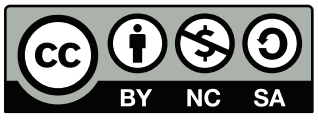
ESTRUCTURAS ALGEBRAICAS

ApuntsFME

Barcelona, Octubre 2018

Última modificación: 21 de octubre de 2018.



Contenidos

Tema 0

Permutaciones

0.1. Repaso de permutaciones

El grupo simétrico $(S_n, \circ)$ es el grupo de las permutaciones de los elementos $\{1, 2, \ldots, n\}$ y el cardinal de S_n es $\#S_n = |S_n| = n!$

Si $\sigma \in S_n$, podemos escribir σ como

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

Cualquier permutación se descompone en ciclos, por ejemplo $\sigma = (1, 4, 5, 2) \in S_5$ es lo mismo que

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}.$$

Entonces $\sigma = \sigma_1 \cdots \sigma_r$, siendo σ_i ciclos disjuntos.

Observación 0.1.1. La multiplicación no es conmutativa. Pero las permutaciones con elementos disjuntos sí que conmutan.

Todo ciclo se puede descomponer como producto de transposiciones $z = (i, j)$. Por lo tanto, podemos descomponer toda permutación como producto de transposiciones, pero esta descomposición no es única. Lo que sí que se mantiene es la paridad del número de trasposiciones. Es decir,

$$\left.\begin{aligned} \sigma &= z_1 \cdots z_r \\ \sigma &= \bar{z}_1 \cdots \bar{z}_s \end{aligned}\right\} \implies (r \text{ par} \iff s \text{ par}).$$

Esto nos permite definir unequívocamente el signo de la permutación:

$$\operatorname{sgn}(\sigma) = (-1)^r,$$

donde r es el número de trasposiciones de cualquiera de sus descomposiciones en transposiciones.

Definición 0.1.2. Definimos el orden de una permutación σ como el mínimo k tal que $\sigma^k = \mathrm{Id}$.

Ejemplo 0.1.3. $\sigma = (1,4,5,2)$. Calcular el orden de σ.

$$\sigma^2 = \sigma \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix},$$

y así sucesivamente, llegaremos a que $\sigma^4 = \mathrm{Id}$.

Proposición 0.1.4. Más en general, se tiene que, si $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$ es una descomposición en permutaciones disjuntas, entonces

$$\mathrm{ord}(\sigma) = \mathrm{mcm}\left(\mathrm{ord}(\sigma_1), \mathrm{ord}(\sigma_2), \ldots, \mathrm{ord}(\sigma_r)\right).$$

0.2. Ejercicios

Ejercicio 0.2.1. En general toda permutación de S_n descompone en producto de trasposiciones $(1,2), (1,3), \ldots (1,n)$.

Demostración. En general tenemos que una trasposición cualquiera

$$(i,j) = (1,i)(1,j)(1,i).$$

□

Ejercicio 0.2.2.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} = (1,3,8)(2,7)(4,9,6,5)$$

Por lo tanto, el orden de σ es

$$\mathrm{ord}(\sigma) = \mathrm{mcm}\,(3,2,4) = 12.$$

Ahora, descomponemos en trasposiciones.

$$\begin{aligned} (1,3,8) &= (1,8)(1,3), \\ (2,7) &= (2,7), \\ (4,9,6,5) &= (4,5)(4,6)(4,9), \end{aligned}$$

con lo cual $\mathrm{sgn}(\sigma) = (-1)^6 = 1$.

Ejercicio 0.2.3. Encontrar todos los valores x, y, z, t tales que

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 6 & x & y & 1 & z & t \end{pmatrix}$$

tenga orden tres.

Primero descomponemos σ.

$$\sigma = (1,3,6)\begin{pmatrix} 2 & 4 & 5 & 7 & 8 \\ 5 & x & y & z & t \end{pmatrix}.$$

Queremos que el segundo miembro tenga orden 3.

