cada 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 todos los productos asociados de todas las maneras posibles. Decimos que un submonoide B de un monoide unitario A es *unitario* si contiene a la unidad de A. Es claro también que el mínimo submonoide unitario $\langle S\rangle_u$, de un monoide unitario A que contiene a un subconjunto S de A, es el mínimo submonoide de A que contiene a la unidad de A y a S. Si $A = \langle S\rangle_u$, decimos que S *genera a* A *como monoide unitario*. De la misma manera que para el caso de submonoides de monoides no unitarios, cuando S sea $\{x_1, \ldots, x_s\}$, escribiremos $\langle x_1, \ldots, x_s\rangle_u$ en lugar no $\langle\{x_1, \ldots, x_s\}\rangle_u$. Notemos además que si un monoide es conmutativo, entonces todo submonoide de él también lo es.

1.5.Subsemigrupos. Es claro que si B es un submonoide unitario de un semigrupo A, entonces B es en si mismo un semigrupo. En este caso, para cada subconjunto S de A,

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

si usamos la convención de que el producto vacío es el neutro. Finalmente, dada una familia $\{A_i\}_{i\in I}$ de subsemigrupos de A existe un mínimo subsemigrupo $\prod_{i\in I} A_i$ de A que contiene a $\bigcup_{i\in I} A_i$. A este subsemigrupo se lo llama el *producto* de $\{A_i\}_{i\in I}$. Es fácil ver que

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

Notemos que si $A_iA_j = A_jA_i$ para todo $i, j \in I$ e 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 semigrupo A, el subconjunto formado por los elementos de A que son cancelables a izquierda es un subsemigrupo 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. Por último, para cada monoide unitario A, vale que $\mathrm{End}_u(A)$ es un subsemigrupo de $\mathrm{End}(A)$.

1.6.Subgrupos. Un subsemigrupo 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 $a = b \in H$ 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 monoides escribiremos $\langle x_1, \ldots, x_s\rangle$ en lugar de $\langle\{x_1, \ldots, x_s\}\rangle$. 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 subsemigrupos de un semigrupo) es un subgrupo de G.

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 $n \in \mathbb{N}$ es 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 $\mathrm{G}_\infty = \bigcup_{n\in\mathbb{N}} \mathrm{G}_n$.

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. Dados subconjuntos K y L de un monoide A, denotamos con KL al subconjunto de A formado por todos los productos ab con $a \in K$ y $b \in L$. Por supuesto que escribiremos aK y Ka en lugar de $\{a\}K$ y $K\{a\}$ respectivamente. Es claro que si A es asociativo, entonces $(KL)M = K(LM)$ para toda terna K, L y M de subconjuntos de A, de manera que no escribiremos los paréntesis. Por último si A es un grupo escribimos $K^{-1} = \{x^{-1} : x \in K\}$. Es inmediato que $(KL)^{-1} = L^{-1}K^{-1}$. Fijemos ahora un subgrupo H de un grupo G. Una *coclase a izquierda* de H en G es un subconjunto de G que tiene la forma xH para algún $x \in G$. Dos coclases a izquierda que no son disjuntas coinciden. En efecto, si $xh = yh'$ con $h, h' \in H$, entonces $xH = xhH = yh'H = yH$. Así, G es la unión disjunta de sus coclases a izquierda. Además, dado que la aplicación $h \mapsto xh$ induce una biyección de H en xH, 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 Hx para algún $x \in G$. Dado que la asignación $xH \mapsto Hx^{-1}$ 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 H y K son subgrupos de un grupo G y $K \subseteq H$. Entonces*

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

Demostración. Escribamos G y H como uniones disjuntas $G = \bigcup_i x_i H$ y $H = \bigcup_j y_j K$, de coclases a izquierda de H en G y de K en H respectivamente. Es claro que $G = \bigcup_{i,j} x_i y_j K$. Debemos ver que esta unión es disjunta. Supongamos que $x_i y_j K = x_{i'} y_{j'} K$. Multiplicando por H a la derecha obtenemos que $x_i H = x_{i'} H$, lo que implica que $i = i'$. Pero entonces $y_j K = y_{j'} K$, de donde $j = j'$. □

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

Observación 1.6.3. *El resultado de arriba dice 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*

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

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

Corolario 1.6.4. *Si un grupo tiene orden primo, entonces es cíclico.*

Observación 1.6.5. *Si H y L son subgrupos de un grupo G, entonces*

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

En efecto la primera desigualdad se sigue de que la aplicación

$$\phi\colon L/(H \cap L) \to G/H, \quad \text{definida por } \phi(g(H \cap L)) = gH,$$

es inyectiva ya que $gH = g'H$ equivale a que $g^{-1}g' \in H$ y por lo tanto a que $g^{-1}g' \in H \cap L$ (ya que $g, g' \in L$) y, en consecuencia, $g(H \cap L) = g'(H \cap L)$. La segunda desigualdad se sigue ahora de que $|G : H \cap L| = |G : L||L : H \cap L|$. Notemos también que la imagen de ϕ es LH/H, de manera de que si $LH = G$, entonces las desigualdades de arriba se convierten en igualdades. Además se sigue claramente de todo esto que si $|G : H|$ es finito y $|L : H \cap L| = |G : H|$, entonces $LH = G$. 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

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

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

Observación 1.6.6. *Si la intersección de una familia $(g_iH_i)_{i\in I}$ de 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 $d \in \bigcap_{i\in I} g_iH_i$, entonces $dH_i = g_iH_i$ para todo $i \in I$ y, por lo tanto $\bigcap_{i\in I} g_iH_i = d\bigcap_{i\in I} H_i$.*

Por último veamos 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 $H \subseteq K$ y L son subgrupos de un grupo G, entonces*

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

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

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

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

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

$$|HK||H \cap K| = |H||K|.$$

Demostración. Como la función $\phi\colon H \times K \to HK$, definida por $\phi(h,k) = hk$ es sobreyectiva, es suficiente ver que $|\phi^{-1}(x)| = |H \cap K|$, para todo $x \in HK$. Para ello bastará probar que si $x = hk$, entonces $\phi^{-1}(x) = \{(hd, d^{-1}k) : d \in H \cap K\}$. Es claro que $\{(hd, d^{-1}k) : d \in H \cap K\} \subseteq \phi^{-1}(x)$. Supongamos ahora que $(h', k') \in \phi^{-1}(x)$. Entonces $h'k' = x = hk$ y así, $d := h^{-1}h' = kk'^{-1} \in H \cap K$, de donde $h' = hd$ y $k' = d^{-1}k$. $\square$

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

1) Si $KH \subseteq HK$, entonces HK es un subgrupos de G.

2) Si HK es un subgrupos de G, entonces $KH = HK$.

Demostración. Supongamos que $KH \subseteq HK$. Entonces

$$HK(HK)^{-1} = HKK^{-1}H = HKH \subseteq HHK = HK$$

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

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

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

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

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

$$|Hg_iKg_i^{-1}| = \frac{|H||g_iKg_i^{-1}|}{|H \cap g_iKg_i^{-1}|} = \frac{|H||K|}{|H \cap g_iKg_i^{-1}|},$$

de donde $(*)$ se sigue inmediatyamente. Notemos que cuando $K = 1$ la fórmula (1) se reduce al teorema de Lagrange.

Subgrupos normales. Un subgrupo H de un grupo G es *normal* o *invariante* si $xHx^{-1} = H$ para todo $x \in G$. 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 1.6.10. *Para cada subgrupo H de G son equivalentes:*

1) *Dado $x \in G$ existe $y \in G$ tal que $xH \subseteq Hy$,*
2) *Dado $x \in G$ existe $y \in G$ tal que $xHy^{-1} \subseteq H$,*
3) *Dado $x \in G$ existe $y \in G$ tal que $Hx \subseteq yH$,*
4) *Dado $x \in G$ existe $y \in G$ tal que $y^{-1}Hx \subseteq H$,*
5) *$Hx = xH$ para todo $x \in G$,*
6) *H es normal.*

Demostración. Es evidente que 5) implica 1) y 3) y claramente 1) es equivalente a 2), ya que de $xH \subseteq Hy$ se sigue que $xHy^{-1} \subseteq Hyy^{-1} = H$ y de $xHy^{-1} \subseteq H$ se sigue que $xH = xHy^{-1}y \subseteq Hy$. Similarmente 3) es equivalente a 4) y 5) a 6). Veamos que 1) implica 5). De $x \in xH \subseteq Hy$ se sigue facilmente que que $Hx = Hy$ y así $xH \subseteq Hx$. Similarmente $x^{-1}H \subseteq Hx^{-1}$ y, por lo tanto, $Hx = xx^{-1}Hx \subseteq xHx^{-1}x = xH$ y, en consecuencia, $xH = Hx$. Para terminar la demostración resta ver que 3) implica 5), lo cual es similar a 1) implica 5). □

Ejercicio. *Pruebe que un subgrupo H de G es invariante si y sólo si $gg' \in H$ implica que $g'g \in H$.*

Observación 1.6.11. *Si $H \subseteq K$ son subgrupos de un grupo G y H es normal en G, entonces H es normal en K.*

Observación 1.6.12. *Si H es un subgrupo normal de G, entonces $HK = KH$ para todo subconjunto K de G. Si además K es un subgrupo de G, entonces HK también es un subgrupo de G. Por último si K es normal en G, entonces HK también lo es.*

La siguiente proposición será mejorada más adelante.

