Grupos

Andrés Abella

10 de mayo de 2020

Índice

1. Divisibilidad

En esta sección repasamos brevemente algunos conceptos de divisibilidad en el conjunto de los números enteros $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$, que necesitamos para el estudio de los grupos.

Proposición 1.1 (División entera)**.** *Dados $a, d \in \mathbb{Z}$ con $d > 0$, existen únicos $q, r \in \mathbb{Z}$ tales que $a = dq + r$ y $0 \leq r < d$. El entero q es el* cociente *y r es el* resto *de* dividir *a por d.*

Dem. Si consideramos $q = \max\{n \in \mathbb{Z} : \ dn \leq a\}$ y $r = a - dq$, entonces vale $a = dq + r$ y $r \geq 0$. Si fuese $r \geq d$, entonces sería $a = dq + r \geq d(q+1)$ contradiciendo la maximalidad de q; luego es $r < d$. Esto prueba la existencia.
Si hubiesen otros enteros $q', r' \in \mathbb{Z}$ tales que $a = dq' + r'$ y $0 \leq r' < d$, entonces sería $dq + r = dq' + r'$ y por lo tanto $d(q - q') = r' - r$. Tomando valor absoluto obtenemos $d|q - q'| = |r' - r| < d$. Si fuese $q \neq q'$, entonces sería $d|q - q'| \geq d$ lo cual nos lleva a una contradicción. Luego es $q = q'$ lo cual implica $r = r'$. $\square$

Si $a, b \in \mathbb{Z}$, decimos que *a divide* a b y escribimos $a \mid b$ si existe $c \in \mathbb{Z}$ tal que $b = ac$. Un entero $a \neq \pm 1$ es *primo* si $b \mid a$ implica $b = \pm a$ o $b = \pm 1$.
Se prueba que dados $a, b \in \mathbb{Z}$ no ambos nulos, siempre existe su *máximo común divisor* $d = \mathrm{mcd}(a, b) \in \mathbb{Z}$ que queda caracterizado por las siguientes condiciones

$$d > 0; \quad d \mid a \text{ y } d \mid b; \quad \text{si } c \mid a \text{ y } c \mid b, \text{ entonces } d \mid c.$$

Observaciones 1.2. A continuación recordamos algunas propiedades de la divisibilidad.

1. Dados $a, b \in \mathbb{Z}$, vale $\mathrm{mcd}(a, b) = \mathrm{mcd}(\pm a, \pm b)$. Esto permite pasar a trabajar con números naturales.

2. *Algortimo de Euclides.* Este algoritmo es un método para hallar el máximo común divisor de dos números. Se basa en aplicar reiteradamente la observación anterior.

   Consideremos a y b naturales tales que $a > b > 0$. Sea $a = bq_1 + r_1$ la división entera de a entre b, Si $r_1 > 0$, entonces dividimos b por r_1 obteniendo $b = r_1 q_2 + r_2$. Si $r_2 > 0$, entonces dividomos r_1 por r_2 obteniendo $r_1 = r_2 q_3 + r_3$. Mientras los restos sean no nulos seguimos, obteniendo

   $$a = bq_1 + r_1, \ b = r_1 q_2 + r_2, \ r_1 = r_2 q_3 + r_3, \cdots ; b > r_1 > r_2 > r_3 > \cdots \geq 0.$$

   Observar que vale $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_1) = \mathrm{mcd}(r_1, r_2) = \cdots$ Como los restos son no negativos y van decreciendo estrictamente, entonces este proceso en algún momento termina; el último resto no nulo es el máximo común divisor de a y b.

3. Supongamos $\mathrm{mcd}(a, b) = d$. Luego el algoritmo de Euclides nos dará

   $$a = bq_1 + r_1, \quad b = r_1 q_2 + r_2, \quad \cdots ; \quad r_{n-2} = r_{n-1} q_n + d.$$

   Despejando d obtenemos que existen $m, n \in \mathbb{Z}$ tales que $d = ma + nb$, esta es la *identidad de Bézout.*

4. Si $\mathrm{mcd}(a, b) = 1$, entonces decimos que a y b son *primos entre sí.* Es faćil de probar que a y b son primos entre sí, si y solo si existen $m, n \in \mathbb{Z}$ tales que $ma + nb = 1$.

5. Si $\mathrm{mcd}(a, b) = d$ y escribimos $a' = a/d$ y $b' = b/d$, entonces $\mathrm{mcd}(a', b') = 1$.

6. Si $a \mid bc$ y $\mathrm{mcd}(a, b) = 1$, entonces $a \mid c$. Luego si p es primo y $p \mid ab$, entonces $p \mid a$ o $p \mid b$.

Congruencia módulo n. Si n es un entero positivo, entonces definimos una relación en $\mathbb{Z}$ mediante

$$a \equiv b \quad \text{mód } n \quad \Leftrightarrow \quad n \mid a-b, \quad \forall a,b \in \mathbb{Z}.$$

esta relación es de equivalencia y se llama la *congruencia módulo n*. La clase de equivalencia de un elemento $a \in \mathbb{Z}$ es $\overline{a} = a + n\mathbb{Z} := \{a + nh : \ h \in \mathbb{Z}\}$. Escribimos $\mathbb{Z}_n = \{\overline{a} : \ a \in \mathbb{Z}\}$ al conjunto cociente. Usando la división entera es fácil de probar que $\mathbb{Z}_n$ tiene exactamente n elementos y se puede describir mediante

$$\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}.$$

Si $a \equiv a'$ mód n y $b \equiv b'$ mód n, entonces $(a+b) \equiv (a'+b')$ mód n y $(ab) \equiv (a'b')$ mód n. Luego podemos definir una suma y producto en $\mathbb{Z}_n$ mediante $\overline{a} + \overline{b} = \overline{a+b}$ y $\overline{a}\overline{b} = \overline{ab}$. Estas operaciones son conmutativas, associativas, el producto es distributivo frente a la suma, $\overline{0}$ es un neutro para la suma, $\overline{1}$ es un neutro para el producto y todo elemento $\overline{a}$ tiene un opuesto que es $\overline{-a}$. Luego $\mathbb{Z}_n$ con esa suma y producto es un anillo conmutativo. Una diferencia de $\mathbb{Z}_n$ con $\mathbb{Z}$ es que en general no vale la propiedad cancelativa del producto, por ejemplo en $\mathbb{Z}_6$ es $\overline{2}\,\overline{3} = \overline{0}$, siendo $\overline{2} \neq \overline{0}$ y siendo $\overline{3} \neq \overline{0}$.

2. Grupos

Sea G un conjunto y $* : G \times G \to G$, $(g,f) \mapsto g * f$ una función que llamamos *producto*[1] en G.

- Un elemento $e \in G$ es un *neutro* para $*$ si verifica $e * g = g * e = g$, para todo $g \in G$.
- El producto $*$ se dice *asociativo* si $g * (f * h) = (g * f) * h$, para todo $g, f, h \in G$.
- Si G tiene un neutro e, entonces $g \in G$ se dice *invertible* si existe $f \in G$ tal que $g * f = f * g = e$.

Observación 2.1. El neutro en caso de existir es único. Si $g \in G$ es invertible y el producto es asociativo entonces el elemento f tal que $g * f = f * g = e$ es único, se escribe $f = g^{-1}$, y se le llama el *inverso* de g.

Un *grupo* es un par $(G, *)$ en la cual G es un conjunto y $G \times G \xrightarrow{*} G$ es un producto que es asociativo, tiene un neutro y todo elemento de G es invertible. Por simplicidad de notación, en general escribiremos G en vez de $(G, *)$. El *orden* de G es su cardinal que lo escribiremos $|G|$. Diremos que G es *finito* o *infinito* de acuerdo a que $|G|$ lo sea. Para mantener una notación coherente, en general al cardinal de un conjunto X lo escribiremos $|X|$ en vez de $\#X$.

Ejemplos 2.2.
1. Si $\mathbb{Z}$ son los enteros, entonces $(\mathbb{Z}, +)$ es un grupo. Lo mismo sucede cambiando $\mathbb{Z}$ por $\mathbb{Z}_n$, o por un cuerpo arbitrario $\Bbbk$ que puede ser los racionales $\mathbb{Q}$, reales $\mathbb{R}$, complejos $\mathbb{C}$, etc.
2. El conjunto de matrices cuadradas $M_n(\Bbbk)$ con la suma es un grupo.
3. El grupo *trivial* es $G = \{e\}$, en el cual definimos $e * e = e$.

Una forma simple de obtener grupos es mediante monoides. Un *monoide* es lo mismo que un grupo, pero en el cual no se exige que todos sus elementos sean invertibles (luego un grupo es un caso particular de monoide). Si $M = (M, *)$ es un monoide y consideramos $M^\times = \{a \in M : \ a \text{ es invertible}\}$, entonces vale

$$e \in M^\times; \quad g, f \in M^\times \ \Rightarrow \ g * f \in M^\times \text{ y } (g * f)^{-1} = f^{-1} * g^{-1}; \quad g \in M^\times \ \Rightarrow \ g^{-1} \in M^\times \text{ y } \left(g^{-1}\right)^{-1} = g.$$

Luego $M^\times$ es un grupo (con el mismo producto y neutro que M) llamado el *grupo de invertibles* de M. Los siguientes ejemplos se obtienen como grupos de invertibles de ciertos monoides.

[1] Al producto también se le llama *operación binaria* o *ley de composición interna*.

Ejemplos 2.3. Los siguientes son ejemplos de grupos.

1. $\Bbbk^\times = \{x \in \Bbbk :\ x \neq 0\}$, $\mathbb{Z}^\times = \{\pm 1\}$ y $\mathbb{Z}_n^\times = \{\overline{a} :\ \mathrm{mcd}(a,n) = 1\}$, con la multiplicación. Notar que si p es primo, entonces $\mathbb{Z}_p^\times = \{\overline{a} \in \mathbb{Z}_p :\ \overline{a} \neq \overline{0}\}$; luego $\mathbb{Z}_p$ es un cuerpo.

2. El *grupo general lineal* es $\mathrm{GL}_n(\Bbbk) = \{A \in M_n(\Bbbk) :\ \det A \neq 0\}$, con el producto de matrices.

3. Si V es un espacio vectorial, entonces a $\mathrm{GL}(V) = \{\varphi : V \to V :\ \varphi \text{ es un isomorfismo lineal}\}$ con la composición también se le llama *grupo general lineal*.

4. Dado $X \neq \emptyset$, el conjunto $\mathrm{Biy}(X) = \{f : X \to X :\ f \text{ es una biyección}\}$, con la composición. Si $X = \{1, \dots, n\}$, entonces a $\mathcal{S}_n = \mathrm{Biy}(X)$ se le llama el *grupo simétrico* y a sus elementos *permutaciones*. La cantidad de elementos de $\mathcal{S}_n$ es $n!$. Para las permutaciones usaremos la notación

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

Sea G un grupo. Dos elementos $g, f \in G$ *conmutan* si $g * f = f * g$. Si todos los elementos de G conmutan, entonces el producto se dice *conmutativo* y el grupo se dice *abeliano*. Por ejemplo $\mathbb{Z}$ y $\Bbbk^\times$ son grupos abelianos, mientras que $\mathrm{GL}_n(\Bbbk)$ y $\mathcal{S}_n$ (ambos para $n \geq 2$) son grupos no abelianos. En la teoría, cuando el grupo es abeliano se suele usar notación aditiva

$$g * f = g + f, \qquad e = 0, \qquad g^{-1} = -g, \qquad \forall g, f \in G.$$

Nota: por simplicidad, de ahora en más en los grupos escribiremos gf en vez de $g * f$ y 1 en vez de e. Por supuesto que esto lo haremos solo en la teoría, en los casos concretos usaremos la notación que corresponda.

Proposición 2.4. *Sea G un grupo.*

1. *Si $g, f, x \in G$, entonces*

$$gx = f \ \Leftrightarrow\ x = g^{-1}f; \quad xg = f \ \Leftrightarrow\ x = fg^{-1}.$$

2. *Si $g \in G$, entonces las funciones de G en G definidas por $x \mapsto gx$ y $x \mapsto xg$, son biyectivas.* □

Si $g \in G$ y $n \in \mathbb{N}$, definimos g^n recursivamente mediante

$$g^n = \begin{cases} 1, & n = 0, \\ g^{n-1}g, & n \geq 1. \end{cases}$$

Esta definición se extiende a potencias negativas mediante $g^{-n} = \left(g^{-1}\right)^n$, para todo $n \in \mathbb{Z}^+$. Si G es abeliano y usamos notación aditiva, entonces se escribe ng en vez de g^n.

Proposición 2.5. *Sea G un grupo.*

1. *Si $g \in G$, entonces $g^n g^m = g^{n+m}$, $(g^n)^m = g^{nm}$, para todo $n, m \in \mathbb{Z}$.*

2. *Si $g, f \in G$ conmutan, entonces $(gf)^n = g^n f^n$, para todo $n \in \mathbb{Z}$.* □

Sea G un grupo y $g \in G$. El *orden* de g es $|g| \in \mathbb{Z}^+ \cup \infty$, que está definido por lo siguiente. Si existe $n \neq 0$ tal que $g^n = 1$, entonces definimos $|g| = \min\{n > 0 :\ g^n = 1\}$; en caso contrario definimos $|g| = \infty$.

Proposición 2.6. *Sea G un grupo y $g \in G$.*

1. Si $|g| = \infty$, entonces $g^k = 1$ si y solo si $k = 0$, y $g^k = g^h$ si y solo si $k = h$.

2. Supongamos $|g| = n < \infty$, entonces.

a) *Vale $g^k = 1$ si y solo si $n \mid k$, y vale $g^k = g^h$ si y solo si $k \equiv h \mod n$.*

b) *Para todo $k \in \mathbb{Z}$ vale que g^k tiene orden finito y $\left|g^k\right| = n/d$, siendo $d = \operatorname{mcd}(n, k)$. En particular, si $k > 0$ y $k \mid n$, entonces $\left|g^k\right| = n/k$.*

Dem.

1. La primer afirmación es obvia y la segunda se deduce de la primera.

2. *a*) Es claro que $n \mid k$ implica $g^k = 1$. El recíproco se deduce dividiendo k por n. El resto es fácil.

   b) Sean $n' = n/d$ y $k' = k/d$. Por un lado $\left(g^k\right)^{n'} = g^{kn'} = g^{dk'n'} = (g^n)^{k'} = 1$. Esto implica que g^k tiene orden finito y si $s = \left|g^k\right|$ entonces $s \mid n'$. Por otro $1 = \left(g^k\right)^s = g^{ks}$, luego $n \mid ks$ y al ser n' primo con k', deducimos $n' \mid s$. Luego $n' = s$. □

3. Subgrupos

Un *subgrupo* de G es un subconjunto H que verifica

$$1 \in H; \qquad g, f \in H \;\Rightarrow\; gf \in H; \qquad g \in H \Rightarrow g^{-1} \in H,$$

o, equivalentemente, si verifica

$$1 \in H; \qquad g, f \in H \;\Rightarrow\; gf^{-1} \in H.$$

Escribimos $H < G$ para indicar que H es un subgrupo de G. Es claro que H es un grupo siendo su producto la restricción a H del producto de G.

Ejemplos 3.1. 1. Dado un grupo G, los subconjuntos $\{1\}$ y G son subgrupos de G. El subgrupo *trivial* es $\{1\}$. Todo subgrupo de G distinto de $\{1\}$ y G se dice que es *propio*.

2. Un *movimiento* o *isometría* del plano $\mathbb{R}^2$ es una función $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ que preserva la distancia euclídea. Se prueba que los movimientos son funciones biyectivas, y que forman un subgrupo del grupo de biyecciones de $\mathbb{R}^2$ en $\mathbb{R}^2$, llamado el *grupo de movimientos* del plano, que escribiremos $\mathcal{M}$. Recordar que $\mathcal{M}$ está formado por rotaciones[2] $\rho_{p,\theta}$, traslaciones τ_v, simetrías axiales σ_L y antitraslaciones[3] $\alpha_{v,L}$.

3. Los movimientos *directos* (los que preservan el sentido del plano) son las rotaciones y las traslaciones. Llamaremos *indirectos* a los que invierten el sentido, que son las simetrías axiales y antitraslaciones. El conjunto $\mathcal{M}_+$ formado por los movimientos directos es un subgrupo de $\mathcal{M}$.

4. Si X es un subconjunto del plano, una *simetría* de X es un movimiento $\varphi \in \mathcal{M}$ que verifica $\varphi(X) = X$. El conjunto $\operatorname{Sim}(X)$ de las simetrías de X es un subgrupo de $\mathcal{M}$ llamado el *grupo de simetrías* de X.

5. Si P_n es un polígono regular de n lados, entonces $D_n := \operatorname{Sim}(P_n)$ es el *grupo diedral*. Supongamos que el origen o es el centro de P_n y que $v_k = \big(\cos(2k\pi/n), \operatorname{sen}(2k\pi/n)\big)$, $k = 0, 1, \ldots, n-1$ son los vértices de P_n. Si $\rho_k = \rho_{o,2k\pi/n}$ y $\sigma_k = \sigma_{L_k}$, siendo L_k la recta que pasa por o y forma un ángulo de $k\pi/n$ con el eje horizontal, entonces D_n tiene $2n$ elementos que son

$$D_n = \{\rho_0, \rho_1, \rho_2, \ldots, \rho_{n-1}, \sigma_0, \sigma_1, \ldots, \sigma_{n-1}\}, \quad \rho_0 = \operatorname{id}.$$

[2]Convenimos que si es $\theta > 0$, entonces el giro se hace en sentido antihorario y si es $\theta < 0$, entonces el giro es horario.

[3]Una *antitraslación* o *simetría con deslizamiento* es la composición de una simetría axial con una traslación de ejes paralelos.

Definimos también $D_1 = \{\rho_0, \sigma_0\}$ y $D_2 = \{\rho_0, \rho_1, \sigma_0, \sigma_1\}$, siendo $\rho_0 = \mathrm{id}$, ρ_1 la simetría central del centro o, y σ_0 y σ_1 simetrías axiales de ejes perpendiculares que se cortan en o.

6. Para cada $n \in \mathbb{Z}^+$ definimos $U_n = \{z \in \mathbb{C} :\ z^n = 1\}$. Sea $S^1 = \{z \in \mathbb{C} :\ |z| = 1\}$ y consideremos

$$U_\infty := \bigcup_{n=1}^{\infty} U_n = \{z \in \mathbb{C} :\ z^n = 1 \text{ para algún } n \in \mathbb{Z}^+\}.$$

Entonces $\{1\} < U_n < U_\infty < S^1 < \mathbb{C}^\times$ $(n \geq 1)$, es una cadena de subgrupos multiplicativos

Proposición 3.2. *Si H_i es un subgrupo de G, para todo $i \in I$, entonces $\bigcap_{i\in I} H_i$ es un subgrupo de G.* $\square$

Ejemplo 3.3. El *grupo de simetrías directas* de un subconjunto X del plano es $\mathrm{Sim}_+(X) := \mathrm{Sim}(X) \cap \mathcal{M}_+$, que es un subgrupo del grupo de simetrías de X.

Si S es un subconjunto de G, entonces el *subgrupo generado* por S es $\langle S\rangle := \bigcap_{S\subset H<G} H$. Notar que $\langle S\rangle$ es el menor subgrupo de G que contiene a S, y se puede describir mediante

$$\langle S\rangle = \left\{ s_1^{n_1} \cdots s_k^{n_k} :\ s_i \in S,\ n_i \in \mathbb{Z},\ i = 1, \ldots, k,\ k \in \mathbb{Z}^+ \right\}.$$

Si $S = \{g_1, \ldots, g_n\}$, escribimos $\langle S\rangle = \langle g_1, \ldots, g_n\rangle$. En particular $\langle g\rangle = \{g^n :\ n \in \mathbb{Z}\}$ es el *subgrupo cíclico* generado por g.

Si $G = \langle S\rangle$, decimos que S *genera* a G o que S es un *conjunto de generadores* de G. El grupo G se dice *finitamente generado* si tiene un conjunto de generadores finito.

Observación 3.4. Todo grupo finito es finitamente generado. El recíproco es falso: $\mathbb{Z} = \langle 1\rangle$ y es infinito.

Ejemplo 3.5. Consideremos el grupo diedral $D_n = \mathrm{Sim}(P_n)$ visto anteriormente. Si $\rho = \rho_1$ y $\sigma = \sigma_0$, entonces $\rho_k = \rho^k$ y $\sigma_k = \sigma\rho^k$, para todo k. Luego $D_n = \langle \rho, \sigma\rangle$ y podemos escribr

$$D_n = \{\mathrm{id}, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\}. \tag{1}$$

Notar $\mathrm{Sim}_+(P_n) = \langle\rho\rangle = \{\mathrm{id}, \rho, \ldots, \rho^{n-1}\}$, que es un subgrupo cíclico de D_n. Escribiremos $C_n = \langle\rho\rangle$.