- Si $y = 2$, tenemos el ciclo $(2,5)$ que tiene orden 2 y por lo tanto $\text{ord}(\sigma)$ es múltiplo de 2.
- Los otros casos quedan como ejercicio.

Tema 1

Grupos

1.1. Grupos

Definición 1.1.1. Un grupo es un par $(G, \cdot)$, donde G es un conjunto no vacío y $\cdot$ es una operación interna, es decir, una aplicación

$$\begin{aligned} \cdot \colon G \times G &\to G \\ (a, b) &\mapsto a \cdot b \end{aligned}$$

que satisface

i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, i.e., la propiedad asociativa,

ii) $\exists e$ t. q. $\forall a \in G$, $a \cdot e = e \cdot a = a$, i.e., existe un elemento neutro,

iii) $\forall a \in G$, $\exists \tilde{a} \in G$ t. q. $a \cdot \tilde{a} = \tilde{a} \cdot a = e$, i.e., todo elemento tiene inverso.

Nota. Cuando la operación del grupo sea irrelevante, evidente o se deduzca del contexto, escribiremos G en lugar de $(G, \cdot)$, o de $(G, +)$, etc., cometiendo un abuso de notación.

Nota segunda. Además, a menudo también escribiremos ab en lugar de $a \cdot b$ y $a \cdot b$ en lugar de $a \circ b$, como por ejemplo en la composición de permutaciones.

Definición 1.1.2. Decimos que G es un grupo abeliano o conmutativo si es un grupo y además satisface la propiedad conmutativa:

$$ab = ba, \quad \forall a, b \in G.$$

Observación 1.1.3. Existen varias notaciones para referirnos a esta operación:

Operación	Símbolo	Elemento neutro	Elemento inverso
Aditiva	$+$	0	$-a$ (e. opuesto)
Multiplicativa	$\cdot$	1	a^{-1}

Nota. Siempre que utilicemos $+$ para la operación del grupo, la operación será conmutativa.

Definición 1.1.4. Sea $(G, \cdot)$ un grupo. Decimos que $\left(H, \cdot_{|H}\right)$ es un subgrupo de $(G, \cdot)$ si $H \subseteq G$ y se satisface

i) $H \neq \varnothing$,

ii) $a, b \in H \implies a \cdot b \in H$ (la operación es cerrada),

iii) $\forall a \in H, a^{-1} \in H$.

Nota. A menudo cometeremos un abuso de notación, escribiendo $(H, \cdot)$ en lugar de $\left(H, \cdot_{|H}\right)$.

Proposición 1.1.5. Los subgrupos son aquellos grupos $\left(H, \cdot_{|H}\right)$ con $H \subseteq G$.

Demostración. Sea $(H, \cdot)$ un subgrupo de $(G, \cdot)$. Queremos ver que $(H, \cdot)$ es un grupo. Tenemos la operación

$$\begin{aligned} \cdot : H \times H &\to H \\ (a, b) &\mapsto a \cdot b \in H. \end{aligned}$$

Tiene la propiedad asociativa porque es la restricción de una operación con la propiedad asociativa. Existe elemento neutro ya que $\exists a \in H$ y $\exists a^{-1} \in H$, de modo que $a \cdot a^{-1} = e \in H$. La última propiedad está impuesta.

Recíprocamente, veamos que si $H \subseteq G$ y $\left(H, \cdot_{|H}\right)$ es un grupo, entonces $\left(H, \cdot_{|H}\right)$ es un subgrupo de G. Por ser $\left(H, \cdot_{|H}\right)$ un grupo, $1 \in H \implies H \neq \varnothing$. Las otras dos propiedades están en la propia definición de grupo. □

Ejemplo 1.1.6.

1. Sea G un grupo. Los subgrupos impropios son $\{1\}$ (el grupo trivial) y G.

2. $(\mathbb{Z}, +), (\mathbb{N}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ son grupos y subgrupos.