Proposición 1.6.13. *Todo subgrupo H de un grupo G de índice 2, es normal.*

Demostración. Tomemos $x \in G \setminus H$. Como H tiene índice 2, es $G = H \bigcup xH = H \bigcup Hx$ con ambas uniones disjuntas. Así $xH = Hx$, de dónde H es normal. □

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 G. Es fácil ver que

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

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

Proposición 1.6.14. 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

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

Demostración. Lo último se sigue de que, por la Observación 1.6.12, $G_iG_j = G_jG_i$, para todo $i, j \in I$. Tomemos ahora $g_{i_1} \cdots g_{i_n} \in \prod_{i \in I} G_i$. Como, para cada $a \in G$

vale que $a(g_{i_1} \cdots g_{i_n})a^{-1} = (ag_{i_1}a^{-1})(ag_{i_2}a^{-1}) \cdots (ag_{i_n}a^{-1}) \in \prod_{i \in I} G_i$, el subgrupo $\prod_{i \in I} G_i$ de G es normal. $\square$

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.

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 es cíclico.

Lema 1.7.1. *Para cada grupo G vale que*

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

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

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

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.

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. Supongamos que G es un grupo de orden n que tiene a lo sumo un subgrupo de orden d para cada divisor d de n. Por el Lema 1.7.1 y la Proposición 1.7.2,

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

donde G recorre el conjunto de los subgrupos cíclicos de G y $\operatorname{gen}(C)$ denota a los generadores de C. En consecuencia G debe tener un subgrupo cíclico de orden d para cada divisor d de n. En particular G tiene un subgrupo cíclico de orden n y así G es cíclico. $\square$

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 monoides. Un *morfismo de monoides* $f\colon A \to B$ es una función de A en B que satisface $f(ab) = f(a)f(b)$. Por ejemplo, la inclusión canónica de un submonoide A de un monoide B en B es un morfismo de monoides y también la composición de dos morfismos de monoides lo es. Un caso particular de lo primero es la función identidad de un monoide en si mismo. Si B es un monoide unitario, entonces cualquiera sea el monoide A, la aplicación $f\colon A \to B$, definida por $f(a) = 1$, para todo $a \in A$ es un morfismo de monoides. Es inmediato que si $f\colon A \to B$ es un morfismo de monoides, entonces $f(KL) = f(K)f(L)$ para todo par de subconjuntos K y L de A. Supongamos que $f\colon A \to B$ es un morfismo sobreyectivo de monoides. 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 $f \circ f^{-1} = \mathrm{id}_B$ y $f^{-1} \circ f = \mathrm{id}_A$. 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 $\mathrm{Hom}(A, B)$, $\mathrm{Iso}(A, B)$, $\mathrm{End}(A)$ y $\mathrm{Aut}(A)$ 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 semigrupo que tiene a la identidad de A como unidad, y que además $\mathrm{Aut}(A) = \mathrm{End}(A)^*$. Decimos que un morfismo $f\colon A \to B$, entre dos monoides unitarios, es un *morfismo de monoides unitarios* o más simplemente que es *unitario* si $f(e) = e$. Es claro que la inclusión canónica de un submonoide unitario A de un moniode unitario B en B es un morfismo de monoides unitarios y que la composición de dos morfismos de monoides unitarios también lo es. Además si un morfismo de monoides unitarios es un isomorfismo de monoides, su inversa también es un morfismo unitario. Con $\mathrm{Hom}_u(A, B)$, $\mathrm{Iso}_u(A, B)$, $\mathrm{End}_u(A)$ y $\mathrm{Aut}_u(A)$ denotamos a los subconjuntos de $\mathrm{Hom}(A, B)$, $\mathrm{Iso}(A, B)$, $\mathrm{End}(A)$ y $\mathrm{Aut}(A)$ respectivamente, formados por los morfismos de monoides unitarios. Es claro que

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

Finalmente diremos que $f\colon A \to B$ es un *monomorfismo* si $f \circ g = f \circ g'$ implica $g = g'$, para todo par de morfismos de monoides $g, g'\colon C \to A$; un *epimorfismo* si $g \circ f = g' \circ f$ implica $g = g'$, para todo par de morfismos de monoides $g, g'\colon B \to C$; 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 y los consideramos así, pedimos que todos los morfismos que aparecen en estas definiciones también lo sean. Notemos de todos modos que si f es unitario, entonces de $g \circ f = \mathrm{id}_A$ se

sigue que g también lo es. No vale sin embargo que si f es unitario, de $f \circ h = \mathrm{id}_B$, se deduzca que h también lo sea. Denotemos con $f\colon A \to B$ y $g\colon B \to C$ a dos morfismos de monoides. 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.

1.9.Morfismos de semigrupos. Un *morfismo* $f\colon A \to B$, de un semigrupo A en otro B, es simplemente morfismo de monoides unitarios. Por ejemplo la inclusión canónica de un subsemigrupo A de un semigrupo B en B es un morfismo de semigrupos. Observemos que en el caso de semigrupos 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 a es inversa a izquierda de b, entonces $f(a)$ es inversa a izquierda de $f(b)$. 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 semigrupos $f\colon A \to B$ es un *monomorfismo* si $f \circ g = f \circ g'$ implica $g = g'$, para todo par de morfismos de semigrupos $g, g'\colon C \to A$, y que es un *epimorfismo* si $g \circ f = g' \circ f$ implica $g = g'$, para todo par de morfismos de semigrupos $g, g'\colon B \to C$. Notemos que, al menos en principio, un morfismo de semigrupos puede ser un monomorfismo o un epimorfismo, cuando se lo considera como morfismo de semigrupos, pero puede dejar de serlo cuando se lo considera como morfismo de monoides. Hay también una definición de sección y de retracción, pero coincide con la dada anteriormente. Es facil ver que los items 1) a 13) del ejercicio con que termina la sección anterior siguen valiendo es el contexto de semigrupos. 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 $f \circ g = f \circ g'$. Esto prueba también que un monomorfismo de semigrupos sigue siendo un monomorfismo cuando se lo considera como morfismo de monoides. Por último, si $f\colon A \to B$ es un morfismo de semigrupos 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* $f\colon G \to H$, de un grupo G en otro H, es por definición morfismo de semigrupos. Como vimos recién es innecesario pedir que $f(1)$ sea 1. Al igual que para el caso de semigrupos pueden darse aquí definiciones de *monomorfismo*, *epimorfismo*, *sección* y *retracción*. Nuevamente estas

últimas coinciden con las definiciones dadas en el caso de monoides 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 semigrupos o monoides. 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 $f\circ g = f\circ g'$, lo que prueba también que un monomorfismo de grupos sigue siendo un monomorfismo cuando se lo considera como morfismo de semigrupos o de monoides. Se puede ver también que todo epimorfismo de grupos es sobreyectivo, pero esto es mucho más dificil. Nuevamente valen con las mismas demostraciones los items 1) a 13) del ejercicio con que termina la sección de morfismos de monoides. Por último es inmediato 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. *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 de grupos.

Ejemplo 2. La exponencial $x \mapsto e^x$ es un isomorfismo de 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 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 4. 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.

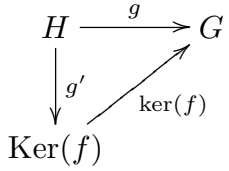
Ejemplo 5. El monomorfismo de $i\colon \mathbb{Z}_2 \to \mathbb{Z}_4$, definido por $\pi(0) = 0$ y $\pi(1) = 2$, no es una sección.

Ejemplo 6. 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.

El núcleo de un morfismo. El *núcleo* de un morfismo de grupos $f\colon G \to G'$ es $\mathrm{Ker}(f) = \{x \in G : f(x) = 1\}$. 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.*

Proposición 1.10.1. *Un morfismo $f\colon G \to G'$ de grupos es inyectivo si y sólo si su núcleo es $\{1\}$.*

Demostración. Esto se sigue immediatamente de que $f(x) = f(y)$ equivale a que $xy^{-1} \in \mathrm{Ker}(f)$. □

1.11.Relaciones de equivalencia compatibles y cocientes de grupos. Consideremos una relación de equivalencia $\sim$ definida en un monoide 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 monoide tal que π es un morfismo si y sólo si

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

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 monoides 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 semigrupo o un grupo, $A/\sim$ también lo es. Se pueden decir muchas cosas acerca de los cocientes de monoides y semigrupos 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

$$a \sim b \Leftrightarrow ab^{-1} \in H \Leftrightarrow a^{-1}b \in H,$$

de manera de que $\sim$ queda determinada por H. Recíprocamente si H es un subgrupo normal de G, entonces por la Proposición 1.6.10, las relaciones de equivalencias

$$x \sim y \Leftrightarrow xy^{-1} \in H \Leftrightarrow x \in Hy \quad \text{y} \quad x \sim' y \Leftrightarrow y^{-1}x \in H \Leftrightarrow x \in yH$$

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

$$xHx'H = xx'HH = xx'H.$$

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

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

conmuta.

Demostración. Por definición $\pi(x) = 1$ significa que $x \sim 1$ o, lo que es lo mismo, que $x = x1^{-1} \in H$. Esto prueba el item 1). Dado $x \in G$ denotemos con $\overline{x}$ a su clase en G/H. Para la primera parte del item 2) basta observar que si $x \sim y$ entonces $xy^{-1} \in H \subseteq \operatorname{Ker}(f)$ y así, $f(x) = f(y)$, lo que permite definir $\overline{f}(\overline{x})$ como $f(x)$. Dado que $\overline{x} = \pi(x)$, esto dice que $f = \overline{f} \circ \pi$. Además $\overline{f}$ es un morfismo de grupos ya que

$$\overline{f}(\overline{x}\,\overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y}).$$

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

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

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

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*

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

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.

Observación 1.11.5. *Si $f\colon G \to G'$ es un morfismo de grupos, entonces por el teorema de Lagrange, $|\operatorname{Im}(f)|$ divide a $|G'|$ y $|\operatorname{Im}(f)| = |G : \operatorname{Ker}(f)|/|G|$ y 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 1.11.6. *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 $xH \mapsto f(x)f(H)$ 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 es suficiente notar que de $f(x)f(H) = f(x')f(H)$ se sigue que $f(x^{-1}x') = f(x^{-1})f(x') \in f(H)$, de donde $x^{-1}x' \in H \operatorname{Ker}(f) = H$, lo que implica que $xH = x'H$. Por último si H es un subgrupo normal de G, entonces $f(H)$ es un subgrupo normal de $f(G)$ y

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

Ejercicio. *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 $\pi' \circ f(x) = 1$ para todo $x \in H$. 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 $\operatorname{Ker}(\overline{f}) = f^{-1}(H')/H$.