Generadores y relaciones. Los generadores ρ y σ del grupo diedral D_n verifican

$$\rho^n = \sigma^2 = \mathrm{id}, \quad \rho\sigma = \sigma\rho^{n-1}. \tag{2}$$

Notar $\rho^{n-1} = \rho^{-1}$. Las fórmulas (2) determinan el producto del grupo. Por ejemplo de las mismas se deducen las "reglas de conmutación" entre σ y las potencias de ρ

$$\rho\sigma = \sigma\rho^{n-1}, \quad \rho^2\sigma = \sigma\rho^{n-2}, \quad \cdots, \quad \rho^{n-1}\sigma = \sigma\rho.$$

También nos permiten calcular el producto de los elementos de D_n, escritos en la forma de (1)

$$\rho^i\rho^j = \rho^{i+j}, \quad \left(\sigma\rho^i\right)\rho^j = \sigma\rho^{i+j}, \quad \rho^i\left(\sigma\rho^j\right) = \sigma\rho^{j-i}, \quad \left(\sigma\rho^i\right)\left(\sigma\rho^j\right) = \rho^{j-i}.$$

Además esas relaciones son minimales, en el sentido de que vale $\rho^n = \mathrm{id}$ y n es el menor entero positivo que lo verifica, análogamente vale $\sigma^2 = \mathrm{id}$ pero es $\sigma \neq \mathrm{id}$. Si G es un grupo que está generado por dos elementos a, b tales que para cierto $n > 0$ vale $a^n = 1$, $a^l \neq 1$ si $1 \leq l < 1$, $b^2 = 1$, $b \neq 1$ y $ab = ba^{n-1}$, entonces identificando a con ρ y b con σ, obtenemos que G se identifica con el grupo diedral D_n (son isomorfos en el sentido que definiremos más adelante). Luego a los grupos de este tipo les llamaremos *diedrales*. En ese caso escribimos $D_n = \langle a, b :\ a^n = b^2 = 1,\ ab = ba^{n-1}\rangle$ y decimos que la anterior es una *presentación* de D_n dada por *generadores y relaciones*. Esta es una forma simple de describir un grupo y se usa frecuentemente[4].

[4] Todo esto se puede formalizar bien introduciendo los *grupos libres*, pero por falta de tiempo no lo haremos.

Si $H < G$ y $K < G$, definimos el *subgrupo generado* por H y K mediante $H \vee K = \langle H \cup K \rangle$; es el menor subgrupo de G que contiene a H y K. Explícitamente

$$H \vee K = \left\{ g_1 \cdots g_n : \ g_i \in H \cup K, \ i = 1, \ldots, n, \ n \in \mathbb{Z}^+ \right\}.$$

Claramente esta definición se generaliza para una familia arbitraria de subgrupos de G.

Observación 3.6. El conjunto de los subgrupos de un grupo forma un *retículo completo* respecto al orden de inclusión, es decir es un conjunto parcialmente ordenado en el cual todo subconjunto no vacío tiene supremo e ínfimo. En particular el supremo de $\{H, K\}$ es $H \vee K$ y el ínfimo es $H \cap K$.

Ejemplo 3.7. Los retículos de subgrupos de $\mathbb{Z}_4$ y $D_2 = \{\mathrm{id}, \rho, \sigma, \sigma\rho\}$ son

$$\begin{tikzcd}
\mathbb{Z}_4 \arrow[d, dash] \\
\langle \overline{2} \rangle \arrow[d, dash] \\
\langle \overline{0} \rangle
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
 & D_2 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \sigma \rangle \arrow[dr, dash] & \langle \rho \rangle \arrow[d, dash] & \langle \sigma\rho \rangle \arrow[dl, dash] \\
 & \langle \mathrm{id} \rangle &
\end{tikzcd}$$

En la representación de arriba las líneas verticales marcan las inclusiones.

Si bien el principal objetivo de estas notas son los grupos finitos, una pregunta natural es ¿qué se sabe de los subgrupos de $\mathbb{R}$ (pensado como grupo con la suma)? El siguiente resultado va en esa dirección.

Teorema 3.8. *Si G es un subgrupo de $\mathbb{R}$, entonces existe $\alpha \in \mathbb{R}$ tal que $G = \mathbb{Z}\alpha$ o G es denso en $\mathbb{R}$.*

Dem. Si $G = \{0\}$ el resultado es obvio tomando $\alpha = 0$. De aquí en más suponemos que este no es el caso.
Sea $\alpha = \inf\{|x| : \ x \in G, \ x \neq 0\}$. Una posibilidad es $\alpha = \min\{|x| : \ x \in G, \ x \neq 0\}$, aquí $\alpha > 0$. Dado $x \in G$, podemos escribir $x = n\alpha + y$, donde $n \in \mathbb{Z}$ y $0 \leq y < \alpha$. Luego $y = x - n\alpha \in G$ y si fuese $y > 0$ llegaríamos a una contradicción; luego es $y = 0$ y $x = n\alpha$. Esto prueba $G = \mathbb{Z}\alpha$.
La otra posibilidad es $\alpha \notin \{|x| : \ x \in G, \ x \neq 0\}$. En este caso probaremos que dados $a < b$ en $\mathbb{R}$, entonces siempre existe $g \in G$ tal que $a < g < b$. Sea $\epsilon = b - a > 0$. Por nuestra asunción sobre α, sabemos que existen $y, z \in G$ tales que $\alpha < y < z < \alpha + \epsilon$, luego $x := z - y \in G$ y $0 < x < \epsilon$. Luego es fácil de probar que existe $m \in \mathbb{Z}$ tal que $a < mx < a + \epsilon = b$. Así $g = mx \in G$ y $a < g < b$. $\square$

4. Morfismos

Una función entre dos grupos $\varphi : G_1 \to G_2$ se dice un *morfismo* u *homomorfismo* de grupos si verifica $\varphi(gf) = \varphi(g)\varphi(f)$, para todo $g, f \in G_1$.

Proposición 4.1. *Si $\varphi : G_1 \to G_2$ es un morfismo, entonces*

1. *$\varphi(1) = 1$ y $\varphi\left(g^{-1}\right) = \varphi(g)^{-1}$, para todo $g \in G_1$.*
2. *$\varphi\left(g^n\right) = \varphi(g)^n$, para todo $g \in G_1$ y $n \in \mathbb{Z}$.* $\square$

Si $\varphi : G_1 \to G_2$ es un morfismo, entonces su *núcleo* es $\operatorname{Ker}(\varphi) = \{g \in G_1 : \ \varphi(g) = 1\}$ y su *imagen* es $\operatorname{Im}(\varphi) = \varphi(G_1)$. Claramente $\operatorname{Ker}(\varphi) < G_1$ y $\operatorname{Im}(\varphi) < G_2$.

Ejemplo 4.2. Sea $SL_n(\Bbbk) = \{A \in M_n(\Bbbk) : \det A = 1\}$. Notar que $\det : GL_n(\Bbbk) \to \Bbbk^\times$ es un morfismo y $SL_n(\Bbbk) = \operatorname{Ker}(\det)$, luego $SL_n(\Bbbk)$ es un subgrupo de $GL_n(\Bbbk)$ llamado el *grupo especial lineal.*

Proposición 4.3. *Sea* $\varphi : G_1 \to G_2$ *un morfismo. Si* $H < G_1$*, entonces* $\varphi(H) < G_2$*. Si* $K < G_2$*, entonces* $\mathrm{Ker}\,(\varphi) < \varphi^{-1}(K) < G_1$*.* □

A continuación veremos algunos nombres y notaciones. Sea $\varphi : G_1 \to G_2$ un morfismo.

- φ es un *monomorfismo* si es inyectivo. Notación: $\varphi : G_1 \rightarrowtail G_2$.
- φ es un *epimorfismo* si es sobreyectivo. Notación: $\varphi : G_1 \twoheadrightarrow G_2$.
- φ es un *isomorfismo* si es biyectivo. Notación: $\varphi : G_1 \xrightarrow{\simeq} G_2$.
- φ es un *endomorfismo* si $G_1 = G_2$.
- φ es un *automorfismo* si es un endomorfismo biyectivo.

Proposición 4.4. *Propiedades:*

1. *Si* $\varphi : G_1 \to G_2$ *es un morfismo, entonces* φ *es un monomorfismo si y solo si* $\mathrm{Ker}\,(\varphi) = \{1\}$*.*
2. *Si* $\varphi : G_1 \to G_2$ *y* $\psi : G_2 \to G_3$ *son morfismos, entonces* $\psi \circ \varphi : G_1 \to G_3$ *es un morfismo.*
3. *Si* $\varphi : G_1 \to G_2$ *es un isomorfismo, entonces* $\varphi^{-1} : G_2 \to G_1$ *es un isomorfismo.* □

Decimos que dos grupos G_1 y G_2 son *isomorfos* y escribimos $G_1 \simeq G_2$ si existe un isomorfismo $\varphi : G_1 \to G_2$. Los grupos isomorfos tienen las mismas propiedades y por lo tanto son indistinguibles como grupos.
Es claro que la relación "ser isomorfos" es de equivalencia. Si G es un grupo y definimos

$$\mathrm{End}(G) = \{\varphi : G \to G : \ \varphi \text{ endomorfismo}\}, \qquad \mathrm{Aut}(G) = \{\varphi : G \to G : \ \varphi \text{ automorfismo}\},$$

entonces $\mathrm{End}(G)$ es un monoide con la composición y $\mathrm{Aut}(G)$ es su grupo de invertibles.

Ejemplos 4.5.

1. Si G_1 y G_2 son grupos, entonces el mapa constante $\varphi : G_1 \to G_2$ definido por $\varphi(g) = 1$, para todo $g \in G_1$, es un morfismo llamado el *morfismo trivial*.
2. Si H es un subgrupo de G, entonces la inclusión $H \hookrightarrow G$ es un monomorfismo.
3. Para cada $n \in \mathbb{Z}^+$, la proyección canónica $\pi : \mathbb{Z} \to \mathbb{Z}_n$ definida por $\pi(x) = \overline{x}$, es un epimorfismo.
4. Si $g \in G$, entonces $\mathrm{int}_g : G \to G$ definido por $\mathrm{int}_g(x) = gxg^{-1}$, para todo $x \in G$, es un automorfismo. Los automorfismos de la forma int_g se llaman automorfismos *internos*.
5. Si G es abeliano, entonces $\varphi : G \to G$ definido por $\varphi(g) = g^{-1}$, para todo $g \in G$, es un automorfismo.
6. Sea V un $\mathbb{k}$-espacio vectorial de dimensión finita n y $\mathcal{B}$ una base de V. Entonces la correspondencia $\varphi \mapsto [\varphi]_{\mathcal{B}}$ es un isomorfismo de $\mathrm{GL}(V)$ en $\mathrm{GL}_n(\mathbb{k})$. Por esto es que tienen el mismo nombre.
7. El mapa $\varphi : \mathbb{R} \to \mathbb{R}^+$ definido por $\varphi(x) = e^x$ para todo $x \in \mathbb{R}$, es un isomorfismo ($\mathbb{R}^+$ con el producto).

Producto directo. Sean G_1 y G_2 dos grupos. En el producto cartesiano $G_1 \times G_2$ definimos un producto mediante

$$(g_1, g_2) \cdot (f_1, f_2) = (g_1 f_1,\ g_2 f_2), \qquad \forall\ g_1, f_1 \in G_1,\ g_2, f_2 \in G_2.$$

El conjunto $G_1 \times G_2$ con este producto es un grupo llamado el *producto directo* de G_1 y G_2.

Consideremos $\iota_1 : G_1 \to G_1 \times G_2$, $\iota_2 : G_2 \to G_1 \times G_2$, $\rho_1 : G_1 \times G_2 \to G_1$ y $\rho_2 : G_1 \times G_2 \to G_2$, definidos por

$$\iota_1(g_1) = (g_1, 1), \quad \iota_2(g_2) = (1, g_2), \quad \rho_1(g_1, g_2) = g_1, \quad \rho_2(g_1, g_2) = g_2, \quad \forall\, g_1, f_1 \in G_1,\ g_2, f_2 \in G_2.$$

Entonces ι_1 y ι_2 son monomorfismos, ρ_1 y ρ_2 son epimorfismos, y valen $\rho_1 \circ \iota_1 = \mathrm{id}_{G_1}$ y $\rho_2 \circ \iota_2 = \mathrm{id}_{G_2}$.
El morfismo $\iota_1 : G_1 \to G_1 \times G_2$ es la *inclusión* de G_1 en $G_1 \times G_2$ y $\rho_1 : G_1 \times G_2 \to G_1$ es la *proyección* de $G_1 \times G_2$ sobre G_1, y se define lo mismo para G_2.

Si G_1 y G_2 son grupos abelianos y usamos notación aditiva, entonces el producto directo $G_1 \times G_2$ se suele escribir $G_1 \oplus G_2$ y en esa notación se le llama también la *suma directa*.

Es claro que la estructura de producto directo se generaliza naturalmente para productos finitos $G_1 \times \cdots \times G_n$ y en general para productos cartesianos de familias arbitrarias de grupos.

5. Grupos cíclicos

Un grupo G se dice *cíclico* si existe $g \in G$ tal que $G = \langle g \rangle = \{g^n : \ n \in \mathbb{Z}\}$. Notar que todo grupo cíclico es abeliano.

Ejemplo 5.1. Los grupos $\mathbb{Z}$ y $\mathbb{Z}_n$ son cíclicos y están generados respectivamente por 1 y $\overline{1}$. Notar que $1 \in \mathbb{Z}$ tiene orden infinito mientras que $\overline{1} \in \mathbb{Z}_n$ tiene orden n.

Proposición 5.2. *Sea $G = \langle g \rangle$ un grupo cíclico.*

1. *Si $|g| = \infty$, entonces $G \simeq \mathbb{Z}$.*
2. *Si $|g| = n < \infty$, entonces $G \simeq \mathbb{Z}_n$.*

Luego el orden del grupo G coincide con el orden del generador g.

Dem. Los mapas $\varphi : \mathbb{Z} \to G$ y $\psi : \mathbb{Z}_n \to G$ definidos respectivamente por $\varphi(n) = g^n$ y $\psi(\overline{m}) = g^m$, son isomorfismos. Notar que ψ está bien definido por la parte 2b) de la proposición 2.6. $\square$

Observación 5.3. Si $G = \langle g \rangle$ es un grupo cíclico finito de orden n, entonces.

1. $G = \{1, g, g^2, \dots, g^{n-1}\}$ y $g^n = 1$;
2. $g^m = 1$ si y solo si $n|m$;
3. $g^r = g^s$ si y solo si $n|r - s$ si y solo si $\overline{r} = \overline{s}$ en $\mathbb{Z}_n$.

Corolario 5.4. *Sea $G = \langle g \rangle$ un grupo cíclico.*

1. *Si $|G| = \infty$, entonces los generadores de G son g y g^{-1}.*
2. *Si $|G| = n < \infty$, entonces g^k genera a G si y solo si* $\mathrm{mcd}(k, n) = 1$.

Dem. Si $|G| = \infty$, como los generadores de $\mathbb{Z}$ son ± 1, deducimos que los de G son $g^{\pm 1}$. Si $|G| = n < \infty$, entonces g^k genera a G si y solo si $\overline{k}$ genera a $\mathbb{Z}_n$ si y solo si $\overline{1} \in \langle \overline{k} \rangle$ si y solo si $\mathrm{mcd}(k, n) = 1$ (usando la observación 1.2). $\square$

Ejemplo 5.5. Sea $n \in \mathbb{Z}^+$ y $U_n = \{z \in \mathbb{C} : \ z^n = 1\}$. Si $\zeta = e^{\frac{2\pi i}{n}}$, entonces $U_n = \langle \zeta \rangle = \left\{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\right\}$ y vale $\zeta^n = 1$. Notar $|U_n| = n$. Los generadores de U_n son los elementos de la forma $\zeta^k = e^{\frac{2k\pi i}{n}}$, con $\mathrm{mcd}(k, n) = 1$; estos generadores se llaman las *raíces primitivas* de orden n de la unidad.

El siguiente resultado determina los subgrupos de los grupos cíclicos.

Proposición 5.6. *Sea $G = \langle g \rangle$ un grupo cíclico.*

1. *Si H es un subgrupo de G, entonces H es cíclico.*
2. *Si G es de orden finito n y H es un subgrupo de G de orden k, entonces k divide a n y $H = \langle g^{n/k} \rangle$.*

Dem. Consideremos la primer afirmación. Si $H = \{1\}$, entonces $H = \langle 1 \rangle$. Supongamos ahora $H \neq \{1\}$. Sea $m = \min\{l \in \mathbb{Z}^+ : \ g^l \in H\}$. Si $x = g^l \in H$, entonces dividiendo l por m obtenemos $l = mq + r$, con $0 \leq r < m$. Luego de $g^l = (g^m)^q g^r$ deducimos $g^r \in H$ y por lo tanto $r = 0$. Esto implica $H = \langle g^m \rangle$.

En lo que sigue asumiremos $|G| = |g| = n < \infty$.

Observemos primero que si $k \mid n$, entonces $\left|g^{n/k}\right| = k$ y por lo tanto $\left\langle g^{n/k} \right\rangle$ es un subgrupo de G de orden k

Supongamos ahora que H un subgrupo de G de orden k. Luego $H = \langle g^m \rangle$, siendo $m = \min\{l \in \mathbb{Z}^+ : \ g^l \in H\}$. Veamos primero que m divide a n. Sea $n = mq + r$ con $0 \leq r < m$ la división entera de n entre m. Luego

$$1 = g^n = g^{mq+r} = (g^m)^q g^r \quad \Rightarrow \quad g^r = (g^m)^{-q} \in H.$$

La minimalidad de m implica $r = 0$, luego $n = mq$. Como m divide a n, entonces $|g^m| = n/m$, pero es $H = \langle g^m \rangle$, luego $k = |H| = |g^m| = n/m$ y por lo tanto $m = n/k$. Luego k divide a n y $H = \langle g^{n/k} \rangle$. $\square$

Aplicación 5.7. Todo subgrupo de $\mathbb{Z}$ es de la forma $m\mathbb{Z} = \{ma : \ a \in \mathbb{Z}\}$, con $m \geq 0$. Todo subgrupo de $\mathbb{Z}_n$ es de la forma $\overline{m}\mathbb{Z}_n = \{\overline{ma} : \ a \in \mathbb{Z}\}$, con $1 \leq m \leq n$ y $m|n$; además $|\overline{m}\mathbb{Z}_n| = n/m$.

A continuación usamos la proposición 2.6 para determinar los morfismos cuyos dominios son grupos cíclicos.

Proposición 5.8. *Sea G un grupo cíclico y F un grupo arbitrario.*

1. *Si $|G| = \infty$, entonces hay una correspondencia uno a uno entre los morfismos de G en F y los elementos de F.*
2. *Si $|G| = n < \infty$, entonces hay una correspondencia uno a uno entre los morfismos de G en F y los elementos $f \in F$ tales que $f^n = 1$.*

Dem. Sea $G = \langle g \rangle = \{g^k : \ k \in \mathbb{Z}\}$. Observar que todo morfismo $\varphi : G \to F$ verifica $\varphi(g^k) = \varphi(g)^k$, para todo $k \in \mathbb{Z}$. Luego si existe un morfismo $\varphi : G \to F$, entonces φ es de la forma

$$\varphi(g^k) = f^k, \quad \forall k \in \mathbb{Z}, \tag{3}$$

siendo $f = \varphi(g)$. Luego a cada morfismo φ le corresponde un único elemento $f = \varphi(g)$ que verifica (3).

Si $|G| = \infty$, entonces $g^k = g^h$ si y solo si $k = h$ y por lo tanto cada $f \in F$ permite definir una función $\varphi : G \to F$ mediante la fórmula (3). Notar que esa función es un morfismo

$$\varphi\big(g^h g^k\big) = \varphi\big(g^{h+k}\big) = f^{h+k} = f^h f^k = \varphi\big(g^h\big)\varphi\big(g^k\big), \quad \forall h, k \in \mathbb{Z}.$$

Supongamos ahora que es $|G| = n < \infty$, tenemos un elemento $f \in F$ y queremos definir un morfismo $\varphi : G \to F$ mediante la fórmula (3). Si eso es posible, entonces $f^n = \varphi(g^n) = \varphi(1) = 1$, luego $f^n = 1$. Recíprocamente, supongamos que tenemos $f \in F$ tal que $f^n = 1$. Si $k, h \in \mathbb{Z}$ son tales que $g^k = g^h$, entonces $n|k - h$ y por lo tanto existe $a \in \mathbb{Z}$ tal que $k = h + an$. Luego $f^k = f^{h+an} = f^h(f^n)^a = f^h$. Así que si $f^n = 1$, entonces $g^k = g^h$ implica $f^k = f^h$. Luego en este caso tiene sentido definir una función $\varphi : G \to F$ mediante la fórmula (3), y la misma cuenta de antes nos prueba que φ es morfismo. $\square$

Observación 5.9. Los grupos cíclicos infinitos son isomorfos a $\mathbb{Z}$ y los grupos cíclicos finitos de orden n son isomorfos a $\mathbb{Z}_n$. Así que, a menos de isomorfismo, hay uno solo de cada tipo. En general a los grupos cíclicos finitos de n elementos los escribiremos C_n y usaremos C_∞ para los grupos cíclicos infinitos. Son de la forma $C_n = \left\{1, g, g^2, \ldots, g^{n-1}\right\}$ con $g^n = 1$ y $C_\infty = \{g^m : \ m \in \mathbb{Z}\}$.

6. Coclases

Sea G un grupo y H un subgrupo. Definimos una relación de equivalencia en G llamada *congruencia módulo* H, que escribimos $\equiv \pmod{H}$, mediante

$$g \equiv f \pmod{H} \quad \overset{\text{def}}{\Leftrightarrow} \quad \exists\, h \in H: \ g = fh \quad \Leftrightarrow \quad f^{-1}g \in H.$$

La clase de equivalencia de $g \in G$ es

$$\overline{g} := \{f \in G : \ f \equiv g \pmod{H}\} = \{gh : \ h \in H\} = gH.$$

El conjunto gH es la *coclase izquierda* de g respecto a H. Escribimos $G/H = \{gH : \ g \in G\}$.

También podemos definir otra relación de equivalencia $\equiv_d \pmod{H}$, mediante

$$g \equiv_d f \pmod{H} \quad \overset{\text{def}}{\Leftrightarrow} \quad \exists\, h \in H: \ g = hf \quad \Leftrightarrow \quad gf^{-1} \in H.$$

Si $g \in G$, su clase de equivalencia es

$$\{f \in G : \ f \equiv_d g \pmod{H}\} = \{hg : \ h \in H\} = Hg.$$

El conjunto Hg se llama la *coclase derecha* de g respecto a H y escribimos $H\backslash G = \{Hg : \ g \in G\}$.