3. $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ es un grupo.

4. Si G y H son dos grupos, entonces

$$G \times H = \left\{(x, y) \mid x \in G,\, y \in H\right\}$$

es un grupo, con $(a, b) \cdot (c, d) = (ac, bd)$.

5. *Grupo simétrico.* $(\mathcal{S}_n, \circ)$ es el grupo simétrico de n elementos (permutaciones de n elementos).

6. *Grupo diedral.* $(D_{2n}, \circ)$, donde D_{2n} son los conjuntos de las isometrías del plano que dejan invariante P_n. P_n es un polígono regular de n lados (raíces n-esimas de 1). Por ejemplo,

$$D_{2\cdot 4} = \left\{id, r, r^2, r^3, s, rs, r^2 s, r^3 s\right\}$$

Con r la rotación horaria de $\pi/2$ y s la simetría respecto del eje x.

1.2. Intersección y producto de subgrupos

Definición 1.2.1. Sea G un grupo y sean $H, K \subset G$ subgrupos de G. Definimos la intersección de H y K como

$$H \cap K = \left\{ x \in G \mid x \in H \text{ y } x \in K \right\}.$$

Observación 1.2.2. Si H y K son subgrupos de G, $H \cap K$ es un subgrupo de G. También es cierto con la instersección arbitraria.

Definición 1.2.3. Sea G un grupo y sean $H, K \subseteq G$ subgrupos de G. Llamamos unión de H y K a

$$H \cup K = \left\{ x \in G \mid x \in H \text{ o } x \in K \right\}.$$

Observación 1.2.4. En general, la unión de subgrupos no es un grupo.

Ejemplo 1.2.5. Tomamos el grupo simétrico como ejemplo:

$$\mathcal{S}_3 = \left\{ \mathrm{Id}, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2) \right\}$$

y tomamos

$$H = \left\{ \mathrm{Id}, (1\,2) \right\}, \; K = \left\{ \mathrm{Id}, (1\,3) \right\}$$

ahora

$$H \cup K = \left\{ \mathrm{Id}, (1\,2), (1\,3) \right\}$$

pero

$$(1\,2)(1\,3) = (1\,3\,2) \notin H \cup K.$$

Definición 1.2.6. Sea G un grupo y sean $H, K \subset G$ subgrupos. Definimos el producto $H \cdot K$ como

$$H \cdot K = \left\{ xy \mid x \in H \text{ y } x \in K \right\}.$$

Observación 1.2.7. En general, el producto de subgrupos, no es grupo.

Ejemplo 1.2.8. Tomando las definiciones de G, H y K del ejemplo anterior, tenemos que

$$H \cdot K = \left\{ \mathrm{Id}, (1\,3), (1\,2), (1\,2)(1\,3) = (1\,3\,2) \right\},$$

que no es un grupo.

Observación 1.2.9. Si G es conmutativo, el producto de subgrupos es un grupo.

Demostración. Comprobemos que $H \cdot K$ satisface las propiedades de los grupos.

i) $\left.\begin{array}{l} H \text{ sg.} \implies 1 \in H \\ K \text{ sg.} \implies 1 \in K \end{array}\right\} \implies 1 = 1 \cdot 1 \in H \cdot K.$

ii) $\left.\begin{array}{l} xy \in HK \\ zt \in HK \end{array}\right\} \implies (xy)(zt) = (xyzt) = (xz)(yt) \in HK.$

iii) $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} \in HK.$

□

Observación 1.2.10. Se tiene que

$$H \cap K \subseteq H, K \subseteq H \cup K \subseteq H \cdot K.$$

Demostración. Tenemos que $H \cup K \subseteq HK$ ya que $\forall x \in H$, $x \cdot 1 = x \in HK$ y análogamente para K. Las otras inclusiones son triviales a partir de las definiciones. □

Observación 1.2.11. Si HK es un subgrupo, entonces es el menor subgrupo que contiene a $H \cup K$.