Observación 1.11.7. *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. *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 $\pi\colon G \to G/H$ y $\pi'\colon G' \to G'/H'$ son las proyecciones canónicas, conmuta y que además $\operatorname{Im}(\overline{f}) = \pi'(\operatorname{Im}(f)) = \operatorname{Im}(f)H'/H'$.

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

$$\Phi_x(yz) = xyzx^{-1} = (xyx^{-1})(xzx^{-1}) = \Phi_x(y)\Phi_x(z)$$

y lo segundo de que

$$\Phi_{xy}(z) = xyz(xy)^{-1} = x(yzy^{-1})x^{-1} = \Phi_x(\Phi_y(z)).$$

Notemos que x está en el núcleo del morfismo $G \to \mathrm{Aut}(G)$ que acabamos de definir si y sólo si $xyx^{-1} = \Phi_x(y) = y$ para todo $y \in G$. Dado que $xyx^{-1} = y$ equivale a $xy = yx$ es natural decir definir el centro $\mathrm{Z}(G)$ de G como este núcleo y decir que $x \in G$ 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 x e y de un grupo G son conjugados si existe $z \in G$ tal que $y = zxz^{-1}$, es decir si $y = \Phi_z(x)$. En particular los ordenes de dos elementos conjugados coinciden. La relación definida por $x \sim y$ si y sólo si x e y son conjugados es claramente de equivalencia, de manera que G queda partido en clases, llamadas *clases de conjugación*. Es evidente que si x e y son elementos arbitrarios de un grupo G, entonces xy es conjugado a yx, ya que $yx = x^{-1}(xy)x$. Recíprocamente, si x e y son conjugados e $y = zxz^{-1} = z(xz^{-1})$, entonces $(xz^{-1})z = x$. Practicamente por definición un subgrupo H de G es normal si y sólo si $\Phi_x(H) \subseteq H$ para todo $x \in G$ (en otras palabras si con cada elemento x de G contiene a su clase de conjugación). Es fácil ver que entonces $\Phi_x(H) = H$ para todo $x \in X$ ya que de $x^{-1}Hx = \Phi_{x^{-1}}(H) \subseteq H$ se sigue que $H \subseteq xHx^{-1} = \Phi_x(H)$. 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 $x \in X$ 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 $x \in \mathrm{Z}(G)$ y $g \in \mathrm{Aut}(G)$, entonces $g(z) \in \mathrm{Z}(G)$, pero

$$g(z)x = g(z)g(g^{-1}(x)) = g(zg^{-1}(x)) = g(g^{-1}(x)z) = g(g^{-1}(x))g(z) = xg(z),$$

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

$$(g \circ \Phi_x \circ g^{-1})(y) = g(\Phi_x(g^{-1}(y))) = g(xg^{-1}(y)x^{-1}) = g(x)yg(x)^{-1} = \Phi_{g(x)}(y),$$

para todo $y \in G$. 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 automorfismo 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 dicha sucesión es *exacta*.

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

Proposición 1.12.1. *Si G no es abeliano, entonces $G/\mathrm{Z}(G)$ no es cíclico.*

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

$$(x^\alpha h)(x^{\alpha'} h') = x^\alpha x^{\alpha'} hh' = x^{\alpha'} x^\alpha h' h = (x^{\alpha'} h')(x^\alpha h),$$

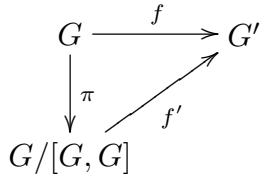
esto es absurdo. □

Observación 1.12.2. *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 $x \in G$. Debemos ver que $\Phi_x(H) = H$. Como L es normal en G, el automorfismo interior Φ_x 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 $\Phi_x(H) = H$. También vale que si H es un subgrupo característico de L y L es 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_x de G hay que considerar un automorfismo arbitrario.

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 característico 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 $[G,G] \subseteq H$. En particular se sigue de todo esto 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 $f'\colon \frac{G}{[G,G]} \to G'$ tal que el diagrama



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 1.11.7, 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

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

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

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

Proposición 1.12.3. *Vale lo siguiente:*

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

Demostración. El item 1) es trivial. Veamos el item 2). Tomemos un automorfismo f de G. Como H y K son subgrupos característicos de G, sabemos que $f(H) = H$ y $f(K) = K$ y así, $f([H,K]) = [f(H), f(K)] = [H,K]$. La demostración del item 3) es similar, pero tomando como f en automorfismo interior de G, en lugar de uno arbitrario. □

Observación 1.12.4. *Si L es un subgrupo normal de G que contiene a $[H,K]$, entonces las imagenes de los elementos de H en G/L conmutan con las de los elementos de K. El mínimo L para el que pasa esto es claramente el mínimo subgrupo normal $\overline{[H,K]}$ de G que contiene a $[H,K]$. Denotemos con $\overline{H}$ y $\overline{K}$ a los mínimos subgrupos normales de H y K respectivamente. Dado que $[H,K] \subseteq [\overline{H}, \overline{K}]$ y que, por el item 3) de la Proposición 1.12.3, $[\overline{H}, \overline{K}]$ es un subgrupo normal de G, es claro que $\overline{[H,K]} \subseteq [\overline{H}, \overline{K}]$.*

Supongamos que H y K 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 $f(K)$, entonces existe un único morfismo $f'\colon \frac{G}{[H,K]} \to G'$ tal que el diagrama

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

donde π denota al epimorfismo canónico, conmuta. Supongamos ahora que H y K son subgrupos normales de un grupo G y que H' y K' son subgrupos normales de un grupo G'. Por el comentario que precede a la Observación 1.11.7, dado un

morfismo de grupos $f\colon G \to G'$ tal que $f(H) \subseteq H'$ y $f(K) \subseteq K'$, existe un único morfismo $\overline{f}\colon \frac{G}{[H,K]} \to \frac{G'}{[H',K']}$ tal que el diagrama

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

donde π y π' denotan a los epimorfismo canónicos, conmuta. Por último vale que $\overline{\mathrm{id}_G} = \mathrm{id}_{G/[H,K]}$ 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 $g(K') \subseteq K''$, donde H'' y K'' son subgrupos normales de G'', entonces $\overline{g \circ f} = \overline{g} \circ \overline{f}$.

Subgrupos conjugados. Similarmente al caso de elementos decimos que dos subgrupos H y L de un grupo G son conjugados si existe $x \in G$ tal que $L = xHx^{-1}$. Es claro que los ordenes de dos subgrupos conjugados coinciden. Veamos que también los índices lo hacen. Fijemos $x \in G$ y consideremos el automorfismo $\Phi_x\colon G \to G$ definido por $\Phi_x(y) = xyx^{-1}$. Por la Obsevación 1.11.6, $|G : \Phi_x(H)| = |G : H|$ y así, para terminar la demostración basta observar que $\Phi_x(H) = xHx^{-1}$. 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 $N = \bigcap_{x\in G} xHx^{-1}$ es el máximo subgrupo normal de G que está incluído en H. En efecto, N es normal ya que

$$yNy^{-1} \subseteq \bigcap_{x\in G} yxHx^{-1}y^{-1} = \bigcap_{x\in G} xHx^{-1} = N,$$

y la maximalidad de N se sigue de que si $L \subseteq H$ es un subgrupo normal de G, entonces $L = xLx^{-1} \subseteq xHx^{-1}$ para todo $x \in G$ y así, $L \subseteq N$. Notemos por último que si $\{g_i\}_{i\in I}$ es un conjunto de representantes de las coclases a izquierda de H en G, entonces $N = \bigcap_{i\in I} g_iHg_i^{-1}$, ya que $(g_ih)H(g_ih)^{-1} = g_iHg_i^{-1}$, para todo $i \in I$ y todo $h \in H$.

Observación 1.12.5. *Supongamos H es un subgrupo de G de índice finito n. Denotemos con $g_1, \ldots, g_n$ a representantes de las coclases a izquierda de H en G y con N a $\bigcap_{i=1}^n g_iHg_i^{-1}$. Por la Observación 1.6.5,*

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

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

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

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

$$gg'g^{-1}h(gg'g^{-1})^{-1} = gg'(g^{-1}hg^{-1})g'^{-1}g = g(g^{-1}hg^{-1})g = h,$$

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

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

$$(h, k)(h', k') = (hh', kk')$$

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

$$\pi_H \colon H \times K \to H, \quad \pi_K \colon H \times K \to K, \quad \iota_H \colon H \to H \times K \quad \text{y} \quad \iota_K \colon K \to H \times K,$$

definidas por

$$\pi_H(h, k) = h, \quad \pi_K(h, k) = k, \quad \iota_H(h) = (h, 1) \quad \text{y} \quad \iota_K(k) = (1, k)$$

son morfismos de grupos que satisfacen

$$h = \pi_H(\iota_H(h)), \quad k = \pi_K(\iota_K(k)) \quad \text{y} \quad (h, k) = \iota_H(\pi_H(h, k))\iota_K(\pi_K(h, k))$$

para todo $h \in H$ y $k \in K$, y además

$$\mathrm{Ker}(\pi_H) = \{1\} \times K = \mathrm{Im}(\iota_K) \qquad \text{y} \qquad \mathrm{Ker}(\pi_K) = H \times \{1\} = \mathrm{Im}(\iota_H).$$

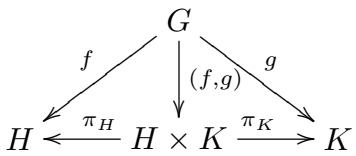
En particular la sucesión

$$1 \longrightarrow H \xrightarrow{\iota_H} H \times K \xrightarrow{\pi_K} K \longrightarrow 1$$

es exacta (es decir que ι_H es inyectiva, π_K es sobreyectiva y $\mathrm{Ker}(\pi_K) = \mathrm{Im}(\iota_H)$) y ι_H y π_K son una sección y una retracción, respectivamente. El producto $H \times K$,

junto con los morfismos π_H y π_K, tiene la siguiente propiedad (que se denomina *propiedad universal del producto directo*):

Si $f\colon G \to H$ y $g\colon G \to K$ son morfismos de grupos, entonces existe un único morfismo de grupos $(f,g)\colon G \to H \times K$ tal que el diagrama



conmuta. Es decir que $\pi_H \circ (f,g) = f$ y $\pi_K \circ (f,g) = g$.