Observación 6.1. Se puede definir un nuevo producto $\star$ en G mediante $a \star b := ba$. El par $G^{\text{op}} = (G, \star)$ es un grupo llamado el *grupo opuesto* de G. Luego $\equiv_d \pmod{H}$ en G coincide con $\equiv \pmod{H}$ en G^{op}.

Ejemplo 6.2. Consideremos el grupo diedral D_3, que se puede describir mediante

$$D_3 = \left\{1, b, b^2, a, ab, ab^2\right\}, \ b^3 = a^2 = 1, \ ba = ab^2, \ b^2a = ab.$$

Sea $H = \langle a \rangle = \{1, a\}$. Las coclases izquierdas de H son

$$1H = aH = H, \quad bH = ab^2H = \left\{b, ab^2\right\}, \quad b^2H = abH = \left\{b^2, ab\right\}, \qquad G/H = \left\{H, bH, b^2H\right\}.$$

Las coclases derechas de H son

$$H1 = Ha = H, \quad Hb = Hab = \{b, ab\}, \quad Hb^2 = Hab^2 = \left\{b^2, ab^2\right\}, \qquad H\backslash G = \left\{H, Hb, Hb^2\right\}.$$

Notar $bH \neq Hb$, $Hb^2 \neq b^2H$ y $G/H \neq H\backslash G$.

Consideremos ahora el subgrupo $K = \langle b \rangle = \{1, b, b^2\}$. En este caso vale $aK = Ka$ y $G/K = K\backslash G = \{K, aK\}$. Luego las coclases izquierdas y derechas pueden coincidir o no, dependiendo del subgrupo.

Proposición 6.3. *Sea G un grupo y H un subgrupo. Entonces*

$$|gH| = |Hg| = |H|, \ \forall g \in G; \qquad |G/H| = |H\backslash G|.$$

Dem. Los mapas $H \to gH$ y $H \to Hg$ definidos respectivamente por $h \mapsto gh$ y $h \mapsto hg$ son biyectivos; esto implica la primer afirmación. Para la segunda, observar que vale

$$gH = fH \quad \Leftrightarrow \quad f^{-1}g \in H \quad \Leftrightarrow \quad f^{-1}\big(g^{-1}\big)^{-1} \in H \quad \Leftrightarrow \quad Hf^{-1} = Hg^{-1}, \quad \forall g, f \in H.$$

Luego tiene sentido definir un mapa $\varphi : G/H \to H\backslash G$ por $\varphi(gH) = Hg^{-1}$ y este mapa es inyectivo. Notar $\varphi(g^{-1}H) = Hg$, luego φ también es sobreyectivo, y por lo tanto es biyectivo. $\square$

Si H es un subgrupo de G, llamamos *índice* de H en G a $[G:H] := |G/H| = |H\backslash G|$.

Observación 6.4. Si $H = G$, entonces $G/G = \{G\}$, luego $[G:G] = 1$. Si $H = \{1\}$, entonces el mapa $G \to G/H$ definido por $g \mapsto g\{1\} = \{g\}$ es biyectivo, luego $[G:\{1\}] = |G|$.

Teorema 6.5 (Lagrange)**.** *Sea G un grupo y H un subgrupo. Entonces $|G| < \infty$ si y solo si $|H| < \infty$ y $[G:H] < \infty$. En ese caso vale*

$$|G| = [G:H]|H|.$$

Dem. El directo es claro. Para el recíproco, supongamos $|H| < \infty$ y $[G:H] < \infty$. Sea $n = [G:H]$, entonces existen $g_1, \dots, g_n \in G$ tales que $G/H = \{g_1H, \dots, g_nH\}$. Luego[5] $G = \bigsqcup_{i=1}^n g_iH$ y por lo tanto

$$|G| = \sum_{i=1}^n |g_iH| = \sum_{i=1}^n |H| = n|H| = [G:H]|H|. \quad \square$$

Observación 6.6. Si G es un grupo finito y H es un subgrupo, entonces el teorema de Lagrange implica que $|H|$ y $[G:H]$ dividen a $|G|$, y $[G:H] = \frac{|G|}{|H|}$.

Corolario 6.7. *Si G es un grupo finito y $g \in G$, entonces $|g|$ divide a $|G|$ y por lo tanto $g^{|G|} = 1$.*

Dem. Como $\langle g \rangle$ es un subgrupo de G, entonces $|g| = |\langle g \rangle|$ divide a $|G|$. Esto implica la última afirmación. $\square$

Aplicación 6.8. Si G es un grupo finito de orden primo p, entonces G es cíclico. Esto se debe a que si $1 \neq g \in G$, entonces es $1 \neq |g| \mid p$. Luego $|g| = p$ y por lo tanto $G = \langle g \rangle$.

Observación 6.9. Si un grupo tiene orden 4, entonces es isomorfo a $\mathbb{Z}_4$ o al grupo de Klein $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Luego todos los grupos de orden menor o igual que 5 son abelianos. Notar que $|D_3| = 6$ y D_3 no es abeliano.

Teorema 6.10. *Sea G un grupo y H, K subgrupos tales que $K \subset H$. Entonces $[G:K] < \infty$ si y solo si $[G:H] < \infty$ y $[H:K] < \infty$; en este caso vale*

$$[G:K] = [G:H][H:K].$$

Dem. Supongamos $[G:H] = n < \infty$ y $[H:K] = m < \infty$. Luego existen $g_1, \dots, g_n \in G$ y $h_1, \dots, h_m \in H$ tales que $G = \bigsqcup_{i=1}^n g_iH$ y $H = \bigsqcup_{j=1}^m h_jK$. Luego

$$G = \bigcup_{i=1}^n g_iH = \bigcup_{i=1}^n g_i \left(\bigcup_{j=1}^m h_jK \right) = \bigcup_{i=j=1}^{n,m} g_ih_jK.$$

Vamos a probar que esa unión es disjunta. Sean i_1, i_2, j_1, j_2 tales que $g_{i_1}h_{j_1}K \cap g_{i_2}h_{j_2}K \neq \emptyset$. Como son coclases (son clases de equivalencia), esto implica $g_{i_1}h_{j_1}K = g_{i_2}h_{j_2}K$. Luego existe $k \in K$ tal que $g_{i_1}h_{j_1} = g_{i_2}h_{j_2}k$. Como h_{j_1}, h_{j_2}, k están en H, esto implica $g_{i_1}H = g_{i_2}H$ y por lo tanto $g_{i_1} = g_{i_2}$ (dado que $G = \bigsqcup_{i=1}^n g_iH$). Luego cancelando en $g_{i_1}h_{j_1} = g_{i_2}h_{j_2}k$ deducimos $h_{j_1} = h_{j_2}k$. Pero esta última relación implica $h_{j_1}K = h_{j_2}K$ y por lo mismo que antes es $h_{j_1} = h_{j_2}$. Luego probamos que es $G = \bigsqcup_{i=j=1}^{n,m} g_ih_jK$. Como los g_ih_jK son coclases de K respecto a G, esta igualdad nos dice que es $[G:K] = nm = [G:H][H:K]$. Notar que en el cálculo anterior no usamos que n y m fuesen finitos, luego $[G:H] = \infty$ o $[H:K] = \infty$, entonces $[G:K] = \infty$. $\square$

[5] Estamos usando $\bigsqcup$ para indicar que la unión es disjunta.

7. Acciones

Sea G un grupo y X un conjunto. Una *acción* de G en X es una función $G \times X \xrightarrow{\cdot} X$, $(g, x) \mapsto g \cdot x$, que verifica

$$1 \cdot x = x, \qquad g \cdot (f \cdot x) = (gf) \cdot x, \qquad \forall\, g, f \in G,\ x \in X.$$

Un *G-conjunto* es un par $(X, \cdot)$ en el cual X es un conjunto y $G \times X \xrightarrow{\cdot} X$ es una acción de G en X.

Ejemplo 7.1. 1. Acción *trivial*: dado un grupo G, todo conjunto X es un G-conjunto definiendo $g \cdot x = x$, para todo $g \in G$, $x \in X$.

2. Si $X \neq \emptyset$ es un conjunto, entonces $\mathrm{Biy}(X)$ actúa en X mediante la evaluación $\varphi \cdot x = \varphi(x)$.

3. $\mathcal{S}_n$ actúa en $I_n = \{1, 2, \dots, n\}$ mediante $\sigma \cdot i = \sigma(i)$.

4. $\mathrm{GL}_n(\Bbbk)$ actúa en $\Bbbk^n$ por multiplicación.

5. Si M es un monoide y G es su grupo de invertibles, entonces hay dos acciones naturales de G en M. La acción por *por traslaciones a la izquierda* es $g \cdot m = gm$ y la *acción por conjugación* $g \cdot m = gmg^{-1}$. Un ejemplo de la segunda es $\mathrm{GL}_n(\Bbbk)$ actuando en $M_n(\Bbbk)$ mediante $A \cdot X = AXA^{-1}$.

   Como un caso particular, G actúa sobre si mismo por traslaciones a la izquierda y por conjugación. Esta última la veremos en más detalle un poco más adelante.

6. Si M es una variedad y $f : M \to M$ es un difeomorfismo, entonces $\mathbb{Z}$ actúa en M mediante $n \cdot p = f^n(p)$. Este tipo de acciones son las que se estudian en los *sistemas dinámicos*.

Observación 7.2. Si $G \times X \xrightarrow{\cdot} X$ es una acción y $g \cdot x = y$, entonces $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = \big(g^{-1} g\big) \cdot x = 1 \cdot x = x$. Luego

$$g \cdot x = y \quad \Rightarrow \quad x = g^{-1} \cdot y.$$

Observación 7.3. La acciones que definimos anteriormente son *acciones a la izquierda*. Una *acción a la derecha* de un grupo G en un conjunto X es una función $X \times G \xrightarrow{\bullet} X$, $(x, g) \mapsto x \bullet g$, que verifica

$$x \bullet 1 = x, \qquad (x \bullet g) \bullet f = x \bullet (gf), \qquad \forall\, g, f \in G,\ x \in X.$$

Por ejemplo, en las matrices $M_{m,n}(\Bbbk)$ tenemos que $\mathrm{GL}_m(\Bbbk)$ actúa por multiplicación a la izquierda mientras que $\mathrm{GL}_n(\Bbbk)$ actúa por multiplicación a la derecha.

Toda acción a la derecha induce una acción a la izquierda y recíprocamente, pasando de una a la otra mediante $g \cdot x = x \bullet g^{-1}$. Esto permite trabajar solo con acciones a la izquierda, que es lo que haremos.

Proposición 7.4. *Sea G un grupo y X un conjunto. Existe una correspondencia uno a uno entre las acciones de G en X y los morfismos de grupos de G en* $\mathrm{Biy}(X)$*:*

$$G \times X \xrightarrow{\cdot} X,\ (g, x) \mapsto g \cdot x \qquad \Leftrightarrow \qquad G \xrightarrow{\alpha} \mathrm{Biy}(X),\ g \mapsto \alpha_g : X \to X, \tag{4}$$

definiendo $\alpha_g(x) = g \cdot x$, para todo $g \in G$, $x \in X$.

Dem. Es claro que la correspondencia definida en (4) es uno a uno entre las funciones $G \times X \xrightarrow{\cdot} X$ y las funciones $\alpha : G \to \mathrm{Fun}(X)$, siendo $\mathrm{Fun}(X) = X^X$ el conjunto de las funciones de X en X.
Si $G \times X \xrightarrow{\cdot} X$ es una acción, entonces

$$\alpha_1(x) = 1 \cdot x = x, \quad \forall x \in X \quad \Rightarrow \quad \alpha_1 = \mathrm{id};$$
$$(\alpha_g \circ \alpha_f)(x) = g \cdot (f \cdot x) = (gf) \cdot x = \alpha_{gf}(x), \quad \forall\, g, f \in G,\ x \in X \quad \Rightarrow \quad \alpha_g \circ \alpha_f = \alpha_{gf}, \quad \forall g, f \in G.$$

De estas dos fórmulas deducimos

$$\alpha_g \circ \alpha_{g^{-1}} = \alpha_{gg^{-1}} = \alpha_1 = \mathrm{id}, \quad \alpha_{g^{-1}} \circ \alpha_g = \alpha_{g^{-1}g} = \alpha_1 = \mathrm{id}, \quad \forall g \in G.$$

Esto implica que $\alpha_g : X \to X$ es invertible con inversa $\alpha_{g^{-1}}$. Luego $\alpha_g \in \mathrm{Biy}(X)$, para todo $g \in G$ y por lo tanto $\alpha : G \to \mathrm{Biy}(X) \subset \mathrm{Fun}(X)$ y por lo que vimos α es un morfismo de grupos.

Recíprocamente, si ahora partimos de que $\alpha : G \to \mathrm{Biy}(X)$ es un morfismo de grupos, entonces razonando a la inversa de las dos fórmulas de arriba deducimos que $G \times X \dot{\to} X$ es una acción. $\square$

Notar que a la acción trivial le corresponde el morfismo trivial. Decimos que una acción es *fiel* si $g \cdot x = x$ para todo $x \in X$, implica $g = 1$. Esto equivale a que el morfismo $G \xrightarrow{\alpha} \mathrm{Biy}(X)$ sea un monomorfismo. Luego en este caso es $G \simeq \alpha(G) < \mathrm{Biy}(X)$.

Teorema 7.5 (Cayley)**.** *Todo grupo finito de orden n es isomorfo a algún subgrupo de $\mathcal{S}_n$.*

Dem. Sea G un grupo de orden n. La acción por traslaciones a la izquierda de G en G es fiel

$$g \cdot x = x, \ \forall x \in G \quad \Rightarrow \quad gx = x, \ \forall x \in G \quad \Rightarrow \quad g = 1.$$

Luego si $\alpha : G \to \mathrm{Biy}(G)$ es el morfismo asociado a la acción, entonces $G \simeq \alpha(G) < \mathrm{Biy}(G) \simeq \mathcal{S}_n$. $\square$

Observación 7.6. Las siguientes son dos formas naturales de obtener nuevas acciones a partir de una acción $G \times X \dot{\to} X$.

1. Si $H < G$, entonces H actúa en X por restricción de $G \times X \dot{\to} X$ a $H \times X \dot{\to} X$.

2. Un subconjunto Y de X se dice *G-invariante* o *G-estable* si $g \cdot y \in Y$, para todo $g \in G$ e $y \in Y$. Si $Y \subset X$ es G-invariante, entonces G actúa en Y por restricción de $G \times X \dot{\to} X$ a $G \times Y \dot{\to} Y$.

Ejemplo 7.7. El grupo $\mathrm{Biy}(\mathbb{R}^2)$ actúa en $\mathbb{R}^2$ mediante $\varphi \cdot p = \varphi(p)$. Como el grupo de los movimientos $\mathcal{M}$ es un subgrupo de $\mathrm{Biy}(\mathbb{R}^2)$, entonces $\mathcal{M}$ actúa en $\mathbb{R}^2$ con la misma acción. Si X es un subconjunto de $\mathbb{R}^2$, entonces $\mathrm{Sim}(X)$ actúa en $\mathbb{R}^2$, y como X es invariante respecto a esta acción, entonces $\mathrm{Sim}(X)$ actúa en X.

Si X es un G-conjunto, entonces definimos una relación en X mediante

$$x \sim y \qquad \Leftrightarrow \qquad \exists g \in G : \ x = g \cdot y.$$

Es un ejercicio el probar que esta relación es de equivalencia (para la propiedad recíproca, recordar la observación 7.2). Las clases de equivalencia se llaman las *órbitas* de la acción

$$o(x) = \{g \cdot x : \ g \in G\}, \qquad \forall x \in X.$$

Escribimos $X/G = \{o(x) : \ x \in X\}$ al conjunto cociente.

La acción se dice que es *transitiva* si dados $x, y \in X$ arbitrarios, entonces siempre existe algún elemento $g \in G$ tal que $y = g \cdot x$; esto equivale a decir que en X hay una sola órbita.

Ejemplo 7.8. La acción de G en G por traslaciones a la izquierda es transitiva, mientras que si G no es trivial, entonces la acción por conjugación no lo es, dado que $o(1) = \{1\}$.

Observación 7.9. Las órbitas de la acción de un grupo G en un conjunto X son conjuntos G-invariantes y G actúa transitivamente en cada órbita.

Sea X un G-conjunto.

1. Un elemento $x \in X$ es un *punto fijo* si $g \cdot x = x$, para todo $g \in G$. Escribimos X^G al conjunto de los puntos fijos de X. Notar que X^G es G-invariante y G actúa trivialmente en X^G.

2. Si $x \in X$, el *estabilizador* o *grupo de isotropía* de x es $G_x := \{g \in G : \ g \cdot x = x\}$; claramente $G_x < G$.

Observación 7.10. Sea X un G-conjunto.

1. Si $x \in X$, entonces $x \in X^G$ si y solo si $o(x) = \{x\}$ si y solo si $G_x = G$.

2. Si $G \overset{\alpha}{\to} \operatorname{Biy}(X)$ es el morfismo asociado a la acción, entonces $\operatorname{Ker}(\alpha) = \bigcap_{x \in X} G_x$. Prueba:

$$g \in \operatorname{Ker}(\alpha) \ \Leftrightarrow \ \alpha_g = \mathrm{id} \ \Leftrightarrow \ g \cdot x = x, \ \forall x \in X \ \Leftrightarrow \ g \in G_x, \ \forall x \in X \ \Leftrightarrow \ g \in \bigcap_{x \in X} G_x.$$

Un mapa $\varphi : X \to Y$ entre dos G-conjuntos es un *G-mapa* si $\varphi(g \cdot x) = g \cdot \varphi(x)$, para todo $g \in G$, $x \in X$. Dos G-conjuntos X e Y son *isomorfos* (como G-conjuntos) si existe una G-mapa biyectivo $\varphi : X \to Y$.

Observación 7.11. Si G es un grupo y $H < G$, entonces G actúa en G/H mediante $g \cdot (fH) = (gf)H$.

Proposición 7.12. *Sea X un G-conjunto y $x \in X$. Entonces $o(x) \simeq G/G_x$ como G-conjuntos; luego $|o(x)| = [G : G_x]$ y por lo tanto $|o(x)|$ divide a $|G|$, si G es finito.*

Dem. Sea $x \in X$ y consideramos su órbita $o(x) = \{g \cdot x : \ g \in G\}$. La función $\varphi : G \to o(x)$ definida por $\varphi(g) = g \cdot x$, para todo $g \in G$ es claramente sobreyectiva. Además, si $g, f \in G$, entonces

$$\varphi(g) = \varphi(f) \ \Leftrightarrow \ g \cdot x = f \cdot x \ \Leftrightarrow \ f^{-1} \cdot (g \cdot x) = x \ \Leftrightarrow \ f^{-1} g \cdot x = x \ \Leftrightarrow \ f^{-1} g \in G_x \ \Leftrightarrow \ \overline{g} = \overline{f} \text{ en } G_x.$$

Luego tiene sentido definir $\hat{\varphi} : G/G_x \to o(x)$ mediante $\hat{\varphi}(\overline{g}) := \varphi(g) = g \cdot x$, para todo $g \in G$, y esta función es inyectiva. Como claramente $\hat{\varphi}$ es sobreyectiva, deducimos que es biyectiva. Ahora consideramos a G/G_x como G-conjunto según la observación anterior. Entonces

$$\hat{\varphi}\left(g \cdot \overline{f}\right) = \hat{\varphi}\left(\overline{gf}\right) = gf \cdot x = g \cdot (f \cdot x) = g \cdot \hat{\varphi}\left(\overline{f}\right), \quad \forall g, f \in G.$$

Luego $\hat{\varphi} : G/G_x \to o(x)$ es un G-mapa biyectivo. $\square$

Sea G un grupo y X un G-conjunto. Un *conjunto de representantes de las órbitas* es un subconjunto $X_0 \subset X$ que contiene un y solo un elemento de cada órbita. Notar $X^G \subset X_0$ y $|X_0| = |X/G|$.

Proposición 7.13. *Si un grupo G actúa no trivialmente en un conjunto finito X, entonces existen elementos $x_1, \ldots, x_n \in X$ tales que*

$$|X| = \left|X^G\right| + \sum_{i=1}^{n} [G : G_{x_i}], \ \text{con } [G : G_{x_i}] > 1, \ \forall i = 1, \ldots, n.$$

Dem. Sea $X_0 = \{x_1, \ldots, x_n, x_{n+1}, \ldots, x_m\}$ un conjunto de representantes de las órbitas tal que $X^G = \{x_{n+1}, \ldots, x_m\}$. Luego $X = \bigsqcup_{i=1}^{m} o(x_i)$, implica

$$|X| = \sum_{i=1}^{m} |o(x_i)| = \sum_{i=1}^{n} |o(x_i)| + \sum_{i=n+1}^{m} |o(x_i)| = \sum_{i=1}^{n} [G : G_{x_i}] + \left|X^G\right|. \quad \square$$

A continuación veremos dos aplicaciones de la proposición anterior.

Acción por conjugación. Sea G un grupo. Recordar que si $g \in G$ y definimos $\mathrm{int}_g : G \to G$ mediante $\mathrm{int}_g(x) = gxg^{-1}$, entonces $\mathrm{int}_g \in \mathrm{Aut}(G)$, para todo $g \in G$. Esto define un mapa $\mathrm{int} : G \to \mathrm{Aut}(G) < \mathrm{Biy}(G)$. Este mapa es un morfismo de grupos, luego induce una acción de G en G mediante

$$g \cdot x = \mathrm{int}_g(x) = gxg^{-1}, \qquad \forall g, x \in G.$$

La órbita de $x \in G$ es $[x] := \left\{gxg^{-1} : \ g \in G\right\}$ y se llama la *clase de conjugación* de x. El estabilizador de x es $C_G(x) = \{g \in G : \ gx = xg\}$ y se llama el *centralizador* de x. El conjunto de los puntos fijos es el *centro* del grupo:

$$Z(G) := \{g \in G : \ gx = xg, \ \forall x \in G\}.$$

Notar $Z(G) = \bigcap_{x \in G} C_G(x) = \mathrm{Ker}\,(\mathrm{int})$, luego $Z(G)$ es un subgrupo de G. Observar que la acción por conjugación solo es interesante cuando G no es abeliano. En ese caso las proposiciones 7.12 y 7.13 implican el siguiente resultado.