En efecto, estas igualdades fuerzan a que sea $(f,g)(x) = (f(x), g(x))$ 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

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

definida por $\Psi(\varphi) = (\pi_H \circ \varphi, \pi_K \circ \varphi)$, es biyectiva.

Observación 1.13.1. *El orden de un elemento (h,k) de $H \times K$ es igual al mínimo de los múltiplos comunes de los órdenes de h y k. En efecto, dado que $(h,k)^n = (h^n, k^n)$, vale que $(h,k)^n = 1$ si y sólo si $h^n = 1$ y $k^n = 1$.*

Observación 1.13.2. *Supongamos que H y K son subgrupos normales de un grupo G y denotemos con $\pi_H\colon G \to G/H$ y $\pi_K\colon G \to G/K$ a las sobreyecciones canónicas. Por lo que acabamos de ver $(\pi_H, \pi_K)\colon G \to \frac{G}{H} \times \frac{G}{K}$ es un morfismo con núcleo igual a $H \cap K$. Afirmamos que este morfismo es sobreyectivo si y sólo si $HK = G$. Supongamos primero que se cumple esta condición y tomemos $(\overline{g}, \overline{g'}) \in \frac{G}{H} \times \frac{G}{K}$, donde $\overline{g}$ denota a la clase de $g \in G$ en G/H y $\overline{g'}$ a la de $g' \in G$ en G/K. Por hipótesis existen $h, h' \in H$ y $k, k' \in K$ tales que $g = hk$ y $g' = h'k'$ y así,*

$$(\pi_H(h'k), \pi_K(h'k)) = (\pi_H(k), \pi_K(h')) = (\pi_H(hk), \pi_K(h'k')) = (\overline{g}, \overline{g'}),$$

de modo de que la imagen de (π_H, π_K) es $\frac{G}{H} \times \frac{G}{K}$. Supongamos ahora que (π_H, π_K) es sobreyectivo. Entonces dado $g \in G$ existe $k \in G$ tal que $(\pi_H(k), \pi_K(k)) = (\pi_H, \pi_K)(k) = (\overline{g}, 1)$, donde $\overline{g}$ denota a la clase de $g \in G$ en G/H. Pero entonces $\pi_K(k) = 1$ y $\pi_H(k) = \pi_H(g)$ lo que significa que $k \in K$ y que existe $h \in H$ tal que $g = hk$.

Observación 1.13.3. *Si $f\colon H \to H'$ y $g\colon K \to K'$ son morfismos de grupos, entonces por la propiedad universal del producto directo queda definido un único morfismo de grupos $f \times g\colon H \times K \to H' \times K'$ tal que $\pi_{H'} \circ (f \times g) = f \circ \pi_H$ y $\pi_{K'} \circ (f \times g) = g \circ \pi_K$. Estas igualdades se expresan también diciendo que los cuadrados*

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

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

Observación 1.13.4. *Vale lo siguiente:*

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

Demostración. Se puede usar la propiedad universal del producto directo, pero también sale por cálculo directo. □

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

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

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

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

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

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

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 $\varphi(g) = 1$. Entonces $\pi(g) = \pi'(\varphi(g)) = 1$ y, por la exactitud de la primera fila, existe $h \in H$ tal que $g = i(h)$. Pero entonces $1 = \varphi(g) = \varphi(i(h)) = i'(h)$ y, como i' es inyectiva, $h = 1$. En consecuencia $g = i(h) = i(1) = 1$. Veamos ahora que φ es sobreyectiva. Tomemos $g' \in G'$. Como π es sobreyectiva existe $g \in G$ tal que $\pi(g) = \pi'(g')$. Por lo tanto $\pi'(\varphi(g)^{-1}g') = \pi(g)^{-1}\pi'(g') = 1$ y así, por la exactitud de la segunda fila, existe $h \in H$ tal que $\varphi(g)^{-1}g' = i'(h)$, de donde $g' = \varphi(g)i'(h) = \varphi(g)\varphi(i(h)) = \varphi(gi(h))$. Es fácil ver ahora que la relación definida entre sucesiones exactas cortas con extremos H y K, 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 1.13.5. *Si*

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

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

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

conmuta. En consecuencia π es una retracción.

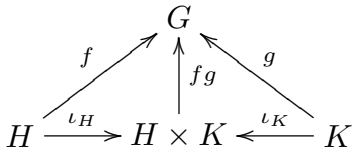
Demostración. Tomemos $\varphi = (r, \pi)$. Por definición

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

de modo de que el diagrama mencionado arriba conmuta. □

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

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



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

En efecto, estas igualdades fuerzan a que sea

$$(fg)(h, k) = (fg)((h, 1)(1, k)) = (fg)(\iota_H(h))(fg)(\iota_K(k)) = f(h)g(k).$$

Veamos que la aplicación fg es un morfismo de grupos:

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

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

Observación 1.13.6. *Supongamos que H y K son subgrupos de un grupo G y que los elementos de H conmutan con los de K (es decir que $hk = kh$ para todo $h \in H$ y $k \in K$). Por la propiedad universal que acabamos de ver existe un morfismo $\varphi \colon H \times K \to G$ que está definido por $\varphi(h, k) = hk$. Es claro que $\operatorname{Im}(\varphi) = HK$ y que $\operatorname{Ker}(\varphi) = \{(x, x^{-1}) : x \in H \cap K\} \simeq H \cap K$. En particular φ es un isomorfismo si y sólo si $HK = G$ y $H \cap K = \{1\}$.*

Teorema 1.13.7. *Si H y K son subgrupos normales de un grupo G son equivalentes:*

1) *$H \cap K = \{1\}$,*
2) *La aplicación $\phi \colon H \times K \to G$, definida por $\phi(h, k) = hk$ es un morfismo inyectivo.*

3) Cada elemento de HK se escribe de manera única como un producto hk con $h \in H$ y $k \in K$.

4) El 1 (que claramente está en HK) satisface la propiedad mencionada en el item 3).

Demostración. Veamos que 1) implica 2). Tomemos $h \in H$ y $k \in K$. Dado que H y K son normales, $h(kh^{-1}k^{-1}) = (hkh^{-1})k^{-1} \in H \cap K$ y así, por hipótesis, $hkh^{-1}k^{-1} = 1$, lo que implica que $hk = kh$. Por la Observación 1.13.6, la aplicación $\phi\colon H \times K \to G$, definida por $\phi(h,k) = hk$ es un morfismo inyectivo. Es claro que 2) implica 3) y 3) implica 4). Veamos ahora que 4) implica 1). Tomemos $g \in H \cap K$. Dado que el 1 de G se escribe como $1 = 1_H 1_K$ y $1 = gg^{-1}$ es $g = 1$. $\square$

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

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

definida por $\psi(g^{\alpha r}, g^{\beta s}) = g^{\alpha r}g^{\beta s} = g^{\alpha r+\beta s}$ 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 $\langle g\rangle$, $\langle g^\beta\rangle$ y $\langle g^\alpha\rangle$, respectivamente, y de que

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

Observación 1.13.8. *Combinando la Observación 1.13.2 y el Teorema 1.13.7 obtenemos que si H y K son subgrupos normales de un grupo G, entonces $H \cap K = \{1\}$ y $HK = G$ si y sólo si las aplicaciones*

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

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

Observación 1.13.9. *Supongamos que H, K y L son tres grupos. Es claro que las aplicaciones $\alpha\colon (H \times K) \times L \to H \times (K \times L)$ y $\beta\colon H \times K \to K \times H$, definidas por $\alpha((h,k),l) = (h,(k,l))$ y $\beta(h,k) = (k,h)$, son isomorfismos naturales de grupos. Esto último por definición significa que si $\phi\colon H \to H'$, $\varphi\colon K \to K'$ y $\psi\colon L \to L'$ son morfismos de grupos, entonces los diagramas*

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

conmutan.

Teorema 1.13.10. *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 todo $1 \leq i \leq n$.*
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). Hacemos la demostración 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 1.13.7, 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 $1 = h_1 \cdots h_{i-1} h_i^{-1}$ y así $h_i = 1$. □

Corolario 1.13.11. *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 $\phi(h_1, \ldots, h_n) = h_1 \cdots h_n$ 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, $|H_1 \cdots H_{i-1}|/|H_1| \cdots |H_{i-1}|$ 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 1.13.11, ϕ es un morfismo inyectivo. Es claro ahora que ϕ es un isomorfismo si y sólo si $|G| = |H_1| \cdots |H_n|$. □

1.14.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 K es otro grupo, podemos considerar los morfismos de grupos

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

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

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

y que ϕ sea un morfismo de grupos que

$$(kk') \cdot h = k \cdot (k' \cdot h) \quad \text{y} \quad 1 \cdot h = h \qquad \text{para todo } k, k' \in K \text{ y } h \in H.$$

Notemos qua las condiciones $k\cdot 1 = 1$ y $1\cdot h = h$ son redundantes. El producto cartesiano $H \times K$, con la operación

$$(h,k)(h',k') = (h(k\cdot h'), kk')$$

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

$$\big((h,k)(h',k')\big)(h'',k'') = (h(k\cdot h'), kk')(h'',k'') = \big(h(k\cdot h')((kk')\cdot h''), kk'k''\big)$$

y

$$(h,k)\big((h',k')(h'',k'')\big) = (h,k)(h'(k'\cdot h''), k'k'') = \big(h(k\cdot(h'(k'\cdot h'')), kk'k''\big),$$

que coinciden ya que

$$k\cdot(h'(k'\cdot h'') = (k\cdot h')(k\cdot(k'\cdot h'')) = (k\cdot h')((kk')\cdot h'').$$

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

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

y

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

Proposición 1.14.1. *Vale que:*

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

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

3) $(H \times \{1\}) \cap (\{1\} \times K) = \{1\}$ y $(H \times \{1\})(\{1\} \times K) = H \times_\phi K$,

4) Hay una sucesión exacta de morfismos de grupos

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

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

Demostración. 1) y 2) se siguen por cálculo directo, ya que

$$\begin{aligned}(h,k)(h',1)(h,k)^{-1} &= (h(k\cdot h'),k)(k^{-1}\cdot h^{-1}, k^{-1})\\ &= \big(h(k\cdot h')(k\cdot(k^{-1}\cdot h^{-1})), kk^{-1}\big)\\ &= \big(h(k\cdot h')((kk^{-1})\cdot h^{-1}), 1\big)\\ &= \big(h(k\cdot h')h^{-1}, 1\big)\end{aligned}$$

y

$$(1,k)(1,k') = (1(k\cdot 1), kk') = (1,kk').$$

3) Es claro que $(H \times \{1\}) \cap (\{1\} \times K) = \{1\}$ y que $(H \times \{1\})(\{1\} \times K) = H \times_\phi K$ se lo deduce de que $(h,1)(1,k) = (h(1\cdot 1),k) = (h,k)$.
4) Es inmediato que π y s son morfismos de grupos, que $\pi \circ s = \mathrm{id}_K$ 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. □

A continuación vamos a caracterizar la sucesiones exactas cortas

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

en las que π es una retracción. Supongamos por lo tanto que este es el caso y fijemos un morfismo $s\colon K \to G$ tal que $\pi \circ s = \mathrm{id}_K$. Llamemos $\phi\colon K \to \mathrm{Aut}(H)$ a la aplicación definida por $i(\phi(k)(h)) = s(k)i(h)s(k)^{-1}$ (notemos que $\pi(s(k)i(h)s(k)^{-1}) = \pi(s(k))\pi(i(h))\pi(s(k))^{-1} = k1k^{-1} = 1$ y que por lo tanto $s(k)i(h)s(k)^{-1} \in \mathrm{Im}(i)$). Es claro que $\phi(k)$ es un morfismo ya que

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

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

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

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

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

Proposición 1.14.2. *La aplicación $\varphi\colon H \times_\phi K \to G$, definida por*

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

es un morfismo de grupos que hace conmutativo al diagrama

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

En particular φ es un isomorfismo.

Demostración. Es claro que

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

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

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

como queríamos ver. □

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

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

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

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

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

Ejemplo. *Denotemos con $H=\langle x\rangle$ y $K=\langle y\rangle$ a dos grupos cíclicos de ordenes n y m respectivamente. Fijemos un entero r tal que $r^m\equiv 1 \pmod n$. Notemos que esto implica que r y n son coprimos. Para cada $0\le i<m$ consideremos la aplicación $\phi(y^i)\colon H\to H$ definida por $\phi(y^i)(a)=a^{r^i}$. Es claro que $\phi(y^i)$ es un morfismo de grupos dado que*

$$\phi(y^i)(ab)=(ab)^{r^i}=a^{r^i}b^{r^i}=\phi(y^i)(a)\phi(y^i)(b).$$

Además $\phi(y^i)$ es inyectiva ya que $a^{r^i}=\phi(y^i)(a)=1$ implica que $|a|$ divide a r^i y como $|a|$ divide a n y r^i y n son coprimos, de esto se sigue que $|a|=1$ y así $a=1$. Como H es finito $\phi(y^i)$ también es sobreyectiva. Afirmamos que la aplicación

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

es un morfismo de grupos. En efecto

$$\phi(y^i y^j)(a) = \phi(y^{i+j})(a) = a^{r^{i+j}} = (a^{r^j})^{r^i} = \phi(y^i)(\phi(y^j)(a)),$$

donde la segunda igualdad se sigue de que si $i + j \geq m$ *y denotamos con* $r_m(i + j)$ *al resto de la división de* $i + j$ *por* m*, entonces*

$$\phi(y^{i+j})(a) = a^{r^{r_m(i+j)}} = a^{r^m r^{r_m(i+j)}} = a^{r^{m+r_m(i+j)}} = a^{r^{i+j}},$$

siendo la segunda igualdad verdadera debido a que $r^m \equiv 1 \pmod{n}$ *y* $a^n = 1$*. Podemos entonces considerar el producto semidirecto* $H \times_\phi K$*. Escribamos* $\overline{x}$ *en lugar de* $(x, 1)$ *e* $\overline{y}$ *en lugar de* $(1, y)$*. Claramente* $H \times_\phi K$ *está generado por* $\overline{x}$ *e* $\overline{y}$ *y además* $\overline{x}^n = 1$*,* $\overline{y}^m = 1$ *y* $\overline{yx} = \overline{x}^r \overline{y}$*. Notemos finalmente que todo esto se puede generalizar facilmente al caso caso en que* H *es un grupo abeliano finito de exponente* n*.*

Observación 1.14.3. *Supongamos que tenemos una equivalencia de extensiones*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\iota_H} & H \times_\phi K & \xrightarrow{\pi_K} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_H} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{id}_K} & & \\ 1 & \longrightarrow & H & \xrightarrow{\iota_H} & H \times_\psi K & \xrightarrow{\pi_K} & K & \longrightarrow & 1 \end{array}$$

Por la conmutatividad del segundo cuadrado,

$$\pi_K(\varphi(1, k)) = \pi_K(1, k) = k$$

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

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

tenemos que

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

Así

$$\varphi\big((h, k)(h', k')\big) = \varphi\big(h(k \cdot_\phi h'), kk'\big) = \big(h(k \cdot_\phi h')f(kk'), kk'\big)$$

y

$$\varphi(h, k)\varphi(h', k') = (hf(k), k)(h'f(k'), k') = \big(hf(k)(k \cdot_\psi (h'f(k'))), kk'\big).$$

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

$$(k \cdot_\phi h')f(kk') = f(k)(k \cdot_\psi (h'f(k'))).$$

Tomando $h' = 1$ *y* $k' = 1$ *obtenemos respectivamente que*

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

Notemos que lo primero implica que $f(1) = 1$*, ya que tomando* $k = k' = 1$ *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 valen estas dos condiciones, entonces*

$$(k \cdot_\phi h')f(kk') = (k \cdot_\phi h')f(k)(k \cdot_\psi f(k')) = f(k)(k \cdot_\psi h')(k \cdot_\psi f(k')) = f(k)(k \cdot_\psi (h'f(k'))).$$

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

$$\phi(k)(h') = f(k)\psi(k)(h')f(k),$$

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

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 disjuntos 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 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.

Escribamos una permutación σ como un producto de ciclos disjuntos dos a dos $\sigma = \sigma_1 \circ \cdots \circ \sigma_s$ y denotemos con r_j al orden de σ_j con $1 \leq j \leq s$. Podemos suponer que $r_1 \leq r_2 \leq \cdots \leq r_s$. Claramente $r_1 + \cdots + r_s < n$ 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 $r_1 + \cdots + r_s < n$ 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.*

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

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

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 $i \in X \setminus \{i_1, \ldots, i_s\}$, entonces $\tau \circ \sigma \circ \tau^{-1} = \sigma'$. □

Por el teorema anterior cada clase de conjugación de S_n se corresponde con la estructura cíclica $(\alpha_1, \ldots, \alpha_n)$ 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 $\alpha_1, \ldots, \alpha_n \geq 0$ que satisfacen $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n$. Para $1 \leq j \leq n$, escribamos $\mu_j = \alpha_j + \cdots + \alpha_n$. 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 $(1,1,1,1,1)$, $(2,1,1,1)$, $(2,2,1)$, $(3,1,1)$, $(3,2)$, $(4,1)$, (5) 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 $(\alpha_1, \ldots, \alpha_n)$ es

$$(*) \qquad \frac{n!}{1^{\alpha_1}\alpha_1!2^{\alpha_2}\alpha_2! \ldots n^{\alpha_n}\alpha_n!}.$$

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

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

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

2.2.Generadores de S_n. Un cálculo directo muestra que

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

y

$$(1, i_1) \circ (1, i_j) \circ (1, i_1) = (i_1, i_j).$$

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

$$(i, i+1) \circ (1, i) \circ (i, i+1) = (1, i+1),$$

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 $1 \leq i \leq n-1$, 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

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

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

Demostración. Es claro que sg es sobreyectiva ya que $\operatorname{sg}(\mathrm{id}) = 1$ y $\operatorname{sg}(1, 2) = -1$. 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 $\operatorname{sg}(\tau \circ \sigma) = \operatorname{sg}(\tau) \operatorname{sg}(\sigma)$. 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, $\operatorname{sg}(\tau \circ \sigma) = (-1)^{n-s-1} = (-1)^{n-(n-1)}(-1)^{n-s} = \operatorname{sg}(\tau) \operatorname{sg}(\sigma)$. 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, $\operatorname{sg}(\tau \circ \sigma) = (-1)^{n-s+1} = (-1)^{n-(n-1)}(-1)^{n-s} = \operatorname{sg}(\tau) \operatorname{sg}(\sigma)$. 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

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

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*

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

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. □

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 a A_n. Afirmamos 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 demostracińn 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 $(1,2,l)$, con $3 \leq l \leq n$, 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 $n \geq 3$. □

Proposición 2.3.7. *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. Por último, dado que $(H \cap A_n) \cap \{\mathrm{id}, \sigma\} = \{\mathrm{id}\}$ y $(H \cap A_n)\{\mathrm{id}, \sigma\} = H$, tenemos que H es el producto semidirecto de $H \cap A_n$ y $\{\mathrm{id}, \sigma\}$. □

Proposición 2.3.8. *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-ciclo 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 2.3.7, $H \cap A_4$ es un subgrupo de orden 6 de A_4, lo que que contradice 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 $[\mathrm{S}_n, \mathrm{S}_n] \subseteq A_n$. 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. *Dado que* A_3 *es abelino, tenemos que* $[A_3, A_3] = 1$. *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, $\sigma = (i_1, i_2, \dots) \circ (j_1, j_2, \dots) \circ \dots$, 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 $n \geq 5$. Supongamos que $H \neq \{1\}$ es un subgrupo normal de A_n y tomemos $\sigma \in A_n$ distinto de la identidad. 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.