Proposición 7.14. *Sea G un grupo finito no abeliano. Entonces.*

1. *Si $x \in G$, es $|[x]| = [G : C_G(x)]$. Luego $|[x]|$ divide a $|G|$.*
2. *Existen $x_1, \dots, x_n \in G$, tales que*

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(x_i)], \tag{5}$$

siendo $[G : C_G(x_i)] > 1$, para todo $i = 1, \dots, n$. La fórmula (5) se llama la ecuación de las clases. □

El siguiente resultado es un recíproco parcial del teorema de Lagrange.

Teorema 7.15 (Cauchy)**.** *Sea G un grupo finito y p un número primo que divide a $|G|$. Entonces G contiene algún subgrupo de orden p.*

Dem. Notar que la tesis equivale a probar que en G existe un elemento de orden p (todo grupo de orden primo es cíclico). Sea $X = \{(g_1, \dots, g_p) \in G^p : \ g_1 g_2 \cdots g_p = 1\}$. Notar

$$(g_1, \dots, g_p) \in X \ \Leftrightarrow \ g_1 g_2 \cdots g_p = 1 \ \Leftrightarrow \ g_2 \cdots g_p = g_1^{-1} \ \Leftrightarrow \ g_2 \cdots g_p g_1 = 1 \ \Leftrightarrow \ (g_2, \dots, g_p, g_1) \in X.$$

Luego tiene sentido definir $\sigma : X \to X$ mediante

$$\sigma(g_1, g_2, \dots, g_p) = (g_2, \dots, g_p, g_1), \quad \forall (g_1, \dots, g_p) \in X.$$

Claramente $\sigma \in \mathrm{Biy}(X)$ y verifica $\sigma^p = \mathrm{id}$, luego la proposición 5.8 implica que podemos definir un morfismo $\mathbb{Z}_p \to \mathrm{Biy}(X)$ mediante $\overline{m} \mapsto \sigma^m$, para todo $m \in \mathbb{Z}$. Este morfismo no es trivial y por lo tanto induce una acción no trivial $\mathbb{Z}_p \times X \to X$. Luego la proposición 7.13 implica que existen $x_1, \dots, x_n \in X$ tales que

$$|X| = \left|X^{\mathbb{Z}_p}\right| + \sum_{i=1}^{n} [\mathbb{Z}_p : (\mathbb{Z}_p)_{x_i}], \ \text{con } [\mathbb{Z}_p : (\mathbb{Z}_p)_{x_i}] > 1, \ \forall i = 1, \dots, n.$$

Notar que la función $\varphi : G^{p-1} \to X$ definida por $\varphi(g_1, \dots, g_{p-1}) = \left(g_1, \dots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1}\right)$ es biyectiva. Luego $|X| = |G|^{p-1}$ y $[\mathbb{Z}_p : (\mathbb{Z}_p)_{x_i}] = p$, para todo $i = 1, \dots, n$; luego $p \mid \left|X^{\mathbb{Z}_p}\right|$. Además $(1, \dots, 1) \in X^{\mathbb{Z}_p}$, luego $\left|X^{\mathbb{Z}_p}\right| \neq 0$. Por lo tanto existe $(g_1, \dots, g_p) \in X^{\mathbb{Z}_p}$ tal que $(g_1, \dots, g_p) \neq (1, \dots, 1)$. Luego $g_1 \neq 1$ y $g_1^p = 1$; como p es primo, esto implica $|g_1| = p$. □

8. Subgrupos normales

Un subgrupo N de un grupo G se dice *normal* si verifica $gNg^{-1} \subset N$, para todo $g \in G$. Escribiremos $N \lhd G$ para indicar la normalidad.

Proposición 8.1. *Sea G un grupo y N un subgrupo. Las siguientes afirmaciones son equivalentes.*

1. *N es normal.*
2. *$gNg^{-1} = N$, para todo $g \in G$.*
3. *$gN = Ng$, para todo $g \in G$.*
4. *Las relaciones $\equiv \pmod{N}$ y $\equiv_d \pmod{N}$ coinciden.*
5. *$G/N = N\backslash G$.*

Dem. Es claro que (2) equivale con (3). Dado que es equivalente tener una relación de equivalencia en un conjunto a tener una partición del conjunto (en clases de equivalencia), se deduce que (3), (4) y (5) son equivalentes.

Es claro que (2) implica (1). Probaremos el recíproco. Sea $g \in G$. Sabemos que vale $gNg^{-1} \subset N$. Aplicando esto a g^{-1} obtenemos $g^{-1}Ng \subset N$, lo cual implica $N \subset gNg^{-1}$. Luego tenemos la doble inclusión y por lo tanto $gNg^{-1} = N$. Luego (1) y (2) son equivalentes y esto termina la prueba. □

Proposición 8.2. *Si $\varphi : G \to F$ es un morfismo de grupos, entonces $\operatorname{Ker}(\varphi) \lhd G$.*

Dem. Ejercicio. □

Proposición 8.3. *Si $N_i \lhd G$, para todo $i \in I$, entonces $\bigcap_{i\in I} N_i \lhd G$*

Dem. Ejercicio. □

Ejemplos 8.4.

1. El subgrupo trivial $\{1\}$ y el grupo G son subgrupos normales de G.
2. Si $K < G$ y $K \subset Z(G)$, entonces $K \lhd G$; en particular $Z(G) \lhd G$.
3. Es un ejercicio el probar que si $N < G$ y $[G : N] = 2$, entonces $N \lhd G$.
4. Si G actúa en X, entonces $\bigcap_{x\in X} G_x \lhd G$ (ver la observación 7.10).
5. Sea $D_3 = \{1, b, b^2, a, ab, ab^2\}$ el grupo diedral visto en el ejemplo 6.2. Si $H = \langle a\rangle = \{1, a\}$, vimos que $bH \neq Hb$, luego H no es normal. Si $K = \langle b\rangle = \{1, b, b^2\}$, entonces $[G : K] = 2$ y por lo tanto $K \lhd D_3$.
6. Como $\det : \mathrm{GL}_n(\Bbbk) \to \Bbbk^\times$ es un morfismo, deducimos $\mathrm{SL}_n(\Bbbk) \lhd \mathrm{GL}_n(\Bbbk)$.

Observaciones 8.5.

1. Si G es abeliano, entonces todo subgrupo de G es normal. El recíproco es falso: los cuaternios son un grupo no abeliano, pero todos sus subgrupos son normales (ejercicio).
2. Si $N \lhd G$ y $N < H < G$, entonces $N \lhd H$.
3. La normalidad **no es transitiva**, *i.e.* dados $N < H < G$, si $N \lhd H$ y $H \lhd G$, esto no implica $N \lhd G$.

Si G es un grupo y H y K son dos subgrupos, entonces llamamos $H \vee K$ al menor subgrupo que los contiene. El problema es que en general no tenemos una buena descipción de $H \vee K$. El siguiente resultado muestra que esto se simplifica mucho cuando alguno de los subgrupos es normal.

Proposición 8.6. *Sean G un grupo y K, H subgrupos de G.*

1. *Si $K \cap H = \{1\}$, entonces todo elemento de HK se escribe de fórma única como hk, con $h \in H$ y $k \in K$. Lo mismo sucede con KH.*

2. *Si $K \lhd G$ o $H \lhd G$, entonces $KH < G$. Luego $K \vee H = KH = HK$.*

3. *Si $K \lhd G$ y $H \lhd G$, entonces $KH \lhd G$.*

4. *Si $K \lhd G$, $H \lhd G$ y $K \cap H = \{1\}$, entonces $kh = hk$, para todo $k \in K$, $h \in H$.*

Dem. (1). Sean $h_1, h_2 \in H$ y $k_1, k_2 \in K$ tales que $h_1 k_1 = h_2 k_2$. Entonces $h_2^{-1} h_1 = k_2 k_1^{-1} \in K \cap H = \{1\}$, luego $h_2^{-1} h_1 = k_2 k_1^{-1} = 1$, lo cual implica $h_1 = h_2$ y $k_1 = k_2$.

(2). Supongamos $K \lhd G$ y $H < G$. Si $k \in K$ y $h \in H$, entonces escribiendo $kh = h(h^{-1}kh)$ deducimos $KH \subset HK$. Esto implica $KH = HK$ lo cual a su vez implica $KH < G$ (ejercicio). Lo mismo se obtiene si es $K < G$ y $H \lhd G$.

(3). Sean $k \in K$, $h \in H$ y $g \in G$, entonces $g(kh)g^{-1} = \left(gkg^{-1}\right)\left(ghg^{-1}\right) \in KH$. Luego $KH \lhd G$.

(4). Si dados $k \in K$ y $h \in H$, consideramos su *conmutador* $[k, h] := khk^{-1}h^{-1}$, entonces $K \lhd G$ y $H \lhd G$ implican $[k, h] \in K \cap H = \{1\}$; luego $[k, h] = 1$, lo cual equivale a $kh = hk$. $\square$

Observación 8.7. Si G es un grupo y H, K son subgrupos tales que $G = KH$ y $kh = hk$, para todo $k \in K$, $h \in H$, entonces es fácil de probar que K y H son subgrupos normales de G. Luego si $G = KH$, entonces vale un recíproco parcial de la parte (4) de la proposición anterior.

Grupo cociente.

Proposición 8.8. *Si G es un grupo y N es un subgrupo normal, entonces G/N admite una estructura de grupo de forma tal que la proyección canónica $\pi : G \to G/N$ es un morfismo.*

Dem. Sean $g_1, g_2, f_1, f_2 \in G$. Si $f_1 \equiv g_1 (\mathrm{mod}\ N)$ y $f_2 \equiv g_2 (\mathrm{mod}\ N)$, entonces existen $n_1, n_2 \in N$ tales que $f_1 = g_1 n_1$ y $f_2 = g_2 n_2$. Luego

$$f_1 f_2 = g_1 n_1 g_2 n_2 = g_1 g_2 \left(g_2^{-1} n_1 g_2\right) n_2, \quad \text{con } \left(g_2^{-1} n_1 g_2\right) n_2 \in N \quad \Rightarrow \quad f_1 f_2 \equiv g_1 g_2 (\mathrm{mod}\ N).$$

Luego tiene sentido definir un producto en G/N mediante $\overline{f}\,\overline{g} = \overline{fg}$, para todo $f, g \in G$. El resto es directo. $\square$

Observación 8.9. Si $N \lhd G$ y $\pi : G \to G/N$ es la proyección canónica, entonces $\operatorname{Ker}(\pi) = N$. Luego los subgrupos normales de G son los núcleos de morfismos que salen de G.

Observación 8.10. Si en un diagrama de grupos y morfismos del tipo

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

pensamos las flechas (morfismos) como caminos, entonces tenemos dos formas de ir de G a F, mediante φ o mediante $\psi \circ \mu$ (primero vamos por μ y luego por ψ). Si se everifica que $\psi \circ \mu = \varphi$, entonces decimos que el diagrama *conmuta*. Esto quiere decir que da lo mismo ir por uno u otro camino. Esto se generaliza a cualquier diagrama de ese tipo. Por ejemplo la conmutatividad de

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & F \arrow[d, "\beta"] \\ H \arrow[r, "\psi"'] & K \end{tikzcd}$$

significa que vale $\psi \circ \alpha = \beta \circ \varphi$.

Proposición 8.11 (Propiedad universal del cociente)**.** *Sea* $\varphi : G \to F$ *un morfismo. Si* $N \lhd G$ *y* $N \subset \operatorname{Ker}(\varphi)$*, entonces existe un único morfismo* $\hat{\varphi} : G/N \to F$ *tal que el siguiente diagrama conmuta*

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

Además $\operatorname{Im}(\hat{\varphi}) = \operatorname{Im}(\varphi)$ *y* $\operatorname{Ker}(\hat{\varphi}) = \operatorname{Ker}(\varphi)/N$*.*

Notar que la conmutatividad del diagrama equivale a que se verifique $\hat{\varphi}(\overline{g}) = \varphi(g)$, para todo $g \in G$.

Dem. Si $g, f \in G$ y $n \in N$ son tales que $g = fn$, entonces $\varphi(g) = \varphi(fn) = \varphi(f)\varphi(n) = \varphi(f)1 = \varphi(f)$. Luego probamos

$$\overline{g} = \overline{f} \in G/N \quad \Rightarrow \quad \varphi(g) = \varphi(f).$$

Esta fórmula implica que tiene sentido definir una función $\hat{\varphi} : G/N \to F$ mediante $\hat{\varphi}(\overline{g}) = \varphi(g)$, para todo $g \in G$. Es fácil de probar que $\hat{\varphi}$ es un morfismo:

$$\hat{\varphi}\left(\overline{g}\,\overline{f}\right) = \hat{\varphi}\left(\overline{gf}\right) = \varphi(gf) = \varphi(g)\varphi(f) = \hat{\varphi}(\overline{g})\,\hat{\varphi}\left(\overline{f}\right).$$

Es claro que vale $\operatorname{Im}(\hat{\varphi}) = \operatorname{Im}(\varphi)$. La igualdad $\operatorname{Ker}(\hat{\varphi}) = \operatorname{Ker}(\varphi)/N$ se deduce de lo siguiente

$$\overline{g} \in \operatorname{Ker}(\hat{\varphi}) \;\Leftrightarrow\; \hat{\varphi}(\overline{g}) = 1 \;\Leftrightarrow\; \varphi(g) = 1 \;\Leftrightarrow\; g \in \operatorname{Ker}(\varphi) \;\Leftrightarrow\; \overline{g} \in \operatorname{Ker}(\varphi)/N. \quad \square$$

El siguiente resultado es un corolario directo de la propiedad universal del cociente.

Teorema 8.12 (Primer teorema de isomorfismo)**.**
Si $\varphi : G \to F$ *es un morfismo, entonces existe un monomorfismo* $\hat{\varphi} : G/\operatorname{Ker}(\varphi) \to F$ *tal que el siguiente diagrama conmuta*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & F \\ G/\operatorname{Ker}(\varphi) \arrow[ur, hook, "\hat{\varphi}"'] & \end{tikzcd}$$

Luego $\operatorname{Im}(\varphi) \simeq G/\operatorname{Ker}(\varphi)$*.* $\square$

Un enunciado equivalente al anterior es el siguiente.

Teorema 8.13. *Si* $\varphi : G \to F$ *es un epimorfismo, entonces existe un isomorfismo* $\hat{\varphi} : G/\operatorname{Ker}(\varphi) \to F$ *tal que el siguiente diagrama conmuta*

$$\begin{tikzcd} G \arrow[r, two heads, "\varphi"] \arrow[d, "\pi"'] & F \\ G/\operatorname{Ker}(\varphi) \arrow[ur, "\simeq", "\hat{\varphi}"'] & \end{tikzcd}$$

Luego $F \simeq G/\operatorname{Ker}(\varphi)$*.* $\square$

Teorema 8.14 (Segundo teorema de isomorfismo).
Sea G un grupo, $K < G$ y $N \lhd G$. Entonces $N \lhd NK$, $N \cap K \lhd K$ y
$$\frac{NK}{N} \simeq \frac{K}{N \cap K}.$$
Dem. Empezamos observando que $K < G$ y $N \lhd G$ implican $NK < G$, y como $N \subset NK$, entonces $N \lhd NK$. Consideremos la composición $K \hookrightarrow NK \twoheadrightarrow NK/N$, es decir el morfismo $\varphi : K \to NK/N$ definido por $\varphi(k) = \overline{k}$, para todo $k \in K$. Si $n \in N$ y $k \in K$, entonces en NK/N vale $\overline{nk} = \overline{n}\,\overline{k} = \overline{1}\,\overline{k} = \overline{k} = \varphi(k)$, luego φ es sobreyectiva. Además, si $k \in K$, entonces
$$k \in \operatorname{Ker}(\varphi) \quad\Leftrightarrow\quad \varphi(k) = \overline{1} \in NK/N \quad\Leftrightarrow\quad \overline{k} = \overline{1} \in NK/N \quad\Leftrightarrow\quad k \in N$$
Luego $\operatorname{Ker}(\varphi) = N \cap K$. Esto implica $N \cap K \lhd K$. Finalmente el primer teorema de isomorfismo aplicado a φ implica $\frac{NK}{N} \simeq \frac{K}{N \cap K}$. $\square$

Lo siguiente permite construir morfismos entre cocientes.

Proposición 8.15. *Sean G, F grupos, $N \lhd G$ y $K \lhd F$. Si $\varphi : G \to F$ es un morfismo tal que $\varphi(N) \subset K$, entonces existe un único morfismo $\hat{\varphi} : G/N \to F/K$ tal que el siguiente diagrama conmuta*

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

Además

1. $\operatorname{Ker}(\hat{\varphi}) = \varphi^{-1}(K)/N$*. Luego $\hat{\varphi}$ es inyectivo si y solo si $\varphi^{-1}(K) = N$;*
2. *$\hat{\varphi}$ es sobreyectivo si y solo si $F = \operatorname{Im}(\varphi)K$.*

Notar que la conmutatividad del diagrama equivale a que se verifique $\hat{\varphi}(\overline{g}) = \overline{\varphi(g)}$, para todo $g \in G$.

Dem. El morfismo $\hat{\varphi}$ se obtiene aplicando la propiedad universal a $\pi \circ \varphi : G \to F/K$, dado que $\varphi(N) \subset K$ implica $N \subset \operatorname{Ker}(\pi \circ \varphi)$. Notar
$$g \in \operatorname{Ker}(\pi \circ \varphi) \quad\Leftrightarrow\quad \overline{\varphi(g)} = \overline{1} \in F/K \quad\Leftrightarrow\quad \varphi(g) \in K \quad\Leftrightarrow\quad g \in \varphi^{-1}(K).$$
Luego $\operatorname{Ker}(\hat{\varphi}) = \operatorname{Ker}(\pi \circ \varphi)/N = \varphi^{-1}(K)/N$; esto prueba la primer afirmación. Para la segunda, observar
$$\operatorname{Im}(\hat{\varphi}) = F/K \;\Leftrightarrow\; \forall f \in F,\ \exists g \in G :\ \overline{f} = \overline{\varphi(g)} \in F/K \;\Leftrightarrow\; \forall f \in F,\ \exists g \in G,\ k \in K :\ f = \varphi(g)k. \quad \square$$

Teorema 8.16 (Tercer teorema de isomorfismo).
Sea G un grupo y $N < H < G$ tales que $N \lhd G$ y $H \lhd G$. Entonces $H/N \lhd G/N$ y
$$\frac{G/N}{H/N} \simeq \frac{G}{H}.$$

Dem. Como es $N \subset H$, entonces el automorfismo identidad de G induce un morfismo $\varphi : G/N \to G/H$ tal que el siguiente diagrama conmuta

$$\begin{tikzcd} G \arrow[r, "\mathrm{id}"] \arrow[d, "\pi"'] & G \arrow[d, "\pi"] \\ G/N \arrow[r, "\varphi"'] & G/H \end{tikzcd} \qquad \Leftrightarrow \qquad \varphi(gN) = gH,\ \forall g \in G.$$

Notar que φ es sobreyectivo y su núcleo es H/N, luego $H/N \lhd G/N$ y el resto de la tesis se obtiene aplicando a φ el primer teorema de isomorfismo. $\square$

Observación 8.17. Si $\varphi : G \to F$ es un morfismo, entonces vale lo siguiente.

1. Si $H \lhd G$, entonces $\varphi(H) \lhd \mathrm{Im}(\varphi)$.
2. Si $K \lhd F$, entonces $\varphi^{-1}(K) \lhd G$.

Recordar que en la familia de subgrupos de un grupo tenemos el orden dado por la inclusión. Además, si $\varphi : G \to F$ es un morfismo, $H < G$ y $K < F$, entonces $\varphi(H) < F$ y $\mathrm{Ker}\,(\varphi) < \varphi^{-1}(K) < G$.

Proposición 8.18. *Sean G un grupo, N un subgrupo normal y $\pi : G \to G/N$ la proyección canónica. Consideramos $\mathcal{S} = \{H :\ N < H < G\}$ y $\hat{\mathcal{S}} = \{K :\ K < G/N\}$. Entonces las correspondencias*

$$\begin{array}{ccc} \mathcal{S} & \to & \hat{\mathcal{S}} \\ H & \mapsto & \pi(H) = H/N \end{array}, \qquad \begin{array}{ccc} \hat{\mathcal{S}} & \to & \mathcal{S} \\ K & \mapsto & \pi^{-1}(K) \end{array}$$

son monótonas crecientes estrictas, preservan la normalidad y son inversas una de la otra.

Dem. Es claro que esas correspondencias son monótonas crecientes. Como $\pi : G \to G/N$ es sobreyectiva, entonces de la observación anterior deducimos que también preservan la normalidad. Veremos ahora que son inversas una de la otra. Sea $K < G/N$, es claro que vale $\pi\big(\pi^{-1}(K)\big) \subset K$, y como $\pi : G \to G/N$ es sobreyectiva, entonces es fácil de probar que vale también la inclusión contraria; luego $\pi\big(\pi^{-1}(K)\big) = K$. Sea ahora $N < H < G$. En este caso es claro que vale $H \subset \pi^{-1}\big(\pi(H)\big)$; veremos ahora la inclusión contraria. Sea $g \in \pi^{-1}\big(\pi(H)\big)$, entonces

$$\exists h \in N \text{ tal que } \pi(g) = \pi(h) \quad \Rightarrow \quad \overline{g} = \overline{h} \in G/N \quad \Rightarrow \quad \exists n \in N \text{ tal que } g = hn \quad \overset{N \subset H}{\Rightarrow} \quad g \in H.$$

Luego $\pi^{-1}\big(\pi(H)\big) \subset H$ y por lo tanto $\pi^{-1}\big(\pi(H)\big) = H$. Luego probamos que las correspondencias son inversas una de la otra, y como son monótonas, deducimos que son monótonas estrictas. □

Observación 8.19. En la correspondencia anterior, si tenemos $N < H < G$ y $H \lhd G$, entonces el tercer teorema de isomorfismo nos dice que los cocientes correspondientes G/H y $(G/N)/(H/N)$ son isomorfos.