1) Si $\sigma = (i_1, i_2, \dots) \circ (j_1, j_2, \dots) \circ \dots$ 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 debidio 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 2.3.8 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 propio 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 2.3.7, 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. □

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) $(gg')\cdot x = g\cdot(g'\cdot x)$, para todo $g, g' \in G$ y $x \in X$.

2) $1\cdot x = x$, para todo $x \in X$,

donde hemos escrito $g \cdot x$ en lugar de $\rho(g, x)$. 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 $\widetilde{\rho}(g)(x)=\rho(g,x)$ y dada $\widetilde{\rho}$ podemos definir ρ por $\rho(g,x)=\widetilde{\rho}(g)(x)$ y evidentemente ambas construcciones son recíprocas una de la otra. Ahora la condición 1) dada arriba es claramente equivalente a que $\widetilde{\rho}(gg')=\widetilde{\rho}(g)\circ\widetilde{\rho}(g')$ y la 2) a que $\widetilde{\rho}(1)=\mathrm{id}$. De esto se sigue que $\widetilde{\rho}(g)$ es biyectiva para cada g, ya que $\widetilde{\rho}(g^{-1})\circ\widetilde{\rho}(g)=\widetilde{\rho}(1)=\mathrm{id}$ 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 $\widetilde{\rho}(gg')=\widetilde{\rho}(g)\circ\widetilde{\rho}(g')$ 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) $x\cdot(gg')=(x\cdot g)\cdot g'$, para todo $g,g'\in G$ y $x\in X$.
2) $x=x\cdot 1$, para todo $x\in X$,

donde $x\cdot g$ signfica $\rho(x,g)$ 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 $\rho^{\mathrm{op}}(g,x)=\rho(x,g)$. 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 $\widetilde{\rho}(gg')=\widetilde{\rho}(g')\circ\widetilde{\rho}(g)$. 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 $\mathrm{Ker}(\rho)=\{g\in G : g\cdot x=x \text{ para todo } x\in X\}$. 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 $\overline{g}\cdot x=g\cdot x$, donde $\overline{g}$ denota a la clase de elemento $g\in G$ en $G/\mathrm{Ker}(\rho)$ (esta definición es correcta ya que si $h\in\mathrm{Ker}(\rho)$, entonces $(gh)\cdot x=g\cdot(h\cdot x)=g\cdot x$). 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 $g\cdot(g'H)=gg'H$. El núcleo de esta acción es el máximo subgrupo $N=\bigcap_{g\in G}gHg^{-1}$ 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 $\widetilde{\rho}(\sigma)(\tau)=\sigma\circ\tau$, 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 Obsevación 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. Entonces para todo $\sigma \in G$ vale que 2^k divide a $|\sigma|$ si y sólo si $\widetilde{\rho}(\sigma) \notin A_n$. En consecuencia si G tiene un elemento σ de orden $2^k m'$ con m' un divisor positivo de m, entonces G tiene un subgrupo de índice 2.*

Demostración. Supongamos que $|\sigma| = 2^{k'} m'$ con $0 \leq k' \leq k$ y m' un divisor positivo de m. Por su definición, $\widetilde{\rho}(\sigma)$ 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 $k' = k$, tenemos que $\widetilde{\rho}(\sigma) \notin A_n$ si y sólo si $k' = k$. Así, si G tiene un elemento σ de orden $2^k m'$ con m' un divisor positivo de m, entonces por la Proposición 2.3.7, $\widetilde{\rho}(G)$ (y por lo tanto también G) tiene un subgrupo de índice 2. □

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

Corolario 3.1.5. *Supongamos que G es un grupo finito y que $|G| = mn$. Todo subgrupo H de orden m 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 o que los que aparecen en la de $(n-1)!$, 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 divide a $n!$. Dado que $|G : N|$ también divide a $|G| = nm$ y que $n = |G : H|$ divide a $|G : N|$, tenemos que $|G : N| = nh$, donde h es un divisor de $\mathrm{mdc}((n-1)!, m)$. □

Corolario 3.1.6. *Supongamos que G es un grupo finito y que $|G| = pn$ con p primo mayor o igual que n, entonces todo subgrupo H de orden p de G es normal.*

Corolario 3.1.7. *Supongamos que G es un grupo finito y denotemos con p al mínimo primo que divide a $|G|$. Todo subgrupo H 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 $g \cdot y \in Y$ para todo $g \in G$ 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 $f(g \cdot x) = g \cdot f(x)$ para todo $g \in G$ 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 semigrupo 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 $g \cdot x = x$ para todo $g \in G$ 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 $g \cdot x = gxg^{-1}$. 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 $g \cdot x = gxg^{-1}$. 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 $g \cdot x = gxg^{-1}$. 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 $h \cdot g = hg$ para todo $h \in H$ y todo $g \in G$. 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 $g \cdot X = gXg^{-1}$. 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 el conjunto $P(G)$ de los subconjuntos de G por traslaciones a izquierda, es decir que $g \cdot X = gX$. Esta acción es claramente fiel.*

Ejemplo 8. *G actúa sobre el conjunto $G \backslash H$ de las coclases a derecha de un subgrupo suyo H via $g(Hg') = Hg'g^{-1}$. El núcleo de esta acción es el máximo subgrupo $N = \bigcap_{g \in G} gHg^{-1}$ de H que es normal en G.*

Ejemplo 9. *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 10. *$\mathrm{GL}(n, k)$ 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 11. *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 12. 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 $g \in G$ tal que $g\cdot x = y$. 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 $\mathcal{O}_x = \{g\cdot x : g \in G\}$ y $\mathcal{O}_x = \mathcal{O}_y$ si y sólo si x e y son conjugados. Decimos que $x \in X$ es un *punto fijo* si $g\cdot x = g$ para todo $g \in G$, 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

$$\#(X) = \sum_{x\in X'} \#(\mathcal{O}_x) = \#(\mathrm{PF}(X)) + \sum_{x\in X'\setminus \mathrm{PF}(X)} \#(\mathcal{O}_x). \tag{3}$$

Decimos que un G-espacio X es *transitivo* 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 $G_x = \{g \in G : g\cdot x = x\}$. Es evidente que G_x es un subgrupo de G y que el núcleo de la acción de G sobre X es la intersección $\bigcap_{x\in X} G_x$ de los estabilizadores de todos los elementos de X.

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

Demostración. Tomemos $h \in G_x$. Entonces

$$(ghg^{-1})\cdot y = g\cdot(h\cdot(g^{-1}\cdot y)) = g\cdot(h\cdot x) = g\cdot x = y$$

y así $gG_xg^{-1} \subseteq G_y$. Por simetría $g^{-1}G_yg \subseteq G_x$, de donde $G_y \subseteq gG_xg^{-1}$. □

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

Teorema 3.1.10. *Supongamos que* X *es un* G*-espacio y tomemos* $x \in X$*. Consideremos a* G/G_x *como* G*-espacio via* $g\cdot g'G_x = gg'G_x$*. La aplicación* $\Phi\colon G/G_x \to \mathcal{O}_x$*, definida por* $\Phi(gG_x) = g\cdot x$ *es un isomorfismo de* G*-espacios.*

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

Corolario 3.1.11. *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 3.1.12. *Si k es un cuerpo finito que tiene q elementos, entonces el orden de* $\mathrm{GL}(n,k)$ *es* $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

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 3.1.11 con la fórmula (3) obtenemos que

$$\#(X)=\sum_{x\in X'}|G:G_x|=\#(\mathrm{PF}(X))+\sum_{x\in X'\setminus\mathrm{PF}(X)}|G:G_x|, \tag{4}$$

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

Veamos que nos dice todo esto en algunos de 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 $G_x=\mathrm{C}_G(x)$ para todo $x\in G$, de manera de que el orden de la clase de conjugación de $x\in G$ es $|G:\mathrm{C}_G(x)|$ y así, si G es finito, divide al orden de G. Además la fórmula (4) queda

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

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 $G_x=\mathrm{C}_G(x)$ para todo $x\in H$, de manera que el orden de la clase de conjugación de $x\in H$ es $|G:\mathrm{C}_G(x)|$ y así, si G es finito, divide al orden de G. Además la fórmula (4) queda

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

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 orden 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 (4) 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 $gSg^{-1} = S$ para todo $g \in G$, y $G_S = \mathrm{N}_G(S)$ para todo subconjunto S de G, de manera de que el orden 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 (4) 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 $G_{gH} = gHg^{-1}$ para toda coclase gH. La fórmula (4) en este caso es trivial.

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

Teorema 3.1.13. *Si X es un G-conjunto finito, entonces la cantidad N de órbitas de X es*

$$N = \frac{1}{|G|} \sum_{g \in G} \#(\mathrm{PF}_g(X)),$$

donde $\mathrm{PF}_g(X) = \{x \in X : g{\cdot}x = x\}$.