Aplicando el primer teorema de isomorfismo se deduce el siguiente.

Corolario 8.20. *Sea $\varphi : G \to F$ un epimorfismo. Consideramos $\mathcal{S} = \{H :\ \mathrm{Ker}\,(\varphi) < H < G\}$ y $\hat{\mathcal{S}} = \{K :\ K < F\}$. Entonces las correspondencias*

$$\begin{array}{ccc} \mathcal{S} & \to & \hat{\mathcal{S}} \\ H & \mapsto & \varphi(H) \end{array}, \qquad \begin{array}{ccc} \hat{\mathcal{S}} & \to & \mathcal{S} \\ K & \mapsto & \varphi^{-1}(K) \end{array}$$

son monótonas crecientes estrictas, preservan la normalidad y son inversas una de la otra. □

El normalizador. Dos subgrupos H y K de G son *conjugados* si existe $g \in G$ tal que $H = gKg^{-1}$, *i.e.* si $H = \mathrm{int}_g(K)$. Claramente los subgrupos conjugados son isomorfos como grupos. El *normalizador* de un subgrupo H de G es el conjunto $N_G(H) = \{g \in G :\ gHg^{-1} = H\}$. Notar $H \lhd G$ si y solo si $N_G(H) = G$.

Proposición 8.21. *Si $H < G$, entonces $N_G(H)$ es el mayor subgrupo de G que contiene a H como subgrupo normal. Además*

$$\#\{K < G :\ K \text{ es conjugado de } H\} = [G : N_G(H)].$$

Dem. Sea $\mathcal{S}$ el conjunto de los subgrupos de G. Si consideramos G actuando en $\mathcal{S}$ por conjugación, entonces la órbita de H es $\{K < G :\ K \text{ es conjugado de } H\}$ y el estabilizador de H es $N_G(H)$. Luego la tesis se deduce de la proposición 7.12 □

Obtención de subgrupos normales

Proposición 8.22. *Sea G un grupo y $H < G$. Consideremos $K := \bigcap_{g\in G} gHg^{-1}$. Entonces:*

1. *K es el mayor subgrupo normal de G contenido en H.*
2. *Existe un morfismo inyectivo $G/K \rightarrowtail \mathrm{Biy}(G/H)$.*

Dem. Consideramos la acción de G en G/H definida por $g \cdot (fH) = gfH$. Empezamos observando que si $g \in G$, entonces el estabilizador de gH es gHg^{-1}:

$$f \cdot (gH) = gH \quad \Leftrightarrow \quad fgH = gH \quad \Leftrightarrow \quad g^{-1}fg \in H \quad \Leftrightarrow \quad f \in gHg^{-1}.$$

Luego $K = \mathrm{Ker}\,(\alpha)$, siendo $\alpha : G \to \mathrm{Biy}(G/H)$ el morfismo asociado a la acción (observación 7.10). Esto implica $K \lhd G$ y $K \subset H$. Además, si $N \lhd G$ y $N \subset H$, entonces

$$N = gNg^{-1} \subset gHg^{-1}, \quad \forall g \in G \quad \Rightarrow \quad N \subset \bigcap_{g\in G} gHg^{-1} = K.$$

Esto prueba la primer afirmación. La segunda, es el primer teorema de isomorfismo aplicado a α. La tercera es inmediata a partir de la segunda. $\square$

Corolario 8.23. *Sea G un grupo finito y H un subgrupo de G.*

1. *Si $|G|$ no divide a $[G : H]!$, entonces existe $K \lhd G$ tal que $\{1\} \neq K \subset H$.*
2. *Si $[G : H] = p$, siendo p el menor número primo que divide a $|G|$, entonces $H \lhd G$.*

Dem. La proposición 8.22 nos dice que existe $K \lhd G$, $K \subset H$ y un morfismo inyectivo $G/K \rightarrowtail \mathrm{Biy}(G/H)$. Entonces G/K es isomorfo a un subgrupo de $\mathrm{Biy}(G/H)$ y aplicando el teorema de Lagrange obtenemos

$$[G : K] \mid [G : H]!. \tag{6}$$

Si es $K = \{1\}$, entonces (6) implica que $|G|$ divide a $[G : H]!$. Luego si $|G|$ no divide a $[G : H]!$, entonces $K \neq \{1\}$.

En el segundo caso, de (6) obtenemos $[G : K] \mid p!$. Escribiendo $[G : K] = [G : H][H : K] = p[H : K]$, deducimos $[H : K] \mid (p-1)!$ y al ser $[H : K]$ un divisor de $|G|$, deducimos $[H : K] = 1$. Luego $H = K$. $\square$

Ejemplo 8.24. Sea G un grupo de orden 15. Por el teorema de Cauchy sabemos que existen subgrupos H y K de G tales que $|H| = 3$ y $|K| = 5$. Luego el corolario 8.23 implica $K \lhd G$.

Ejemplo 8.25. Sea G un grupo de orden 99. Al ser $99 = 3^2 11$, sabemos que G contiene subgrupos H y K tales que $|H| = 3$ y $|K| = 11$. Aplicando el corolario 8.23 encontramos que existe $\{1\} \neq N \lhd G$ tal que $N < K$; al ser $|K|$ primo deducimos $K = N$, luego $K \lhd G$. Claramente $H \cap K = \{1\}$, luego $HK < G$ y $|HK| = 33$. Al ser $[G : HK] = 3$, el corolario 8.23 implica $HK \lhd G$.

En lo que sigue usaremos reiteradamente la proposición 8.6.

Producto semidirecto. Sea G un grupo y N y K subgrupos de G tales que $N \cap K = \{1\}$ y $G = NK$. Estas condiciones implican que todo elemento de G se escribe en forma única como producto de un elemento de N por uno de K, luego la función $\varphi : N \times K \to G$ definida por $\varphi(n, k) = nk$ es una biyección.

Si vale $N \lhd G$, entonces K actúa en N definiendo $k \cdot n = knk^{-1}$. Esta acción verifica $k \cdot (n_1 n_2) = (k \cdot n_2)(k \cdot n_2)$, luego induce un morfismo de grupos $\alpha : K \to \mathrm{Aut}(N)$, dado por $\alpha_k(n) = k \cdot n$. Notar que vale

$$(n_1 k_1)(n_2 k_2) = n_1 (k_1 \cdot n_2) k_1 k_2, \qquad \forall n_1, n_2 \in N,\ k_1, k_2 \in K.$$

Luego podemos copiar mediante la biyección $\varphi : N \times K \to G$ la estructura de grupo de G, obteniendo un producto $*$ en $N \times K$ definido por

$$(n_1, k_1) * (n_2, k_2) = \big(n_1 (k_1 \cdot n_2),\, k_1 k_2\big), \qquad \forall n_1, n_2 \in N,\ k_1, k_2 \in K. \tag{7}$$

Con este producto $N \times K$ es un grupo y $\varphi : N \times K \to G$ es un isomorfismo de grupos.

Dado que estamos asumiendo $N \lhd G$, entonces sabemos por la observación 8.7 que es $K \lhd G$ si y solo si los elementos de K conmutan con los de N, lo cual a su vez equivale a que la acción $K \times N \xrightarrow{\cdot} N$ sea trivial o a que α sea el morfismo trivial. Pero en ese caso obtenemos $n_1 k_1 n_2 k_2 = n_1 n_2 k_1 k_2$, para todo $n_1, n_2 \in N$, $k_1, k_2 \in K$. Luego si $K \lhd G$, entonces el producto dado por (7) queda en $(n_1, k_1) * (n_2, k_2) = (n_1 n_2,\, k_1 k_2)$ y por lo tanto la estructura de grupo inducida en $N \times K$ es la del producto directo.

Recíprocamente, consideremos dos grupos N y K y un morfismo de grupos $\alpha : K \to \mathrm{Aut}(N)$. El mapa $\alpha : K \to \mathrm{Aut}(N) < \mathrm{Biy}(N)$ induce una acción $K \times N \xrightarrow{\cdot} N$ definida por $k \cdot n = \alpha_k(n)$. Si definimos un producto $*$ en $N \times K$ mediante (7), entonces es un ejercicio el probar que el conjunto $N \times K$ con este producto es un grupo, que se llama el *producto semidirecto* de N y K y lo escribimos $N \rtimes_\alpha K$. En $N \rtimes_\alpha K$ vale

$$(n_1, 1) * (n_2, 1) = (n_1 n_2,\, 1), \quad (1, k_1) * (1, k_2) = (1,\, k_1 k_2), \quad \forall n_1, n_2 \in N,\ k_1, k_2 \in K.$$

Luego si definimos $N_0 = \{(n, 1) :\ n \in N\}$ y $K_0 = \{(1, k) :\ k \in K\}$, obtenemos que N_0 y K_0 son subgrupos de $N \rtimes_\alpha K$ y los mapas $n \mapsto (n, 1)$ y $k \mapsto (1, k)$ definen isomorfismos $N \simeq N_0$ y $K \simeq K_0$. El inverso en $N \rtimes_\alpha K$ está dado por $(n, k)^{-1} = \left(\left(k^{-1} \cdot n\right)^{-1}, k^{-1}\right)$. Usando está fórmula es fácil probar que N_0 es normal en $N \rtimes_\alpha K$. Además para todo $n \in N$ y $k \in K$, valen

$$(n, 1) * (1, k) = (n, k), \quad (1, k) * (n, 1) = (k \cdot n, k), \quad (1, k) * (n, 1) * (1, k)^{-1} = (k \cdot n, 1). \tag{8}$$

luego es $N \rtimes_\alpha K = N_0 K_0$ y claramente vale $N_0 \cap K_0 = \{(1, 1)\}$. Así en $N \rtimes_\alpha K$ tenemos la misma descomposición que teníamos en G.

Notar que $N \rtimes_\alpha K = N \times K$ si y solo si α es trivial. Además, si α no es trivial entonces existen $k \in K$ y $n \in N$ tales que $k \cdot n \neq n$, luego $(n, 1) * (1, k) \neq (1, k) * (n, 1)$, y por lo tanto $N \rtimes_\alpha K$ no es abeliano (aunque lo sean N y K).

Resumimos la discusión anterior en el siguiente resultado.

Teorema 8.26. *Un grupo G verifica que existen $N \lhd G$ y $K < G$ tales que $G = NK$ y $N \cap K = \{1\}$, si y solo si G es isomorfo a un producto semidirecto $N \rtimes_\alpha K$, para cierto morfismo $\alpha : K \to \mathrm{Aut}(N)$. Además $K \lhd G$ si y solo si α es el morfismo trivial si y solo si $G \simeq N \times K$.* □

Ejemplo 8.27. Consideremos el grupo diedral $D_n = \langle a, b :\ a^n = b^2 = 1,\ ab = ba^{n-1} \rangle$, $n \geq 3$. Sean $N = \langle a \rangle$ y $K = \langle b \rangle$. Es $D_n = NK$, $N \cap K = \{1\}$ y N tiene índice 2, luego es normal. Entonces

$$D_n \simeq N \rtimes_\alpha K \simeq C_n \rtimes_\alpha C_2.$$

Si escribimos los grupos cíclicos mediante $C_n = \langle a \rangle$ y $C_2 = \langle b \rangle$, entonces $\alpha : C_2 \to \mathrm{Aut}(C_n)$ está definido por $\alpha_1 = \mathrm{id}$ y $\alpha_b(x) = x^{-1}$, para todo $x \in C_n$. Por otro lado, si escribimos $C_n = \mathbb{Z}_n$ y $C_2 = \mathbb{Z}_2$ (notación aditiva), entonces

$$D_n \simeq N \rtimes_\alpha K \simeq \mathbb{Z}_n \rtimes_\alpha \mathbb{Z}_2.$$

y $\alpha : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n)$ está definido por $\alpha_{\overline{0}} = \mathrm{id}$ y $\alpha_{\overline{1}} = -\,\mathrm{id}$.

Grupos de orden pq. Como una aplicación de lo anterior veremos la clasificación de los grupos de orden pq, siendo p y q primos tales que $p < q$.

Lo primero es obtener grupos de orden pq. Un grupo abeliano de orden pq es $\mathbb{Z}_{pq}$; notar que al ser p y q primos distintos, vale $\mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq}$. Un grupo no abeliano de orden pq se podría obtener mediante el producto semidirecto $\mathbb{Z}_q \rtimes_\tau \mathbb{Z}_p$, siendo $\tau : \mathbb{Z}_p \to \operatorname{Aut}(\mathbb{Z}_q)$ un morfismo no trivial. Sabemos que ese morfismo τ es de la forma $\tau_{\overline{k}}(x) = \overline{r}^k x$, para todo $\overline{k} \in \mathbb{Z}_p, x \in \mathbb{Z}_q$, para cierto $r \in \mathbb{Z}^+$ tal que $r^p \equiv 1 (\operatorname{mod}\ q)$ y $r \not\equiv 1 (\operatorname{mod}\ q)$. El siguiente resultado da una condición necesaria y suficiente para que exista un tal r.

Lema 8.28. *Sean p y q primos. Entonces existe $r \in \mathbb{Z}^+$ tal que $r^p \equiv 1 (\operatorname{mod}\ q)$ y $r \not\equiv 1 (\operatorname{mod}\ q)$ si y solo si $q \equiv 1 (\operatorname{mod}\ p)$.*

Dem. Sea $r \in \mathbb{Z}^+$. Si r verifica $r^p \equiv 1 (\operatorname{mod}\ q)$ y $r \not\equiv 1 (\operatorname{mod}\ q)$, entonces vale $\overline{r}^p = \overline{1}$ y $\overline{r} \neq \overline{1}$ en $\mathbb{Z}_q$. Esto implica $\overline{r} \in \mathbb{Z}_q^\times$ y como p es primo, entonces $|\overline{r}| = p$ en $\mathbb{Z}_q^\times$. Luego aplicando el teorema de Lagrange deducimos $p \mid \left|\mathbb{Z}_q^\times\right| = q - 1$, lo cual equivale a $q \equiv 1 (\operatorname{mod}\ p)$.

Recíprocamente, $q \equiv 1 (\operatorname{mod}\ p)$ implica $p \mid \left|\mathbb{Z}_q^\times\right|$. Luego aplicando el teorema de Cauchy sabemos que existe $\overline{r} \in \mathbb{Z}_q^\times$ tal que $|\overline{r}| = p$ en $\mathbb{Z}_q^\times$, lo cual equivale a $r^p \equiv 1 (\operatorname{mod}\ q)$ y $r \not\equiv 1 (\operatorname{mod}\ q)$. □

Observación 8.29. La condición $q \equiv 1 (\operatorname{mod}\ p)$ equivale a $p \mid q-1$ y por lo tanto tiene que ser $p \leq q-1 < q$. Luego solo puede darse $q \equiv 1 (\operatorname{mod}\ p)$ cuando es $p < q$.

Teorema 8.30. *A menos de isomorfismo existen a lo más dos grupos de orden pq con $p < q$ primos: el cíclico $\mathbb{Z}_{pq}$ y el no abeliano $G = \langle a, b :\ a^p = b^q = 1,\ aba^{-1} = b^r \rangle$, siendo $r \in \mathbb{Z}^+$ tal que $r^p \equiv 1 (\operatorname{mod}\ q)$ y $r \not\equiv 1 (\operatorname{mod}\ q)$. Esta última posibilidad solo puede ocurrir si $q \equiv 1 (\operatorname{mod}\ p)$.*

Dem. Sea G un grupo de orden pq. Aplicando el teorema de Cauchy sabemos que existen subgrupos N y K tales que $|N| = q$ y $|K| = p$. Al ser p, q primos distintos deducimos $N \cap K = \{1\}$, luego $G = NK$. El corolario 8.23 implica que N es normal. Luego es $G \simeq N \rtimes_\tau K \simeq \mathbb{Z}_q \rtimes_\tau \mathbb{Z}_p$, para cierto morfismo $\tau : \mathbb{Z}_p \to \operatorname{Aut}(\mathbb{Z}_q)$. Además sabemos que τ es de la forma $\tau_{\overline{k}}(\overline{n}) = \overline{r}^k \overline{n}$, para todo $\overline{k} \in \mathbb{Z}_p, \overline{n} \in \mathbb{Z}_q$, siendo $r \in \mathbb{Z}^+$ tal que $r^p \equiv 1 (\operatorname{mod}\ q)$.

Si G es abeliano, entonces K es normal y el morfismo τ es trivial. Luego $G \simeq \mathbb{Z}_q \times \mathbb{Z}_p \simeq \mathbb{Z}_{pq}$.

Si G no es abeliano, entonces K no puede ser normal y por lo tanto el morfismo τ no es trivial, lo cual equivale a $r \not\equiv 1 (\operatorname{mod}\ q)$. Esto a su vez implica $q \equiv 1 (\operatorname{mod}\ p)$, por el lema 8.28.

En resumen, probamos que si G es abeliano, entonces $G \simeq \mathbb{Z}_{pq}$, y si G no es abeliano, entonces $q \equiv 1 (\operatorname{mod}\ p)$ y $G \simeq \mathbb{Z}_q \rtimes_\tau \mathbb{Z}_p$, para cierto morfismo no trivial $\tau : \mathbb{Z}_p \to \operatorname{Aut}(\mathbb{Z}_q)$. Por otro lado vimos en el lema 8.28 que si $q \equiv 1 (\operatorname{mod}\ p)$, entonces existe un morfismo no trivial $\tau : \mathbb{Z}_p \to \operatorname{Aut}(\mathbb{Z}_q)$ y por lo tanto $\mathbb{Z}_q \rtimes_\tau \mathbb{Z}_p$ es un grupo no abeliano de orden pq. Esto completa la prueba de la existencia y unicidad.

Probaremos ahora que si $q \equiv 1 (\operatorname{mod}\ p)$, entonces $\mathbb{Z}_q \rtimes_\tau \mathbb{Z}_p$ admite la presentación por generadores y relaciones dada en la tesis. En estas hipótesis sabemos que $\tau : \mathbb{Z}_p \to \operatorname{Aut}(\mathbb{Z}_q)$ está definido por $\tau_{\overline{k}}(\overline{n}) = \overline{r}^k \overline{n}$, siendo $r \in \mathbb{Z}^+$ tal que $r^p \equiv 1 (\operatorname{mod}\ q)$ y $r \not\equiv 1 (\operatorname{mod}\ q)$; luego la acción correspondiente es $\overline{k} \cdot \overline{n} = \overline{r}^k \overline{n}$. Notar que en $\mathbb{Z}_p$ y $\mathbb{Z}_q$ usamos notación aditiva, luego en $\mathbb{Z}_q \rtimes_\tau \mathbb{Z}_p$ el neutro es $1 = \left(\overline{0}, \overline{0}\right)$ y el producto es

$$\left(\overline{n_1}, \overline{k_1}\right)\left(\overline{n_2}, \overline{k_2}\right) = \left(\overline{n_1} + \overline{k_1} \cdot \overline{n_2},\ \overline{k_1} + \overline{k_2}\right) = \left(\overline{n_1} + \overline{r}^{k_1} \overline{n_2},\ \overline{k_1} + \overline{k_2}\right).$$

Sean $a = (\overline{0},\overline{1})$ y $b = (\overline{1},\overline{0})$. Notar $a^n = 1 \Leftrightarrow (\overline{0},\overline{1})^n = (\overline{0},\overline{0}) \Leftrightarrow (\overline{0},\overline{n}) = (\overline{0},\overline{0}) \Leftrightarrow \overline{n} = \overline{0} \in \mathbb{Z}_p \Leftrightarrow p \mid n$. Luego $|a| = p$ y análogamente se prueba $|b| = q$. Además $b^n a^k = (\overline{1},\overline{0})^n (\overline{0},\overline{1})^k = (\overline{n},\overline{0})(\overline{0},\overline{k}) = (\overline{n},\overline{k})$. Luego a y b generan $\mathbb{Z}_q \rtimes_\tau \mathbb{Z}_p$. Además usando la tercer fórmula de (8) obtenemos

$$aba^{-1} = (\overline{0},\overline{1})(\overline{1},\overline{0})(\overline{0},\overline{1})^{-1} = (\overline{1}\cdot\overline{1},\overline{0}) = (\overline{r},\overline{0}) = b^r.$$

Luego $\mathbb{Z}_q \rtimes_\tau \mathbb{Z}_p = \langle a, b : \ a^p = b^q = 1,\ aba^{-1} = b^r\rangle$. □

En la tesis del teorema anterior, la descripción del grupo en el caso no abeliano pasa por la elección de un cierto elemento r. La siguiente proposición muestra que el grupo obtenido no depende de dicha elección.