Demostración. En $\sum_{g \in G} \#(\mathrm{PF}_g(X))$ cada $x \in X$ es contado $|G_x|$ veces (pues G_x consiste de todos los $g \in G$ tales que $x \in \mathrm{PF}_g(X)$). 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 ellos son contados en total $|G| = |G : G_x||G_x|$ veces. Recorriendo todas las órbitas de X obtenemos así que $\sum_{g \in G} \mathrm{PF}_g(X) = N|G|$. □

Ejemplo. *La cantidad c de clases de conjugación de un grupo finito G es*

$$c = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{C}_G(g)|,$$

En efecto, para la acción de conjugación,

$$\mathrm{PF}_g(G) = \{x \in G : gxg^{-1} = x\} = \{x \in G : x^{-1}gx = g\} = \mathrm{C}_G(g).$$

Corolario 3.1.14. *Si X es un G-conjunto finito y transitivo y $\#(X) > 1$, entonces existe $g \in G$ tal que $\mathrm{PF}_g(X) = \emptyset$.*

Demostración. Dado que X es transitivo la cantidad de órbitas es 1. Así, por el Teorema 3.1.13, $|G| = \sum_{g\in G} \#(\mathrm{PF}_g(X))$ y, como $\#(\mathrm{PF}_1(X)) = \#(X) > 1$, debe existir $g \in G$ tal que $\mathrm{PF}_g(X) = \emptyset$. □

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. Hacemos la demostración por inducción en $|G|/p$. El caso $|G|/p = 1$ es obvio. Para el paso inductivo tomemos $x \in G$ de orden $|x| > 1$. Si p divide a $|x|$, entonces $x^{|x|/p}$ tiene orden p. Si no, p divide a $|G/\langle x\rangle|$ y, por hipótesis inductiva, existe $y \in G$, tal que su clase $\overline{y}$ en $G/\langle x\rangle$ tiene orden p. Pero entonces el orden $|y|$ de y es múltiplo de p e $y^{|y|/p}$ 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 $|HP : P| = |H : P \cap H|$, de donde se sigue facilmente que HP es un p-subgrupo de G. Como P es un p-subgrupo maximal de G, tenemos 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. Hacemos la demostración 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

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

se sigue entonces que p divide a $|\,\mathrm{Z}(G)|$. Por el Lema 3.2.1 existe $x \in \mathrm{Z}(G)$ de orden p. Como $x \in \mathrm{Z}(G)$ el subgrupo $\langle x\rangle$ de G es normal. Tomemos un p-subgrupo de Sylow P' de $G/\langle x\rangle$ y escribamos $P = \pi^{-1}(P')$, donde $\pi\colon G \to G/\langle x\rangle$ es el epimorfismo canónico. Dado que $\langle x\rangle \subseteq P$ y que π aplica P sobre P' tenemos la sucesión exacta corta

$$1 \longrightarrow \langle x\rangle \longrightarrow P \xrightarrow{\pi} P' \longrightarrow 1$$

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

$$\mathrm{PF}_H(X) = \{xPx^{-1} : H \subseteq \mathrm{N}_G(xPx^{-1})\} = \{xPx^{-1} : H \subseteq xPx^{-1}\},$$

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 3.1.11, el cardinal de cada órbita no trivial de X es una potencia positiva de p. Así,

$$\{xPx^{-1} : H \subseteq xPx^{-1}\} \equiv \#(X) \pmod p.$$

Tomando $H = P$ en esta igualdad vemos que $\#(X) \equiv 1 \pmod p$, puesto que $\{xPx^{-1} : P \subseteq xPx^{-1}\} = \{P\}$. En consecuencia

$$\{xPx^{-1} : H \subseteq xPx^{-1}\} \equiv 1 \pmod p.$$

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 corolarioanterior y de que $|G : \mathrm{N}_G(P)|$ divide a $|G : P| = m$. □

Corolario 3.2.6. *Un grupo finito G tiene sólo un p-subgrupo de Sylow P si y sólo si P es normal.*

Demostración. Si G tiene sólo un p-subgrupo de Sylow P, entonces P es normal en G ya que todo conjugado de P es también un p-subgrupo de Sylow de G. Recíprocamente, si P es un p-subgrupo de Sylow normal de G, entonces es único, ya que todos los p-subgrupos de Sylow de G son conjugados. □

Observación 3.2.7. *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 $|PH/H| = |P/(H \cap P)|$ y $|G/H : HP/H| = |G : HP|$. 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 3.2.8. *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*

$$\frac{\#(\mathrm{Syl}_p(G))}{\#(\mathrm{Syl}_p(H))} = \frac{|\,\mathrm{N}_G(P_H)|}{|\,\mathrm{N}_G(P)|} = \frac{|G:H||\,\mathrm{N}_H(P_H)|}{|\,\mathrm{N}_G(P)|}.$$

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 3.2.9. *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 3.2.7,

$$\#(\mathrm{Syl}_p(G/H)) = \#(\{PH/H : P \in \mathrm{Syl}_p(G)\}),$$

tenemos que $\#(\mathrm{Syl}_p(G/H))$ divide a $|G : \mathrm{N}_G(P)| = \#(\mathrm{Syl}_p(G))$. □

Proposición 3.2.10. *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, entonces $\mathrm{N}_G(H) = H$.*

Demostración. Supongamos que $x \in G$ satisface $xHx^{-1} = H$. Entonces P y xPx^{-1} son p-subgrupos de Sylow de H y, como todos los p-subgrupos de Sylow de H son conjugados, existe $y \in H$ tal que $yxPx^{-1}y^{-1} = P$. En consecuencia $yx \in \mathrm{N}_G(P) \subseteq H$, de dónde $x = y^{-1}yx \in H$. □

3.3.Aplicaciones de los teoremas de Sylow. A continuación damos unas pocas aplicaciones de los teoremas de Sylow.

Teorema 3.3.1 (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 $x \neq 1$ en P donde P es un p-subgrupo de Sylow de G. Entonces $|x| = p^\alpha$ con $\alpha \geq 1$ y así $x^{p^{\alpha-1}}$ tiene orden p. □

Corolario 3.3.2. *Un grupo finito es un p-grupo si y sólo si el orden de cada uno de sus elementos es una potencia de p.*

Como aplicación del teorema de Cauchy vamos a caracterizar los grupos de orden pq con p y q primos distintos.

Proposición 3.3.3. *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 de Cauchy 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 1.13.11, $G \simeq \langle x\rangle \times \langle z\rangle \simeq \mathbb{Z}_{pq}$. 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 $yxy^{-1} = z^\alpha x z^{-\alpha} = x^{r^\alpha} = x^{r_0}$. □

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 último de los ejemplos que aparecen en la sección 1.14 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 resta de esta sección denotaremos con n_p a la cantidad de p-subgrupos de Sylow de un grupo finito G.

Proposición 3.3.4. *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. □

Proposición 3.3.5. *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 $(G \setminus S) \cup \{1\}$. □

Otros ejemplos.

1) *No existen subgrupos simples G de orden $36 = 2^2 3^2$. Tomemos un 3-subgrupo de Sylow de G. Por el Teorema 3.1.4, P contiene un subgrupo normal P', cuyo índice divide a $4! = 24 < 36$.*
2) *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.*

3.4.p-grupos finitos. Denotemos con p a un número primo. En esta sección probaremos algunas propiedades básicas de los p-grupos finitos.

Teorema 3.4.1. *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

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

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 $|G : \mathrm{C}_G(x)|$ 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 3.4.2. *Todo subgrupo normal de orden p de un p-grupo G está incluído en el centro de $|G|$.*

Corolario 3.4.3. *Si $|G| = p^\alpha$, entones toda cadena*

$$0 = G_0 \subseteq G_{i_1} \subseteq G_{i_2} \subseteq \cdots \subseteq G_{i_r} \subseteq G_\alpha = G$$

de subgrupos normales de G con $1 \leq i_1 < i_2 < \cdots < \alpha$ y $|G_{i_j}| = p^{i_j}$ se puede completar a una cadena

$$0 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_{\alpha-1} \subseteq G_\alpha = G$$

de subgrupos normales de G con $|G_j| = p^j$. En particular G tiene un subgrupo normal de orden p^j para cada $1 \leq j \leq \alpha$.

Demostración. Por inducción en α. Tomando $x \in \mathrm{Z}(G) \cap G_{i_1}$ de orden p obtenemos un subgrupo normal $G_1 = \langle x \rangle$ de orden 1 de G incluído en G_{i_1}. Supongamos ahora que el resultado vale para p-grupos de orden menor que p^α. Consideremos la sobreyección canónica $\pi\colon G \to G/\langle x \rangle$. Por hipótesis inductiva la cadena

$$0 = \overline{G}_0 \subseteq \overline{G}_{i_1} \subseteq \overline{G}_{i_2} \subseteq \cdots \subseteq \overline{G}_{i_r} \subseteq \overline{G}_\alpha = G,$$

donde $\overline{G}_j$ denota a $\pi(G_j)$ se puede extender a una cadena

$$0 = \overline{G}_0 \subseteq \overline{G}_1 \subseteq \overline{G}_2 \subseteq \cdots \subseteq \overline{G}_{\alpha-1} \subseteq \overline{G}_\alpha$$

con $|\overline{G}_j| = p^{j-1}$, para $1 \leq 1 \leq \alpha$. Es claro que la cadena

$$0 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_{\alpha-1} \subseteq G_\alpha = G$$

obtenida tomando $G_j = \pi^{-1}(\overline{G}_j)$, para $1 \leq 1 \leq \alpha$, satisface las condiciones pedidas en el enunciado. □

Corolario 3.4.4. *Todo grupo G de orden p^2 es abeliano.*

Demostración. Supongamos que G no fuera abeliano. Debido a esto y al Teorema 3.4.1, $\mathrm{Z}(G)$ tiene orden p y así $G/\mathrm{Z}(G)$ también tiene orden p. Pero entonces es cíclico, lo que contradice la Proposición 1.12.1. □