Lema 8.31. *Sean p y q primos tales que $p < q$ y $q \equiv 1 (\mathrm{mod}\ p)$. Sean r, s tales que $r^p \equiv 1(\mathrm{mod}\ q)$, $r \not\equiv 1(\mathrm{mod}\ q)$, $s^p \equiv 1(\mathrm{mod}\ q)$ y $s \not\equiv 1(\mathrm{mod}\ q)$. Entones los grupos $G = \langle a, b : \ a^p = b^q = 1,\ aba^{-1} = b^r\rangle$ y $F = \langle \alpha, \beta : \ \alpha^p = \beta^q = 1,\ \alpha\beta\alpha^{-1} = \beta^s\rangle$ son isomorfos.*

Dem. Como q es primo, entonces $\mathbb{Z}_q$ es un cuerpo y por lo tanto el polinomio $X^p - \overline{1} \in \mathbb{Z}_q[X]$ tiene a lo más p raíces en $\mathbb{Z}_q$. Luego $H = \{\overline{a} \in \mathbb{Z}_q : \ \overline{a}^p = \overline{1}\}$ es un subgrupo de $\mathbb{Z}_q^\times$ y $|H| \leq p$. Las condiciones en r y s implican $\overline{r}^p = \overline{s}^p = \overline{1}$ y $\overline{r}, \overline{s} \neq \overline{1}$ en $\mathbb{Z}_q$. Luego $\overline{r}, \overline{s} \in H$ y $|\overline{r}| = |\overline{s}| = p$ en $\mathbb{Z}_q^\times$. Entonces necesariamente es $\langle\overline{r}\rangle = \langle\overline{s}\rangle = H \simeq \mathbb{Z}_p$. Como p es primo, entones la única posibilidad es $\overline{s} = \overline{r}$ o $\overline{s} = \overline{r}^{-1}$ en $\mathbb{Z}_q$. Si $\overline{s} = \overline{r}$, entonces $\beta^s = \beta^r$ y por lo tanto $G \simeq F$. Si $\overline{s} = \overline{r}^{-1}$, entonces existe n tal que $sr = 1 + qn$. Luego en F vale

$$\alpha\beta^r\alpha^{-1} = (\alpha\beta\alpha^{-1})^r = \beta^{rs} = \beta \quad \Rightarrow \quad \alpha^{-1}\beta\alpha = \beta^r.$$

Entonces escribiendo $\gamma = \alpha^{-1}$ obtenemos $F = \langle \gamma, \beta : \ \gamma^p = \beta^q = 1,\ \gamma\beta\gamma^{-1} = \beta^r\rangle$ y por lo tanto $F \simeq G$. □

Ejemplos 8.32. Sea G un grupo.

1. Si $|G| = 15$, como es $5 \not\equiv 1(\mathrm{mod}\ 3)$, entonces $G \simeq \mathbb{Z}_{15}$.

2. Si $|G| = 6$, veremos que G es isomorfo a $\mathbb{Z}_6$ o D_3. En este caso es $3 \equiv 1(\mathrm{mod}\ 2)$. Luego la proposición anterior nos dice que a menos de isomorfismo hay solo dos grupos de orden 6, uno es abeliano y el otro no. Como $\mathbb{Z}_6$ es abeliano y D_3 no lo es, deducimos que son esos. En particular $\mathcal{S}_3 \simeq D_3$.

   Explícitamente, si G es no abeliano, entonces tiene que ser $G = \langle a, b : \ a^2 = b^3 = 1,\ aba^{-1} = b^r\rangle$, siendo r tal que $r^2 \equiv 1(\mathrm{mod}\ 3)$ y $r \not\equiv 1(\mathrm{mod}\ 3)$. Como $r = 2$ lo verifica, deducimos $G \simeq D_3$.

9. El grupo simétrico

Sea $I_n = \{1, \dots, n\}$, $n \geq 1$. Recordar que el *grupo simétrico* es $\mathcal{S}_n = \mathrm{Biy}(I_n)$ y que vale $|\mathcal{S}_n| = n!$. A los elementos de $\mathcal{S}_n$ se les llama *permutaciones*. Para las permutaciones usaremos la notación

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

Una permutación $\sigma \in \mathcal{S}_n$ que verifica que existen $i_1, i_2, \dots, i_r \in I_n$ $(2 \leq r \leq n)$ tales que

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

se dice que es un *r-ciclo* o *ciclo de longitud r* y se escribe $\sigma = (i_1 i_2 \cdots i_r)$. Los 2-ciclos se llaman *trasposiciones*.

Observación 9.1.

1. Si $\sigma = (i_1 i_2 \cdots i_r)$, entonces $|\sigma| = r$ y $\sigma^{-1} = (i_r i_{r-1} \cdots i_1)$.

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

3. Si σ es un r-ciclo, $x \in I_n$ y $\sigma(x) \neq x$, entonces $\sigma = \big(x\, \sigma(x)\, \sigma^2(x)\, \cdots\, \sigma^{r-1}(x)\big)$. Esto se debe a que si $\sigma = (i_1 i_2 \cdots i_r)$ y $\sigma(x) \neq x$, entonces existe un k tal que $x = i_k$, luego $\sigma(x) = i_{k+1}$, $\sigma^2(x) = i_{k+2}$, etc.

Dos ciclos $(i_1 i_2 \cdots i_r)$ y $(j_1 j_2 \cdots j_s)$ se dicen *disjuntos* si los conjuntos $\{i_1, i_2, \ldots, i_r\}$ y $\{j_1, j_2, \ldots, j_s\}$ son disjuntos.

Proposición 9.2. *Si dos ciclos son disjuntos, entonces conmutan.*

Dem. Sean $\sigma_1 = (i_1 i_2 \cdots i_r)$ y $\sigma_2 = (j_1 j_2 \cdots j_s)$ dos ciclos disjuntos. Si $x \notin \{i_1, i_2, \ldots, i_r, j_1, j_2, \ldots, j_s\}$, entonces $(\sigma_1\sigma_2)(x) = (\sigma_2\sigma_1)(x) = x$. Si $x = i_k$, es

$$(\sigma_1\sigma_2)(i_k) = \sigma_1(i_k) = i_{k+1}, \quad (\sigma_2\sigma_1)(i_k) = \sigma_2(i_{k+1}) = i_{k+1} \quad \Rightarrow \quad (\sigma_1\sigma_2)(i_k) = (\sigma_2\sigma_1)(i_k).$$

Para $x = j_k$ es análogo. □

Para probar el próximo teorema necesitamos el siguiente resultado.

Proposición 9.3. *Sea $G = \langle a \rangle$ un grupo cíclico y H un subgrupo no trivial de G. Sabemos que existe $k \in \mathbb{Z}^+$ tal que $H = \langle a^k \rangle$. Entonces $G/H = \{\overline{1}, \alpha, \ldots, \alpha^{k-1}\}$ es un grupo cíclico de orden k, siendo $\alpha = \overline{a} \in G/H$.*

Dem. Si $x \in G$, entonces existe $n \in \mathbb{Z}$ tal que $x = a^n$, luego $\overline{x} = \overline{a^n} = \overline{a}^n = \alpha^n$. Esto prueba $G/H = \langle \alpha \rangle$. Además $a^k \in H$, luego $\alpha^k = \overline{1}$. Si $m \in \mathbb{Z}^+$ es tal que $\alpha^m = \overline{1}$, entonces $a^m \in H = \langle a^k \rangle$ y por lo tanto existe $q \in \mathbb{Z}^+$ tal que $m = nk$. Luego $\alpha^k = \overline{1}$ y vimos que $\alpha^m = \overline{1}$ implica $k \mid m$. Esto prueba $|\alpha| = k$. □

Teorema 9.4. *Si $\sigma \in \mathcal{S}_n$ es una permutación distinta de la identidad, entonces σ se escribe en forma única (a menos del orden) como producto de ciclos disjuntos.*

Dem. La acción natural de $\mathcal{S}_n$ en I_n dada por $\alpha \cdot x = \alpha(x)$ induce por restricción una acción de $G := \langle \sigma \rangle < \mathcal{S}_n$ en I_n. Luego existen $x_1, \ldots, x_t \in I_n$ tales que

$$I_n = o(x_1) \sqcup o(x_2) \sqcup \cdots \sqcup o(x_t) \sqcup I_n^G, \qquad I_n^G = \{x \in I_n : \ \sigma(x) = x\}. \tag{9}$$

Sea $i \in \{1, \ldots, t\}$. Sabemos $o(x_i) \simeq G/G_{x_i}$ y al ser $G = \langle \sigma \rangle$ entonces existe $m_i \in \mathbb{Z}^+$ tal que $G_{x_i} = \langle \sigma^{m_i} \rangle$. Luego $G/G_{x_i} = \{\overline{\mathrm{id}}, \overline{\sigma}, \overline{\sigma}^2, \ldots, \overline{\sigma}^{m_i-1}\}$, con $|G/G_{x_i}| = m_i$, por lo tanto

$$|o(x_i)| = m_i, \quad o(x_i) = \{x_i, \sigma(x_i), \sigma^2(x_i), \ldots, \sigma^{m_i-1}(x_i)\}, \quad \sigma^{m_i}(x_i) = x_i.$$

Para cada $i \in \{1, \ldots, t\}$ consideramos el ciclo $\eta_i = \big(x_i\, \sigma(x_i)\, \sigma^2(x_i)\, \cdots\, \sigma^{m_i-1}(x_i)\big)$. Notar $\eta_i(x_i) = \sigma(x_i)$, $\eta_i^2(x_i) = \sigma^2(x_i)$, etc. Luego $\eta_i^l(x_i) = \sigma^l(x_i)$, para todo $l = 1, i$. Observar también que como las órbitas son disjuntas, entonces $\eta_1, \ldots, \eta_t$ son ciclos disjuntos.
A continuación usando (9) probaremos $\sigma = \eta_1 \cdots \eta_t$. Sea $x \in I_n$. Si $x \in I_n^G$, entonces $\sigma(x) = \eta_1 \cdots \eta_t(x) = x$. En caso contrario $x \in o(x_i)$ para algún i y por lo tanto $x = \sigma^l(x_i) = \eta_i^l(x_i)$ para algún l. Luego, teniendo en cuenta que vale $\eta_k(x_i) = x_i$ si $k \neq i$, obtenemos

$$(\eta_1 \cdots \eta_t)(x) = (\eta_i \eta_1 \cdots \eta_{i-1} \eta_{i+1} \cdots \eta_t)(x) = \eta_i(x) = \eta_i\big(\eta_i^l(x_i)\big) = \eta_i^{l+1}(x_i) = \sigma^{l+1}(x_i) = \sigma\big(\sigma^l(x_i)\big) = \sigma(x).$$

Luego $\sigma = \eta_1 \cdots \eta_t$.

Recíprocamente, supongamos $\sigma = \gamma_1 \cdots \gamma_r$, siendo $\gamma_1, \ldots, \gamma_r$ ciclos disjuntos. Consideremos la acción de $G = \langle \sigma \rangle < \mathcal{S}_n$ en I_n. Si $\gamma_k = (i_1 \ldots i_r)$, entonces $o(i_1) = \cdots = o(i_r) = \{i_1, \ldots, i_r\}$. Luego las órbitas con más de un punto son los conjuntos formados por las componentes de $\gamma_1, \ldots, \gamma_r$, y el conjunto de puntos fijos es su complemento. Esto prueba la unicidad. □

Ejemplo 9.5. Si $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$ y $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$, entonces $\sigma_1 = (13)(245)$ y $\sigma_2 = (13)(25)$.

Recordemos que dos elementos $\sigma_1, \sigma_2 \in \mathcal{S}_n$ son conjugados si existe $\alpha \in \mathcal{S}_n$ tal que $\sigma_1 = \alpha\sigma_2\alpha^{-1}$.

Proposición 9.6. *Sea $(i_1 \cdots i_r)$ un r-ciclo, $r \geq 2$ y $\sigma \in \mathcal{S}_n$. Entonces*

$$\sigma(i_1 \cdots i_r)\sigma^{-1} = \big(\sigma(i_1) \cdots \sigma(i_r)\big).$$

Dem. Se prueba fácilmente que vale $\sigma(i_1 \cdots i_r) = \big(\sigma(i_1) \cdots \sigma(i_r)\big)\sigma$, como funciones de I_n en I_n. $\square$

Corolario 9.7. *Para cada $r = 2, \ldots, n$ se cumple que todos los r-ciclos en $\mathcal{S}_n$ son conjugados entre sí.*

Dem. Dados $(i_1 \cdots i_r)$ y $(j_1 \cdots j_r)$, definimos $\sigma : I_n \to I_n$ por $\sigma(i_k) = j_k$, para todo $k = 1, \ldots, r$, y como una biyección cualquiera entre sus complementos. Luego $\sigma(i_1 \cdots i_r)\sigma^{-1} = (j_1 \cdots j_r)$. $\square$

Proposición 9.8. *Sean $\sigma = \sigma_1 \cdots \sigma_r$ y $\tau = \tau_1 \cdots \tau_s$ dos permutaciones escritas como producto de ciclos disjuntos tales que $|\sigma_1| \geq \cdots \geq |\sigma_r|$ y $|\tau_1| \geq \cdots \geq |\tau_s|$. Entonces σ y τ son conjugadas si y solo si $r = s$ y $|\sigma_i| = |\tau_i|$, para todo $i = 1, \ldots, r$.*

Dem. Directo. Si $\tau = \alpha\sigma\alpha^{-1}$ y $\sigma = \sigma_1 \cdots \sigma_r$ es la descomposición en ciclos disjuntos de σ, entonces $\tau = \left(\alpha\sigma_1\alpha^{-1}\right) \cdots \left(\alpha\sigma_r\alpha^{-1}\right)$ es la descomposición en ciclos disjuntos de τ y $|\alpha\sigma_i\alpha^{-1}| = |\sigma_i|$, para todo $i = 1, \ldots, r$.
Recíproco. Sean $\sigma = \sigma_1 \cdots \sigma_r$ y $\tau = \tau_1 \cdots \tau_r$ con $|\sigma_i| = |\tau_i|$, para todo $i = 1, \ldots, r$. Notar que σ y τ mueven la misma cantidad de puntos. Teniendo en cuenta la proposición 9.6, definimos $\alpha \in \mathcal{S}_n$ de forma tal que $\alpha\sigma_i\alpha^{-1} = \tau_i$, para todo $i = 1, \ldots, r$ y como una biyección cualquiera entre el complemento de los puntos fijos de σ y de τ. Entonces $\alpha\sigma\alpha^{-1} = \left(\alpha\sigma_1\alpha^{-1}\right) \cdots \left(\alpha\sigma_r\alpha^{-1}\right) = \tau_1 \cdots \tau_r = \tau$. $\square$

En lo que sigue estudiaremos propiedades vinculadas a las trasposiciones. Empezamos probando que las trasposiciones generan al grupo simétrico.

Proposición 9.9. *Toda permutación se escribe como producto de trasposiciones.*

Dem. Por el teorema 9.4, alcanza con probarlo para la identidad y los r-ciclos. Eso es fácil

$$\mathrm{id} = (ij)(ij), \qquad (i_1 i_2 \cdots i_r) = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_3)(i_1 i_2),\ \forall r = 2, \ldots, n. \quad \square$$

Observación 9.10. Notar que $(xa)(ab)(xa) = (xb)$, luego $(xa)(ab) = (xb)(xa)$. Esto muestra que no hay unicidad en la descomposición de una permutación en producto de trasposiciones, tanto en la cantidad de factores como en los factores que aparecen. Además, si $\tau_1, \ldots, \tau_r$ son trasposiciones disjuntas, entonces el orden del producto $\tau_1 \cdots \tau_r$ es 2, luego si $\sigma \in \mathcal{S}_n$ y $|\sigma| \geq 3$, entonces σ no se puede escribir como producto de trasposiciones disjuntas. Luego en la descomposición dada por la proposición 9.9, en general las trasposiciones no son disjuntas y no hay unicidad en la descomposición

Signo de una permutación. Definimos una función $\mathbb{R}^n \times \mathcal{S}_n \xrightarrow{\bullet} \mathbb{R}^n$ mediante

$$(x_1, \ldots, x_n) \bullet \sigma = \left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right), \quad \forall \sigma \in \mathcal{S}_n,\ (x_1, \ldots, x_n) \in \mathbb{R}^n.$$

Proposición 9.11. *La función $\mathbb{R}^n \times \mathcal{S}_n \xrightarrow{\bullet} \mathbb{R}^n$ es una acción a derecha de $\mathcal{S}_n$ en $\mathbb{R}^n$.*

Dem. Es claro que vale $v \bullet \mathrm{id} = v$, para todo $v \in \mathbb{R}^n$. Para la otra condición, sean $\sigma, \eta \in \mathcal{S}_n$ y $(x_1, \dots, x_n) \in \mathbb{R}^n$. Sea $(y_1, \dots, y_n) = (x_1, \dots, x_n) \bullet \sigma$, luego $y_i = x_{\sigma(i)}$, para todo i. Entonces

$$\begin{aligned}\big((x_1, \dots, x_n) \bullet \sigma\big) \bullet \eta &= (y_1, \dots, y_n) \bullet \eta = \big(y_{\eta(1)}, \dots, y_{\eta(n)}\big) = \left(x_{\sigma\left(\eta(1)\right)}, \dots, x_{\sigma\left(\eta(n)\right)}\right) \\ &= \big(x_{\sigma\eta(1)}, \dots, x_{\sigma\eta(n)}\big) = (x_1, \dots, x_n) \bullet \sigma\eta. \quad \square\end{aligned}$$

Esta acción a derecha induce una acción a la izquierda $\mathcal{S}_n \times \mathbb{R}^n \xrightarrow{\cdot} \mathbb{R}^n$ definiendo

$$\sigma \cdot (x_1, \dots, x_n) := (x_1, \dots, x_n) \bullet \sigma^{-1} = \big(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)}\big), \quad \forall \sigma \in \mathcal{S}_n,\ (x_1, \dots, x_n) \in \mathbb{R}^n.$$

Proposición 9.12. *Si $\sigma \in \mathcal{S}_n$, $a \in \mathbb{R}$ y $u, v \in \mathbb{R}^n$, entonces*

$$\sigma \cdot (av) = a(\sigma \cdot v); \quad \sigma \cdot (u + v) = \sigma \cdot u + \sigma \cdot v.$$

Dem. Sea $v = (x_1, \dots, x_n)$ y $av = (y_1, \dots. y_n)$, luego $y_i = ax_i$, para todo i. Entonces

$$\begin{aligned}\sigma \cdot (av) &= \sigma \cdot (y_1, \dots, y_n) = \big(y_{\sigma^{-1}(1)}, \dots, y_{\sigma^{-1}(n)}\big) = \big(ax_{\sigma^{-1}(1)}, \dots, ax_{\sigma^{-1}(n)}\big) = a\left(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)}\right) \\ &= a(\sigma \cdot v).\end{aligned}$$

La otra igualdad se prueba en forma análoga. $\square$

La proposición anterior muestra que la imagen del morfismo $\mathcal{S} \to \mathrm{Biy}(\mathbb{R}^n)$ asociado a esta acción está contenida en $\mathrm{GL}(\mathbb{R}^n)$. Identificando en la forma usual $\mathrm{GL}(\mathbb{R}^n)$ con $\mathrm{GL}_n(\mathbb{R})$ (las matrices invertibles) obtenemos un morfismo de grupos $P : \mathcal{S}_n \to \mathrm{GL}_n(\mathbb{R})$, $\sigma \mapsto P_\sigma$, definido por

$$\sigma \cdot v = P_\sigma v, \quad \forall \sigma \in \mathcal{S}_n,\ v \in \mathbb{R}^n.$$

Observación 9.13. No es difícil probar que si $\sigma \in \mathcal{S}_n$, entonces $P_\sigma = \sum_{i=1}^n E_{\sigma(i),i}$, siendo $\{E_{i,j} :\ 1 \le i, j \le n\}$ la base canónica del espacio de matrices $M_n(\mathbb{R})$. Esto implica que las matrices P_σ son las matrices que en cada fila y columna tienen exactamente un 1 y 0 en los lugares restantes.

Componiendo $P : \mathcal{S}_n \to \mathrm{GL}_n(\mathbb{R})$ con el determinante $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ obtenemos un morfismo $\varepsilon : \mathcal{S}_n \to \mathbb{R}^\times$ definido por

$$\varepsilon(\sigma) = \det(P_\sigma), \quad \forall \sigma \in \mathcal{S}_n.$$

Proposición 9.14. *Vale $\varepsilon(\sigma) = \pm 1$, para todo $\sigma \in \mathcal{S}_n$.*

Dem. Sea $\sigma \in \mathcal{S}_n$. Como $\mathcal{S}_n$ es finito, entonces σ tiene orden finito, luego existe $k \in \mathbb{Z}^+$ tal que $\sigma^k = \mathrm{id}$. Entonces

$$1 = \varepsilon(\mathrm{id}) = \varepsilon(\sigma^k) = \varepsilon(\sigma)^k \quad \Rightarrow \quad \varepsilon(\sigma) = \pm 1. \quad \square$$

Luego hemos definido un morfismo de grupos $\varepsilon : \mathcal{S}_n \to \{\pm 1\}$. Para cada $\sigma \in \mathcal{S}_n$, $\varepsilon(\sigma) = \pm 1$ es el *signo* de σ.

Proposición 9.15. *Si $\tau \in \mathcal{S}_n$ es una trasposición, entonces $\varepsilon(\tau) = -1$.*

Dem. Sea $\tau = (ij)$. Entonces τ actuando en $(x_1, \dots, x_n)$ intercambia las coordenadas x_i y x_j. Esto implica que P_τ es la matriz elemental obtenida intercambiando en la matriz identidad la fila i con la fila j. Luego $\varepsilon(\tau) = \det(P_\tau) = -\det(\mathrm{Id}) = -1$. $\square$

Corolario 9.16. *Sea $\sigma \in \mathcal{S}_n$ y sean $\sigma = \tau_1 \cdots \tau_k = \tau_1' \cdots \tau_h'$ dos descomposiciones de σ en producto de trasposiciones. Entonces $k \equiv h (\mathrm{mod}\ 2)$.*

Dem. Como ε es un morfismo y $\varepsilon(\tau) = -1$, para toda trasposición τ, entonces la hipótesis implica $\varepsilon(\sigma) = (-1)^k = (-1)^h$. Esta última igualdad equivale a $k \equiv h (\mathrm{mod}\ 2)$. $\square$

Observación 9.17. La proposición anterior implica que se preserva la paridad de la cantidad de factores en las distintas formas de descomponer una permutación como producto de trasposiciones. Luego decimos que una permutación σ es *par* si se escribe como producto de un número par de trasposiciones (lo cual equivale a $\varepsilon(\sigma) = 1$) y que es *impar* en caso contrario.

Luego el núcleo de $\varepsilon : \mathcal{S}_n \to \{\pm 1\}$ es el conjunto formado por las permutaciones pares de $\mathcal{S}_n$, al cual se le llama el *grupo alternado* A_n. Al ser un núcleo es $A_n \lhd \mathcal{S}_n$. Aplicando a ε el primer teorema de isomorfismo deducimos $[\mathcal{S}_n : A_n] = 2$; luego $|A_n| = n!/2$.

Observación 9.18. la fórmula $(i_1 i_2 \cdots i_r) = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_3)(i_1 i_2)$, implica que todo r-ciclo se escribe como producto de $(r-1)$-trasposiciones, luego un r-ciclo es par si y solo si r es impar. Hay que tener cuidado de no confundirse con eso.

Simplicidad de A_n. Un grupo se dice *simple* si no es el grupo trivial y no tiene subgrupos normales propios.

Observación 9.19. Sea G un grupo finito. Si G no es simple, entonces contiene algún subgrupo normal propio maximal[6] $G_1 \subsetneq G$ (alcanza con tomar un subgrupo normal propio de orden máximo). Si G_1 no es simple, entonces contiene algún subgrupo normal propio maximal $G_2 \subsetneq G_1 \subsetneq G$, y así seguimos. Como G es finito y los órdenes verifican $|G| > |G_1| > |G_2| > \cdots$, entonces existe un cierto n tal que $G \supsetneq G_1 \supsetneq \cdots \supsetneq G_n$ y G_n es simple. Notar que de la maximalidad de los G_i se deduce que cada grupo cociente G_i/G_{i+1} es un grupo simple. Luego probamos que para todo grupo finito G, existe una cadena de subgrupos

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n \supsetneq G_{n+1} = \{1\}$$

tal que $G_{i+1} \lhd G_i$ y G_i/G_{i+1} es un grupo simple, para todo $i = 0, \ldots, n$. Esto es lo que se llama una *serie de composición* de G. Se prueba que dos series de composición de un mismo grupo siempre tienen la misma cantidad de términos y los grupos cocientes son isomorfos (aunque no necesariamente en el mismo orden). Esto explica el interés en los grupos simples.

Observación 9.20.

1. Si G es un grupo abeliano finito, entonces el teorema de Cauchy implica que G es simple si y solo si G tiene orden primo (y por lo tanto es cíclico).
2. Observar que $|A_3| = 3$, luego A_3 es simple. Es un ejercicio el probar que $N \lhd A_4$, siendo

   $$N = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\},$$

   luego A_4 no es simple.

En lo que sigue probaremos que si $n \geq 5$, entonces A_n es simple.

Lema 9.21. *Si $n \geq 3$, entonces A_n es el subgrupo de $\mathcal{S}_n$ generado por los 3-ciclos.*

Dem. Sabemos que A_n contiene a todos los 3-ciclos de $\mathcal{S}_n$. Además, como todo elemento de A_n es producto de un número par de trasposiciones, entonces la tesis se deduce de las siguientes igualdades

$$(ac)(bc) = (abc), \qquad (xa)(yb) = (xa)(ay)\,(ay)(yb) = (xya)(aby). \quad \square$$

[6] Que sea *maximal* es que no está contenido propiamente en ningun subgrupo normal propio.

Lema 9.22. *Si $n \geq 5$, entonces todos los 3-ciclos son conjugados entre sí dentro de A_n.*

Dem. Sean (abc) e (ijk) dos 3-ciclos. Sabemos que existe $\sigma \in \mathcal{S}_n$ tal que $(ijk) = \sigma(abc)\sigma^{-1}$. Si $\sigma \in A_n$, entonces ya está probado. Si no, sean $d, e \in I_n$ distintos de a, b, c. Entonces $\sigma(de) \in A_n$ y

$$\sigma(de)(abc)\big(\sigma(de)\big)^{-1} = \sigma(de)(abc)(de)\sigma^{-1} = \sigma(abc)\sigma^{-1} = (ijk). \quad \square$$

Ejercicio 9.23. Sea G un grupo. Recordar que el *conmutador* de $g, f \in G$ es $[g, f] = gfg^{-1}f^{-1}$. Probar.

1. Si $g, f, h \in G$ y $gh = hg$, entonces $[g, fh] = [g, f]$.
2. Si $N \lhd G$, $n \in N$ y $g \in G$, entonces $[g, n] \in N$ y $[n, g] \in N$.

Teorema 9.24. *Si $n = 3$ o $n \geq 5$, entonces el grupo alternado A_n es simple.*

Dem. Para $n = 3$ ya lo sabemos. Supongamos $n \geq 5$ y sea $N \lhd A_n$, $N \neq \{\mathrm{id}\}$. Si probamos que N contiene un 3-ciclo, entonces de los lemas 9.21 y 9.22 se deduce $N = A_n$, que es lo que queremos probar.

Como $N \neq \{\mathrm{id}\}$, entonces existe $\sigma \in N$, $\sigma \neq \mathrm{id}$. Sea $\sigma = \gamma_1 \cdots \gamma_r$ su descomposición en ciclos disjuntos. Tenemos cuatro casos posibles:

1. Existe i tal que $|\gamma_i| \geq 4$.
2. $|\gamma_i| \leq 3$, para todo $i = 1, \dots, r$ y existen $i \neq j$ tales que $|\gamma_i| = |\gamma_j| = 3$.
3. $|\gamma_i| \leq 3$, para todo $i = 1, \dots, r$ y existe un único i_0 tal que $|\gamma_{i_0}| = 3$.
4. $|\gamma_i| = 2$, para todo $i = 1, \dots, r$.

Caso 1: Es $\sigma = (a_1 \cdots a_l)\gamma_2 \cdots \gamma_r$, con $l \geq 4$. Como $\alpha = (a_1a_2a_3) \in A_n$, entonces $[\alpha, \sigma] \in N$. Notar que $(a_1a_2a_3)$ y $\gamma_2 \cdots \gamma_r$ conmutan. Luego aplicando el ejercicio anterior y la proposición 9.6 obtenemos

$$\begin{aligned}[\alpha, \sigma] &= [(a_1a_2a_3), (a_1 \cdots a_l)\gamma_2 \cdots \gamma_r] = [(a_1a_2a_3), (a_1 \cdots a_l)] = (a_1a_2a_3)(a_1 \cdots a_l)(a_3a_2a_1)(a_1 \cdots a_l)^{-1} \\ &= (a_1a_2a_3)(a_4a_3a_2) = (a_1a_2a_4).\end{aligned}$$

Luego $(a_1a_2a_4) \in N$.

Caso 2: Es $\sigma = (a_1a_2a_3)(a_4a_5a_5)\gamma_3 \cdots \gamma_r$. Si $\alpha = (a_1a_2a_4) \in A_n$, entonces razonando como antes obtenemos

$$\begin{aligned}[\alpha, \sigma] &= [(a_1a_2a_4), (a_1a_2a_3)(a_4a_5a_5)\gamma_3 \cdots \gamma_r] = [(a_1a_2a_4), (a_1a_2a_3)(a_4a_5a_5)] \\ &= (a_1a_2a_4)\big((a_1a_2a_3)(a_4a_5a_5)\big)(a_4a_2a_1)\big((a_1a_2a_3)(a_4a_5a_5)\big)^{-1} \\ &= (a_1a_2a_4)(a_5a_3a_2) = (a_1a_2a_5a_3a_4).\end{aligned}$$

Luego $(a_1a_2a_5a_3a_4) \in N$ y caemos en el caso 1.

Caso 3: Es $\sigma = (a_1a_2a_3)\gamma_2 \cdots \gamma_r$, siendo $\gamma_2, \dots, \gamma_r$ trasposiciones. Luego $N \ni \sigma^2 = (a_1a_2a_3)^2 = (a_3a_2a_1)$.

Caso 4: Es $\sigma = (a_1a_2)(a_3a_4)\gamma_3 \cdots \gamma_r$, siendo $\gamma_3, \dots, \gamma_r$ trasposiciones. Si $\alpha = (a_1a_2a_3) \in A_n$, es

$$\begin{aligned}[\alpha, \sigma] &= [(a_1a_2a_3), (a_1a_2)(a_3a_4)\gamma_3 \cdots \gamma_r] = [(a_1a_2a_3), (a_1a_2)(a_3a_4)] \\ &= (a_1a_2a_3)\big((a_1a_2)(a_3a_4)\big)(a_3a_2a_1)\big((a_1a_2)(a_3a_4)\big)^{-1} = (a_1a_2a_3)(a_4a_1a_2) = (a_1a_3)(a_2a_4).\end{aligned}$$

Luego $(a_1a_3)(a_2a_4) \in N$. Como $n \geq 5$, existe $b \in I_n$ tal que $b \notin \{a_1, a_2, a_3, a_4\}$. Si $\beta = (a_1a_3b) \in A_n$, es

$$[(a_1a_3b), (a_1a_3)(a_2a_4)] = [(a_1a_3b), (a_1a_3)] = (a_1a_3b)(a_1a_3)(a_1a_3b)^{-1}(a_1a_3) = (a_3b)(a_1a_3) = (a_1ba_3).$$

Luego $(a_1ba_3) \in N$. $\square$

10. Subgrupos de Sylow

En esta sección los grupos son finitos.

Si G es un grupo y $H < G$, entonces $|H|$ divide a $|G|$ (teorema de Lagrange). La pregunta que nos hacemos es si vale el recíproco, es decir si dado un divisor m de $|G|$, entonces existe $H < G$ tal que $|H| = m$.
Si el grupo es abeliano, la respuesta es afirmativa (ver más adelante el corolario 10.18).
Si el grupo no es abeliano, la respuesta en general es negativa. Un ejemplo es el grupo alternado A_4 (de orden 12) que no tiene subgrupos de orden 6. Además, si $n \geq 5$ el grupo alternado A_n tiene orden $\frac{n!}{2}$ y es simple, por lo que no puede tener subgrupos de orden $\frac{n!}{4}$.
Por otro lado el teorema de Cauchy dice que si un número primo p divide a $|G|$, entonces existe $H < G$ tal que $|H| = p$. Probaremos que este resultado se puede generalizar para todo n tal que p^n divide a $|G|$.

Sea p un número primo. Un *p-grupo* es un grupo de orden p^n para algún $n = 0, 1, \ldots$

Proposición 10.1. *Si $|G| = p^2$, con p primo, entonces $G \simeq \mathbb{Z}_{p^2}$ o $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. En particular G es abeliano.*

Dem. Si $g \in G$ y $g \neq 1$, entonces $|g| = p$ o $|g| = p^2$. Si existe $g \in G$ tal que $|g| = p^2$, entonces $G = \langle g \rangle \simeq \mathbb{Z}_{p^2}$. Supongamos ahora que para todo $1 \neq g \in G$, es $|g| = p$. Sea $H < G$ tal que $|H| = p$. Sea $f \notin H$ y $N = \langle f \rangle$. Notar que $N \cap H = \{1\}$, luego $|G| = |NH|$ y por lo tanto $G = NH$. Al ser $[G : N] = [G : H] = p$, el corolario 8.23 implica $H \lhd G$ y $N \lhd G$, luego $G = NH \simeq N \times H \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. □

Observación 10.2. Si p es un primo y $|G| = p$, entonces G es cíclico, y si $|G| = p^2$, entonces G es abeliano. Eso es lo más que podemos afirmar, ya que los grupos D_4 y Q tienen orden $8 = 2^3$ y no son abelianos.

Proposición 10.3. *Si G es un p-grupo que actúa en un conjunto finito X, entonces*

$$\left|X^G\right| \equiv |X| (\text{mod } p).$$

Dem. Si la acción es trivial, es $X^G = X$. Si no, entonces existen $x_1, \ldots, x_n \in X$ tales que

$$|X| = \left|X^G\right| + \sum_{i=1}^{n} [G : G_{x_i}], \text{ con } [G : G_{x_i}] > 1, \ \forall i = 1, \ldots, n.$$

Como G es un p-grupo, entonces p divide a $[G : G_{x_i}]$, para todo i. Esto implica la tesis. □

Corolario 10.4. *Si G es un p-grupo no trivial, entonces su centro $Z(G)$ es no trivial.*

Dem. Considerando G actuando sobre sí mismo por conjugación, aplicando la proposición anterior deducimos que p divide a $|Z(G)|$. Al ser $|Z(G)| \neq 0$, se tiene $|Z(G)| \geq p$. □

Recordar que si G es un grupo cualquiera y $H < G$ es tal que $H \subset Z(G)$, entonces $H \lhd G$.

Proposición 10.5. *Si G es un p-grupo no trivial, entonces existe una torre de subgrupos*

$$\{1\} = G_0 < G_1 < \cdots < G_n = G \tag{10}$$

tal que $G_i \lhd G$ y $|G_i| = p^i$, para todo $i = 0, \ldots, n$.

Dem. Lo probaremos por inducción en n, siendo $|G| = p^n$.

Si $n = 1$, es $\{1\} = G_0 < G_1 = G$ y se cumple la tesis. Supongamos que $|G| = p^n$, $n > 1$, y que la tesis es válida para grupos de orden p^{n-1}. Como G es un p-grupo no trivial, entonces $Z(G)$ es no trivial. Luego existe $H < Z(G)$ tal que $|H| = p$. Al ser $H < Z(G)$, es $H \lhd G$; luego G/H es un grupo de orden p^{n-1} y aplicando la hipótesis inductiva sabemos que existe una torre de subgrupos

$$\{\bar{1}\} = \tilde{G}_0 < \tilde{G}_1 < \cdots < \tilde{G}_{n-1} = G/H$$

tal que $\tilde{G}_i \lhd G/H$ y $|\tilde{G}_i| = p^i$, para todo $i = 0, \ldots, n-1$. Esto implica que existe una torre de subgrupos

$$H = \hat{G}_0 < \hat{G}_1 < \cdots < \hat{G}_{n-1} = G$$

tal que $\hat{G}_i \lhd G$ y $\tilde{G}_i = \hat{G}_i/H$, para todo $i = 0, \ldots, n-1$. Observar $\left|\hat{G}_i\right| = \left|\tilde{G}_i\right||H| = p^{i+1}$, para todo i. Luego la tesis se obtiene definiendo $G_0 = \{1\}$ y $G_i = \hat{G}_{i-1}$, para todo $i = 1, \ldots, n$. □

Observación 10.6. Los subgrupos de la torre (10) verifican $G_i/G_{i-1} \simeq \mathbb{Z}_p$, para todo $i = 1, \ldots, n$. Luego forman una serie de composición de G.

Sea G un grupo y p un primo. Un *p-subgrupo* de G es un subgrupo de orden p^n, para algún $n \in \mathbb{N}$. Un *p-subgrupo de Sylow* de G es p-subgrupo de orden p^n, siendo n el mayor natural tal que p^n divide a $|G|$. Notar que los p-subgrupos de Sylow son elementos maximales de la familia de p-subgrupos del grupo.

Observación 10.7.

1. Si $H < G$ es un p-subgrupo, entonces H es un p-grupo.
2. Si G es un p-grupo, entonces G es el único p-subgrupo de Sylow de G.
3. Si p no divide a $|G|$, entonces el único p-subgrupo que tiene G es el trivial.

Teorema 10.8 (Primer teorema de Sylow)**.** *Si G es un grupo y p es un primo, entonces G contiene un p-subgrupo de Sylow.*

Dem. La prueba es por induccción en $|G|$. Si $|G| = 1$, entonces $G = \{1\}$ es su propio p-subgrupo de Sylow. Sea ahora G un grupo no trivial y supongamos que sabemos que todo grupo de orden menor que $|G|$ contiene algún p-subgrupo de Sylow.

Si p no divide a $|G|$, entonces el único p-subgrupo que tiene G es el trivial y ya está probado.
Supongamos ahora $|G| = p^n k$, con $p \nmid k$ y $n \geq 1$. El grupo G puede ser abeliano o no. Si G no es abeliano, entonces aplicando la ecuación de las clases obtenemos

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)], \text{ con } [G : C_G(x_i)] > 1, \ \forall i = 1, \ldots, m. \tag{11}$$

para ciertos $x_1, \ldots, x_m \in G$. Tenemos dos posibilidades:

1. $p \mid [G : C_G(x_i)]$, para todo $i = 1, \ldots, m$.
2. Existe $i_0 \in \{1, \ldots, m\}$ tal que $p \nmid [G : C_G(x_{i_0})]$.

Caso 1: Como p divide a $|G|$, se deduce de (11) que p divide a $|Z(G)|$. Aplicando el teorema de Cauchy a $Z(G)$ sabemos que existe $H < Z(G)$ tal que $|H| = p$. Al ser $H < Z(G)$, es $H \lhd G$. Entonces G/H es un grupo de orden $p^{n-1}k$ y aplicando la hipótesis inductiva deducimos que tiene un subgrupo $\tilde{K}$ de orden p^{n-1}. El subgrupo $\tilde{K}$ es de la forma $\tilde{K} = K/H$, siendo $H < K < G$. Luego $|K| = \left|\tilde{K}\right||H| = p^n$ y por lo tanto K es un p-subgrupo de Sylow de G.

Caso 2: Si llamamos $L = C_G(x_{i_0})$, es $L < G$ y $p \nmid [G : L]$. Al ser $|G| = [G : L]|L|$, deducimos que existe r tal que $|L| = p^n r$ y $p \nmid r$. Como $[G : L] > 1$, se deduce $|L| < |G|$, luego aplicando la hipótesis inductiva deducimos que L tiene un subgrupo M de orden p^n y por lo tanto M es un p-subgrupo de Sylow de G.

Si G es abeliano, entonces $G = Z(G)$ y se aplica el razonamiento del Caso 1 anterior. □

Corolario 10.9. *Si G es un grupo y p es un primo tal que $|G| = p^n k$, con $p \nmid k$, entonces G tiene subgrupos de orden p^l, para todo $l = 0, 1, \dots, n$.*

Dem. Aplicar el teorema 10.8 y la proposición 10.5. □

Recordar que el normalizador de un subgrupo H de G es $N_G(H) = \{g \in G : \; gHg^{-1} = H\}$ y es el mayor subgrupo de G que contiene a H como subgrupo normal.

Lema 10.10. *Sean G un grupo, p un primo que divide a $|G|$, H un p-subgrupo de G y S un p-subgrupo de Sylow de G. Si $H \subset N_G(S)$, entonces $H \subset S$.*

Dem. Como $H < N_G(S)$ y $S \lhd N_G(S)$, es $HS < N_G(S)$; luego $HS < G$. Observar que $S \lhd HS$, luego aplicando el segundo teorema de isomorfismo obtenemos $[HS : S] = [H : H \cap S]$. Entonces $[HS : S] = p^l$, para algún $l \geq 0$ y esto implica $|HS| = p^l|S|$. Como $S \subset HS$ y S es un p-subgrupo de Sylow de G, la única posibilidad es $l = 0$ y por lo tanto $S = HS$; luego $H \subset S$. □

En general escribiremos n_p a la cantidad de p-subgrupos de Sylow de un grupo G.

Teorema 10.11 (Segundo teorema de Sylow)**.** *Sea G un grupo y p un primo que divide a $|G|$. Entonces.*

1. *Todo p-subgrupo de G está contenido en algún p-subgrupo de Sylow.*
2. *Todos los p-subgrupos de Sylow de G son conjugados.*
3. *Vale $n_p \equiv 1 (\mathrm{mod}\ p)$.*

Dem. Sea $|G| = p^n k$, con $p \nmid k$ y consideramos G actuando en el conjunto de sus subgrupos por conjugación.

Sea S un p-subgrupo de Sylow de G fijo. Sea $\mathcal{S} = \{gSg^{-1} : \; g \in G\}$ la órbita de S. Observar que $\mathcal{S}$ está formada por p-subgrupos de Sylow de G. En la proposición 8.21 vimos que el estabilizador de S es el normalizador $N_G(S)$, luego $|\mathcal{S}| = [G : N_G(S)]$. Observar que es $S < N_G(S) < G$ y que $|S| = p^n$ y $|G| = p^n k$, con $p \nmid k$, luego de $[G : N_G(S)][N_G(S) : S] = [G : S] = k$, deducimos $p \nmid |\mathcal{S}|$.

Sea H un p-subgrupo arbitrario. Consideremos la acción por conjugación de H en $\mathcal{S}$. Como H es un p-grupo, la proposición 10.3 implica $\left|\mathcal{S}^H\right| \equiv |\mathcal{S}| (\mathrm{mod}\ p)$ y al ser $p \nmid |\mathcal{S}|$, se deduce $\mathcal{S}^H \neq \emptyset$.
Sea $Q \in \mathcal{S}^H$. Entonces Q es un p-subgrupo de Sylow y vale $hQh^{-1} = Q$, para todo $h \in H$. Luego $H \subset N_G(Q)$ y entonces el lema 10.10 implica $H \subset Q$. Esto prueba la primera afirmación.

Supongamos ahora que H es además un p-subgrupo de Sylow. Como H y Q son p-subgrupos de Sylow y $H \subset Q$, es $H = Q$. Pero $Q \in \mathcal{S}$, luego existe $g \in G$ tal que $H = gSg^{-1}$. Esto prueba la segunda afirmación y muestra que $\mathcal{S}$ es el conjunto de todos los p-subgrupos de Sylow de G.
Además probamos que si $Q \in \mathcal{S}^H$, entonces $Q = H$; luego $\mathcal{S}^H = \{H\}$. Entonces de $\left|\mathcal{S}^H\right| \equiv |\mathcal{S}| (\mathrm{mod}\ p)$ se deduce $|\mathcal{S}| \equiv 1 (\mathrm{mod}\ p)$, que es la tercera afirmación. □

Un subgrupo H de un grupo G se dice que es *característico* si verifica $\varphi(H) = H$, para todo $\varphi \in \mathrm{Aut}(G)$. Es fácil de probar que todo subgrupo característico es normal y que si H es el único subgrupo de G de de orden $|H|$, entonces H es un subgrupo característico de G. El ser característico es una condición más fuerte que la normalidad, dado que hay subgrupos normales que no son característicos.