Corolario 3.4.5. *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 3.4.1, $\mathrm{Z}(G) \neq \{1\}$ y dado que G no es abeliano, $\mathrm{Z}(G) \neq G$. Además por la Proposición 1.12.1, $G/\mathrm{Z}(G)$ no es cíclico. Por lo tanto su orden es al menos p^2 y así $|\mathrm{Z}(G)| = p$. Como, por el Corolario 3.4.4, $G/\mathrm{Z}(G)$ 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 3.4.2, $\mathrm{Z}(G)$ es el único subgrupo invariante de G de orden p. □

Teorema 3.4.6. *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 entonces 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 conjugaión 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 gHg^{-1}. Entonces $hgHg^{-1}h^{-1} = gHg^{-1}$ para todo $h \in H$, lo que implica que $g^{-1}hg \in \mathrm{N}_G(H)$ para todo $h \in H$. Pero como $gHg^{-1} \neq H$ algún $g^{-1}hg$ no está en H. □

Corolario 3.4.7. *Si H es un subgrupo maximal de un p-grupo finito G, entonces H es normal en G y su índice es p.*

Demostración. Por el Teorema 3.4.6 o el Corolario 3.1.7, H es normal y G/H no tiene subgrupos no triviales. Así, por el Corolario 3.4.3, $|G/H| = p$. □

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 el número 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 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 $A(A' \cap B) \lhd A(A' \cap B')$, $(A \cap B')(A' \cap B) \lhd A' \cap B'$ 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 $G_{ij}/G_{i-1,j} \simeq H_{ij}/H_{i,j-1}$, 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 $H/(H \cap L) \simeq HL/L$. □

4.2.Grupos resolubles. Una serie normal de un grupo G es *resoluble* si sus grupos factores son conmutativos. Un grupo G es *resoluble* si tiene una serie resoluble. Claramente 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.

Teorema 4.2.2. *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 4.2.3. *Si*

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

es una una sucesión exácta corta de grupos, entonces G es resoluble si y sólo si G' y G'' lo son.

Demostración. Supongamos que G es resoluble. Por el teorema anterior sabemos que G' lo es. Para comprobar que también lo es G'', 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

$$\frac{\pi(G_{i+1})}{\pi(G_i)} \simeq \frac{i(G')G_{i+1}}{i(G')G_i} = \frac{i(G')G_iG_{i+1}}{i(G')G_i} \simeq \frac{G_{i+1}}{i(G')G_i \cap G_{i+1}} \simeq \frac{G_{i+1}/G_i}{(i(G')G_i \cap G_{i+1})/G_i},$$

que es conmutativo. Reciprocamente, si $\{1\} = G'_0 \lhd G'_1 \lhd \cdots \lhd G'_n = G'$ es una serie resoluble de G' y $\{1\} = G''_0 \lhd G''_1 \lhd \cdots \lhd G''_m = G''$ es una serie resoluble de G'', entonces

$$\{1\} = i(G'_0) \lhd i(G'_1) \lhd \cdots \lhd i(G'_n) = G' = \pi^{-1}(G''_0) \lhd \pi^{-1}(G''_1) \lhd \cdots \lhd \pi^{-1}(G''_m) = G$$

es una serie resoluble de G. □

Teorema 4.2.4. *Supongamos que H y L 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 $H/(H \cap L) \simeq HL/L$. □

Corolario 4.2.5. *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 4.2.6. *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 4.2.3, tampoco S_n lo es. □

Definición 4.2.7. *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 $G^{i+1} = [G^{(i)}, G^{(i)}]$.

Teorema 4.2.8. *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. Hacemos inducción en i. El caso $i = 0$ es trivial. Supongamos que el resultado vale para i, de manera 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 4.2.9. *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 dice el teorema anterior es que la serie derivada de un grupo es una serie normal si y sólo si el grupo es resoluble.

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

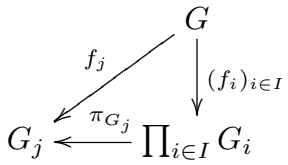
$$(g_i)_{i\in I}(g_i')_{i\in I} = (g_i g_i')_{i\in I}$$

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 $\pi_{G_j} \circ (f_i)_{i\in I} = f_j$.

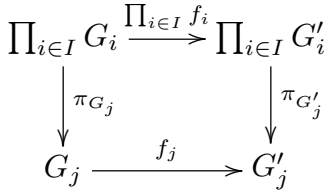
En efecto, estas igualdades fuerzan a que sea $(f_i)_{i\in I}(x) = (f_i(x))_{i\in I}$ y es claro que con esta definición $(f_i)_{i\in I}$ es un morfismo de grupos que satisface las igualdades mencionadas arriba. El claro también que $\operatorname{Ker}((f_i)_{i\in I}) = \bigcap_{i\in I} \operatorname{Ker}(f_i)$.

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*

$$\mathrm{Ker}\Big(\prod_{i\in I} f_i\Big) = \prod_{i\in I} \mathrm{Ker}(f_i) \quad e \quad \mathrm{Im}\Big(\prod_{i\in I} f_i\Big) = \prod_{i\in I} \mathrm{Im}(f_i).$$

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*

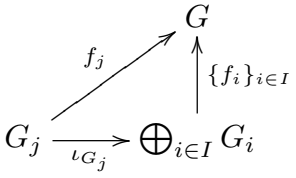
$$\prod_{i\in I} \pi_i\colon \prod_{i\in I} G_i \to \prod_{i\in I} \frac{G_i}{H_i}$$

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 $i_1,\dots,i_n$ es una subfamilia arbitraria de elementos de I y g_{i_j} pertenece a G_{i_j} para todo $1\le j\le n$. 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 $i_1, \ldots, i_n$ es una subfamilia arbitraria de elementos de I y h_{i_j} pertenece a H_{i_j} para todo $1 \leq j \leq n$. 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 $i_1, \ldots, i_n$ es una subfamilia arbitraria de elementos de I y h_{i_j} pertenece a $H_{i_j} \setminus \{1\}$ para todo $1 \leq j \leq n$.*
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 $i_1, \ldots, i_n$ una subfamilia arbitraria de elementos de $I\setminus\{j\}$ y h_{i_j} pertenece a H_{i_j} para todo $1 \leq j \leq n$.*

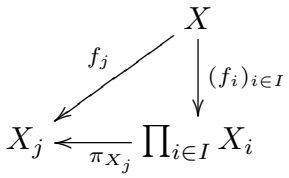
Es claro por definición que los items 1) y 2) son equivalentes y que el 3) es equivalente a que $\ker(\varphi) = \{1\}$. Veamos que 3) implica 4). Si existieran $h_i \neq 1$ en H_i y $h_{i_1} \in H_{i_1}, \ldots, h_{i_n} \in H_{i_n}$ con $i \notin \{i_1, \ldots, i_n\}$ tales que $h_i = h_{i_1}\cdots h_{i_n}$, 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 $n \geq 1$ e $i_1, \ldots, i_n$ es una subfamilia arbitraria de elementos de I y $h_{i_j} \neq 1$ pertenece a H_{i_j} para todo $1 \leq j \leq n$, entonces claramente $n \geq 2$ 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 1.13.7 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 $\pi_{X_j}\circ(f_i)_{i\in I} = f_j$.

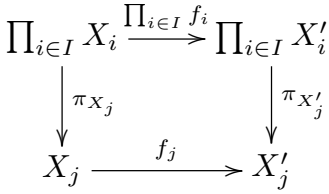
En efecto, estas igualdades fuerzan a que sea $(f_i)_{i\in I}(x) = (f_i(x))_{i\in I}$ y es claro que con esta definición $(f_i)_{i\in I}$ es un morfismo de G-conjuntos que satisface las igualdades mencionadas arriba.

Notemos que lo que la propiedad universal del producto directo dice es simplemente que para todo G-conjunto X, la aplicación

$$\Psi\colon \mathrm{Hom}_G\Big(X, \prod_{i\in I} X_i\Big) \to \prod_{i\in I} \mathrm{Hom}_G(X, X_i),$$

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*



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* $\left(\prod_{i\in I} f_i'\right) \circ \left(\prod_{i\in I} f_i\right) = \prod_{i\in I}(f_i' \circ f_i)$.

Demostración. Se puede usar la propiedad universal del producto directo, pero también sale por cálculo directo. □

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

$$\begin{array}{ccc} & & X \\ & \overset{f_j}{\nearrow} & \uparrow{\scriptstyle \{f_i\}_{i\in I}} \\ X_j & \xrightarrow[i_{X_j}]{} & \bigsqcup_{i\in I} X_i \end{array}$$

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

$$\Psi\colon \mathrm{Hom}_G\Big(\bigsqcup_{i\in I} X_i, X\Big) \to \prod_{i\in I} \mathrm{Hom}_G(X_i, X),$$

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* $\left(\bigsqcup_{i\in I} f_i\right) \circ i_{X_j} = i_{X_j'} \circ f_j$ *para todo* $j \in I$. *Estas igualdades se expresan también diciendo que los cuadrados*

$$\begin{array}{ccc} X_j & \xrightarrow{f_j} & X_j' \\ \downarrow{\scriptstyle i_{X_j}} & & \downarrow{\scriptstyle i_{X_j'}} \\ \bigsqcup_{i\in I} X_i & \xrightarrow{\bigsqcup_{i\in I} f_i} & \bigsqcup_{i\in I} X_i' \end{array}$$

conmutan. Es claro que $\left(\bigsqcup_{i\in I} f_i\right)(x) = f_i(x)$ *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* $\left(\bigsqcup_{i\in I} f_i'\right) \circ \left(\bigsqcup_{i\in I} f_i\right) = \bigsqcup_{i\in I}(f_i' \circ f_i)$.

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 subgrupo 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, 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 1.12.2, 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 3.2.2 y 5.6.2, todo grupo finito, característicamente simple y resoluble, es elemental abeliano.