Corolario 10.12. *Sea G un grupo, p un primo que divide a $|G|$ y S un p-subgrupo de Sylow de G. Entonces las siguientes afirmaciones son equivalentes*

$$S \text{ es normal}; \quad S \text{ es característico}; \quad n_p = 1.$$

Dem. Sea $|G| = p^m k$, con $p \nmid k$ y ≥ 1. El número n_p es la cantidad de subgrupos de G de orden p^m. Si $n_p = 1$, entonces S es el único subgrupo de G de de orden p^m y por lo tanto S es un subgrupo característico. Ya sabemos que si S es característico, entonces S es normal. Si S es normal, entonces todos sus conjugados coinciden con S, y como los conjugados de S son todos los p-subgrupos de Sylow, deducimos $n_p = 1$. $\square$

Observación 10.13. Si n_p es la cantidad de p-subgrupos de Sylow de G y S es un p-subgrupo de Sylow, entonces la proposición 8.21 implica

$$n_p = [G : N_G(S)].$$

Luego de $S < N_G(S) < G$, se deduce $n_p \mid [G : S]$. Por lo tanto si $|G| = p^n k$, con $p \nmid k$, entonces

$$n_p \mid k \qquad \text{y} \qquad n_p \equiv 1 (\mathrm{mod}\ p). \tag{12}$$

En los ejemplos que siguen se utilizan las fórmulas (12) para determinar los posibles valores de cada n_p. En general S_p va a denotar un p-subgrupo de Sylow del grupo.

Ejemplo 10.14. Probaremos que si $|G| = 11^2 13^2$, entonces G es abeliano. La única posibilidad es $n_{11} = n_{13} = 1$. Luego $S_{11} \lhd G$ y $S_{13} \lhd G$. Al ser $|S_{11}| = 11^2$ y $|S_{13}| = 13^2$, se deduce que ambos son abelianos y $S_{11} \cap S_{13} = \{1\}$. Luego $G = S_{11} S_{13} \simeq S_{11} \times S_{13}$.

Ejemplo 10.15. Probaremos que si $|G| = 30$, entonces G contiene un subgrupo normal de orden 15. Es $n_3 = 1$ o 10 y $n_5 = 1$ o 6. Si fuesen $n_3 = 10$ y $n_5 = 6$, entonces tendríamos 20 elementos de orden 3 (cada 3-subgrupo de Sylow es de orden 3 y por lo tanto tiene dos elementos de orden 3) y tendríamos 24 elementos de orden 5 (por lo mismo), eso nos da $20 + 24 = 44$, que es mayor que el orden de G. Luego ese caso no es posible y por lo tanto $n_3 = 1$ o $n_5 = 1$. Entonces $S_3 \lhd G$ o $S_5 \lhd G$ y por lo tanto $H = S_3 S_5$ es un subgrupo de G de orden 15. Como $[G : H] = 2$, deducimos $H \lhd G$.

Ejemplo 10.16. Probaremos que si $|G| = 72$, entonces G no es simple. Es $n_3 = 1$ o 4. Si $n_3 = 1$, entonces $S_3 \lhd G$. Si $n_3 = 4$, entonces $[G : N_G(S_3)] = 4$ y por lo tanto $|G| \nmid [G : N_G(S_3)]!$. Luego existe $\{1\} \neq K \subset N_G(S_3) \subsetneq G$ tal que $K \lhd G$.

Proposición 10.17. *Si todos los subgrupos de Sylow de G son normales, entonces G es isomorfo a su producto directo. Además si un natural m divide a $|G|$, entonces existe $H < G$ tal que $|H| = m$.*

Dem. Sean $p_1, \ldots, p_r$ los primos que dividen al orden de G y $S_1, \ldots, S_r$ los subgrupos de Sylow correspondientes. Como $S_1, \ldots, S_r$ son normales y sus órdenes son primos dos a dos, se deduce que su producto $S_1 \cdots S_r$ es un subgrupo normal de G isomorfo a $S_1 \times \cdots \times S_r$. Por otro lado es claro que $|S_1 \cdots S_r| = |G|$, luego $G \simeq S_1 \times \cdots \times S_r$. La última afirmación se prueba aplicando la proposición 10.5 a cada S_i. $\square$

Corolario 10.18. *Sea G un grupo abeliano. Si m divide a $|G|$, entonces existe $H < G$ tal que $|H| = m$.* $\square$

11. Grupos abelianos finitamente generados

Recordar que usamos $C_\infty \simeq \mathbb{Z}$ para el grupo cíclico infinito y $C_n \simeq \mathbb{Z}_n$ para el grupo cíclico de orden $n = 2, 3, \dots$ Por coherencia de notación vamos a usar notación multiplicativa para los grupos abelianos, en lugar de la más común aditiva. Observar que un grupo abeliano G está finitamente generado si existe una cantidad finita de elementos $g_1, \dots, g_k \in G$ tales que

$$G = \left\{ g_1^{n_1} \cdots g_k^{n_k} : \ n_1, \dots, n_k \in \mathbb{Z} \right\}.$$

Teorema 11.1 (Teorema de estructura)**.** *Sea G un grupo abeliano finitamente generado.*

1. *Existen $k \in \mathbb{N}$ y H grupo abeliano finito tales que $G \simeq H \times (C_\infty)^k$.*
2. *Si $G \neq \{1\}$ es un grupo abeliano finito, entonces*
   a) *Existen $d_1, \dots, d_s \in \mathbb{Z}^+$, con $2 \leq d_1 \mid d_2 \mid \cdots \mid d_s$, tales que $G \simeq C_{d_1} \times \cdots \times C_{d_s}$.*
   b) *Existen primos $p_1, \dots, p_r$ y enteros $n_1, \dots, n_r \in \mathbb{Z}^+$ tales que $G \simeq C_{p_1^{n_1}} \times \cdots \times C_{p_r^{n_r}}$.*

El grupo H de la primer parte es único a menos de isomorfismo. Todo el resto (incluidos r y s) es único, aunque pueden aparecer elementos repetidos.

Dem. Ver la bibliografía. $\square$

Observaciones 11.2. 1. El producto directo es "conmutativo" en el sentido $H \times K \simeq K \times H$. Luego la unicidad en la última descomposición es a menos del orden de los factores.

2. Si m y n son primos entre sí, entonces $C_m \times C_n \simeq C_{mn}$ es cíclico. Luego si $p_1, \dots, p_k$ son primos distintos, entonces $C_{p_1^{n_1}} \times \cdots \times C_{p_k^{n_k}} \simeq C_{p_1^{n_1} \cdots p_k^{n_k}}$ es cíclico. En contraposición, notar $C_p \times C_p \not\simeq C_{p^2}$.

3. Si G es un grupo abeliano finito de orden ${p_1}^{n_1} \cdots {p_k}^{n_k}$, entonces la proposición 10.17 implica $G \simeq S_1 \times \cdots \times S_k$, siendo S_i el p_i-subgrupo de Sylow correspondiente. Notar $|S_i| = p_i^{n_i}$. Esto prueba parte de la existencia de la última descomposición.

Ejemplo 11.3. Si G es un grupo abeliano de orden 72, entonces G es isomorfo a uno de los siguientes

$$C_2 \times C_2 \times C_2 \times C_3 \times C_3; \quad C_4 \times C_2 \times C_3 \times C_3; \quad C_8 \times C_3 \times C_3; \quad C_2 \times C_2 \times C_2 \times C_9; \quad C_4 \times C_2 \times C_9; \quad C_8 \times C_9.$$

La otra forma de describirlos es

$$C_2 \times C_6 \times C_6; \quad C_6 \times C_{12}; \quad C_3 \times C_{24}; \quad C_2 \times C_2 \times C_{18}; \quad C_2 \times C_{36}; \quad C_{72}.$$

12. Grupos de orden bajo

En esta sección veremos de clasificar todos los grupos de orden menor o igual que 15.

Empezamos recordando algunos resultados:

- El teorema de estructura nos dice cómo son los grupos abelianos finitos.
- Si $|G| = p$, p primo, entonces G es cíclico ($G = C_p$).
- Si $|G| = p^2$, p primo, entonces G es abeliano ($G = C_{p^2}$ o $G \simeq C_p \times C_p$).

- Sea G un grupo y N, K dos subgrupos tales que N es normal, $G = NK$ y $N \cap K = \{1\}$. Si K es normal entonces $G \simeq N \times K$, en caso contrario $G \simeq N \rtimes_\alpha K$ para algún morfismo no trivial $\alpha : K \to \mathrm{Aut}(N)$.

  Por ejemplo el grupo diedral D_n se puede escribir $D_n \simeq C_n \rtimes_\alpha C_2$. Si es $C_2 = \langle a \rangle$, entonces α queda determinado por $\alpha_a(x) = x^{-1}$, para todo $x \in C_n$.

- Supongamos $|G| = pq$, $p < q$ primos. Si G es abeliano, entonces es cíclico $G \simeq C_{pq}$. Si G no es abeliano entonces es isomorfo a un producto semidirecto $C_q \rtimes_\alpha C_p$ y además admite una presentación $G = \langle a, b :\ a^p = b^q = 1,\ aba^{-1} = b^r \rangle$, siendo $r \in \mathbb{Z}^+$ tal que $r^p \equiv 1 (\mathrm{mod}\ q)$ y $r \not\equiv 1 (\mathrm{mod}\ q)$. Esta última posibilidad solo puede ocurrir si $q \equiv 1 (\mathrm{mod}\ p)$.

Teorema 12.1. *A menos de isomorfismo hay solo dos grupos no abelianos de orden 8, el diedral D_4 y el grupo de los cuaternios Q.*

Dem. Sea G un grupo no abeliano de orden 8. Si $g^2 = 1$ para todo $g \in G$, entonces G sería abeliano. Tampoco puede tener elementos de orden 8 porque sería cíclico. Luego existe $a \in G$ de orden 4. Observar que $\langle a \rangle$ tiene índice 2, luego es normal. Sea $b \in G$ tal que $b \notin \langle a \rangle$, entonces

$$G = \langle a \rangle \sqcup b\langle a \rangle = \left\{1, a, a^2, a^3, b, ba, ba^2, ba^3\right\}. \tag{13}$$

Como $\langle a \rangle = \{1, a, a^2, a^3\}$ es normal y bab^{-1} tiene el mismo orden que a, deducimos $bab^{-1} = a$ o $bab^{-1} = a^3$. Si fuese $bab^{-1} = a$, sería $ba = ab$ y esto implicaría que $G = \langle a, b \rangle$ es abeliano, lo cual no es el caso; luego $bab^{-1} = a^3$. Notar que de (13) se deduce $b^2 \in \langle a \rangle$. Si fuese $b^2 = a$ o $b^2 = a^3$, sería $|b| = 8$ que no es posible; luego $b^2 = 1$ o $b^2 = a^2$.

Resumiendo tenemos dos posibilidades:

- $G = \langle a, b \rangle$, con $|a| = 4$, $ba = a^3 b$ y $b^2 = 1$, luego $G \simeq D_4$.
- $G = \langle a, b \rangle$, con $|a| = 4$, $ba = a^3 b$ y $b^2 = a^2$, luego $G \simeq Q$. □

Observación 12.2. Consideremos la descripción de los cuaternios dada en (13). Se ve directamente que a^2 tiene orden 2 y todos los elementos restantes menos el neutro tienen orden 4. En particular hay un solo subgrupo de orden 2 que es $\langle a^2 \rangle$ y los subgrupos de orden 4 de Q son:

$$\langle a \rangle = \left\langle a^3 \right\rangle = \{1, a, a^2, a^3\}, \qquad \langle b \rangle = \left\langle ba^2 \right\rangle = \{1, b, a^2, ba^2\}, \qquad \langle ba \rangle = \left\langle ba^3 \right\rangle = \{1, ba, a^2, ba^3\}.$$

Luego todo subgrupo de orden 4 contiene al único subgrupo de orden 2. Esto implica que Q no es un producto semidirecto[7], a diferencia de $D_4 = C_4 \rtimes_\alpha C_2$.

En lo que sigue estudiaremos los grupos de orden 12. Para eso necesitamos el siguiente resultado.

Proposición 12.3. *Sea $\alpha : C_2 \times C_2 \to \mathrm{Aut}(C_3)$ un morfismo no trivial. Entonces el producto semidirecto $C_3 \rtimes_\alpha (C_2 \times C_2)$ es isomorfo al grupo diedral D_6.*

Dem. Sea $G = C_3 \rtimes_\alpha (C_2 \times C_2)$. Sabemos que si definimos $N = \{(x, 1) :\ x \in C_3\}$ y $K = \{(1, y) :\ y \in C_4\}$, entonces valen

$$C_3 \simeq N \lhd G, \quad C_2 \times C_2 \simeq K < G, \quad G = NK, \quad N \cap K = \{1\}.$$

Luego existen $x, y, z \in G$ tales que $K = \{1, x, y, xy\}$, con $yx = xy$, $x^2 = y^2 = 1$ y $N = \{1, z, z^2\}$, con $z^3 = 1$.

[7] Nos referimos a un producto semidirecto no trivial, dado que siempre tenemos $G \simeq G \times \{1\}$.

Probaremos que existe $g \in K$, $g \neq 1$, tal que $gz = zg$. Consideremos $x \in K$. Como es $N \lhd G$, entonces $xzx^{-1} \in N$ y al ser $\left|xzx^{-1}\right| = |z| = 3$, deducimos, $xzx^{-1} = z$ o $xzx^{-1} = z^2$, lo cual equivale a $xz = zx$ o $xz = z^2x$. En el primer caso ya tenemos lo que queríamos. Supongamos ahora que es $xz = z^2x$. Razonando análogamente con $y \in K$ deducimos que vale $yz = zy$ o $yz = z^2y$. De nuevo en el primer caso tenemos lo que queríamos y nos queda por considerar cuando valen $xz = z^2x$ y $yz = z^2y$. En ese caso es $(xy)z = x(yz) = x(z^2y) = (xz^2)y = (zx)y = z(xy)$. Luego $xy \in K$ y verifica $(xy)z = z(xy)$.

Entonces, eventualmente cambiándole el nombre a los elementos de K, podemos asumir que vale $xz = zx$. Sea $b = xz$. Como es $|x| = 2$, $|z| = 3$ y $xz = zx$, entonces $|b| = 6$. Luego $[G : \langle b\rangle] = 2$ y por lo tanto $\langle b\rangle \lhd G$.

Consideremos $y \in K$. Notar $\langle y\rangle = \{1, y\}$. Como $N \cap K = \{1\}$ y $b = xz$, entonces $y \notin \langle b\rangle$. Luego $\langle y\rangle \cap \langle b\rangle = \{1\}$ y por lo tanto $|\langle y\rangle\langle b\rangle| = 12 = |G|$, lo cual implica $G = \langle y\rangle\langle b\rangle = \langle y, b\rangle$. Por otro lado la normalidad de $\langle b\rangle$ implica $yby^{-1} \in \langle b\rangle$. Como tiene que ser $\left|yby^{-1}\right| = |b| = 6$, deducimos que vale $yb = by$ o $yb = b^5y$. Como es $G = \langle y, b\rangle$, si fuese $yb = by$ entonces G sería abeliano, lo cual no es posible. Luego es $yb = b^5y$. Así obtuvimos $G = \langle y, b\rangle$, con $|y| = 2$, $|b| = 6$ y $yb = b^5y$; luego $G \simeq D_6$. $\square$

Observación 12.4. Es $\mathrm{Aut}(C_3) = \{\mathrm{id}, \sigma\}$, siendo $\sigma(x) = x^{-1}$, para todo $x \in C_3$. Observar que vale $\sigma^2 = \mathrm{id}$ y por lo tanto $\sigma^4 = \mathrm{id}$. Luego si escribimos $C_4 = \langle a\rangle$, entonces existe un único morfismo no trivial $\alpha : C_4 \to \mathrm{Aut}(C_3)$ determinado por $\alpha_a = \sigma$. Luego existe un único grupo no abeliano de la forma $C_3 \rtimes_\alpha C_4$.

Teorema 12.5. *A menos de isomorfismo hay solo tres grupos no abelianos de orden 12, el diedral D_6, el alternado A_4 y el producto semidirecto $C_3 \rtimes_\alpha C_4$, siendo $\alpha : C_4 \to \mathrm{Aut}(C_3)$ el morfismo no trivial.*

Dem. Sea G un grupo no abeliano de orden 12. Sea H un subgrupo de G de orden 3 (un 3-subgrupo de Sylow). Si n_3 es la cantidad de 3-subgrupos de Sylow de G, entonces $n_3 \mid 4$ y $n_3 \equiv 1 (\mathrm{mod}\ 3)$, luego $n_3 = 1, 4$.

Supongamos $n_3 = 4$, luego H no es normal. Aplicando la proposición 8.22 obtenemos un morfismo $\varphi : G \to \mathrm{Biy}(G/H) \simeq \mathcal{S}_4$ que verifica $\mathrm{Ker}\,\varphi < H$. Si φ no fuese inyectivo, entonces sería $H = \mathrm{Ker}\,(\varphi)$, lo cual no es posible porque H no es normal. Luego φ es inyectivo y por lo tanto $[\mathcal{S}_4 : \varphi(G)] = 2$. Como A_4 es el único subgrupo de índice 2 de $\mathcal{S}_4$, se deduce $G \simeq \varphi(G) = A_4$.

Supongamos ahora $n_3 = 1$ y por lo tanto H es normal. Sea K un 2-subgrupo de Sylow de G. Observar que $|H \cap K| = 1$, luego $G = HK$, siendo $H \cap K = \{1\}$. Notar que H es cíclico y K es abeliano. Si K fuese normal, entonces $G \simeq H \times K$ sería abeliano. Luego K no es normal. Por lo tanto existe un morfismo no trivial $\alpha : K \to \mathrm{Aut}(H)$ tal que $G \simeq H \rtimes_\alpha K$, siendo $H = C_3$.
Notar que al ser $|K| = 4$, es $K = C_4$ o $K \simeq C_2 \times C_2$. Como los 2-subgrupos de Sylow son conjugados (y por lo tanto isomorfos), entonces todos los subgrupos de orden 4 de G son de una forma o de la otra.
Si $K = C_4$ entonces $G \simeq C_3 \rtimes_\alpha C_4$, siendo α el único morfismo no trivial de C_4 en $\mathrm{Aut}(C_3)$. Si $K \simeq C_2 \times C_2$, entonces $G \simeq C_3 \rtimes_\alpha (C_2 \times C_2)$ y por lo tanto la proposición 12.3 implica $G \simeq D_6$.

Para distinguir los grupos A_4, $C_3 \rtimes_\alpha C_4$ y D_6 consideramos sus 2-subgrupos de Sylow. El grupo A_4 tiene un subgrupo normal de orden 4, $C_3 \rtimes_\alpha C_4$ tiene a C_4 como subgrupo no normal y $D_6 \simeq C_3 \rtimes_\alpha (C_2 \times C_2)$ tiene un subgrupo del tipo $C_2 \times C_2$ que no es normal; luego no pueden haber isomorfismos entre estos ellos. $\square$

Proposición 12.6. *El grupo no abeliano $C_3 \rtimes_\alpha C_4$ admite la presentación $\langle a, b :\ a^4 = b^3 = 1,\ ab = b^2a\rangle$.*

Dem. Sea $G = C_3 \rtimes_\alpha C_4$. Razonando como en la proposición 12.3 sabemos que existen subgrupos N, K de G tales que $G = NK$, $N \cap K = \{1\}$, $C_3 \simeq N \lhd G$, $C_4 \simeq K < G$. Luego existen $a \in G$ tal que $K = \langle a\rangle$, con $|a| = 4$ y $b \in G$ tal que $N = \langle b\rangle$, con $|b| = 3$. Como es $N \lhd G$, entonces $aba^{-1} \in N$, y como además sabemos $\left|aba^{-1}\right| = |b| = 3$, entonces deducimos que vale $aba^{-1} = b$ o $aba^{-1} = b^2$, lo cual equivale a $ab = ba$ o $ab = b^2a$. Como es $G = NK = \langle b\rangle\langle a\rangle = \langle a, b\rangle$, si fuese $ab = ba$ entonces G sería abeliano, lo cual no es posible. Luego es $G = \langle a, b\rangle$ y valen $|a| = 4$, $|b| = 3$ y $ab = b^2a$, lo cual implica la tesis. $\square$

Aplicando los resultados anteriores, la lista de grupos de orden menor o igual a 15 es la siguiente:

orden	abeliano	no abeliano
1	$\{1\}$	
2	C_2	
3	C_3	
4	C_4, $C_2 \times C_2$	
5	C_5	
6	$C_6 = C_2 \times C_3$	D_3
7	C_7	
8	C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$	D_4, Q
9	C_9, $C_3 \times C_3$	
10	$C_{10} = C_2 \times C_5$	D_5
11	C_{11}	
12	$C_{12} = C_3 \times C_4$, $C_2 \times C_6 = C_2 \times C_2 \times C_3$	$D_6 = C_2 \times D_3$, A_4, $C_3 \rtimes_\alpha C_4$
13	C_{13}	
14	$C_{14} = C_2 \times C_7$	D_7
15	$C_{15} = C_3 \times C_5$	

Referencias

[1] T. W. Hungerford, *Algebra*, Springer-Verlag.

[2] S. Lang, *Algebra*, Addison-Wesley, 1993.