Demostración. Sabemos que $H \cup K \subseteq HK$ por 1.2.10. Suponemos ahora que L es un subgrupo de G que contiene a $H \cup K$. Queremos ver que $H \cdot K \subseteq L$. Sea $z = ab \in HK$ ($a \in H$, $b \in K$),

$$\left.\begin{array}{l} a \in H \subset L \\ b \in K \subset L \\ L \text{ es subgrupo} \end{array}\right\} \implies ab = z \in L \implies HK \in L.$$

□

Definición 1.2.12. Sea $(G, \cdot)$ un grupo y sea $S \subseteq G$. Definimos el subgrupo generado por S a

$$\langle S \rangle = \left(\{1\} \cup \left\{ a_1 \cdots a_r \mid a_i \in S \text{ ó } a_i^{-1} \in S \right\}, \cdot \right).$$

Observación 1.2.13. Si $S = \varnothing$, entonces $\langle S \rangle = \left(\{1\}, \cdot \right)$.

Observación 1.2.14. $\langle S \rangle$ es el menor subgrupo de de G que contiene a S.

Demostración. Si $S = \varnothing$ entonces es trivial. Si $S \neq \varnothing$, es trivial que $S \subset \langle S \rangle$, veamos ahora que es un subgrupo de G.

i) $\exists a \in S \implies a \in \langle S \rangle \implies \langle S \rangle \neq \varnothing$,

ii) Si $a_1 \cdots a_r, b_1 \cdots b_s \in \langle S \rangle$, entonces $a_1 \cdots a_r b_1 \cdots b_s \in \langle S \rangle$,

iii) Si $a_1 \cdots a_r \in \langle S \rangle$, entonces $(a_1 \cdots a_r)^{-1} = a_r^{-1} \cdots a_1^{-1} \in \langle S \rangle$.

Tomamos ahora L un subgrupo de G que contiene a S. Queremos ver que $\langle S \rangle \subseteq L$. Para cualquier $a_1 \cdots a_r \in \langle S \rangle$ tenemos que

$$\left.\begin{array}{l} a_1 \in S \subseteq L \text{ o } a_1^{-1} \in S \implies \left(a_1^{-1}\right)^{-1} \in L \\ \vdots \\ a_r \in S \subseteq L \text{ o } a_r^{-1} \in S \implies \left(a_r^{-1}\right)^{-1} \in L \end{array}\right\} \implies a_1 \cdots a_r \in L.$$

y por lo tanto, $\langle S \rangle \subset L$. □

Ejercicio 1.2.15. Demostrar que

$$\langle S \rangle = \left\{ a_1^{n_1} \cdots a_r^{n_r} \mid a_i \in S,\, n_i \in \mathbb{Z} \right\}.$$

Ejercicio 1.2.16. Demostrar que

$$\langle S \rangle = \bigcap_{\substack{H \text{ sg. de } G \\ S \subseteq H}} H.$$

1.3. Orden de un elemento

Definición 1.3.1. Sea G un grupo y sea $x \in G$. Llamamos orden de x, si existe, al menor entero $n \geq 1$ tal que

$$x^n = 1.$$

Si no existe, decimos que x tiene orden infinito.

Observación 1.3.2. Escribimos el orden de x como $\mathrm{o}(x)$ o $\mathrm{ord}(x)$.

Definición 1.3.3. Sea G un grupo. Llamamos orden de G a su cardinal y lo denotamos $\mathrm{o}(G)$, $\mathrm{ord}(G), |G|$ o $\mathrm{card}(G)$.

Ejemplo 1.3.4.

1. $\mathrm{ord}(e) = 1$ y es el único elemento (el neutro) que tiene orden 1.
2. En el grupo simétrico $G = \mathcal{S}_n$, sean $a_1, \ldots, a_n \in G$, $\mathrm{ord}\left((a_1, \ldots, a_n)\right) = n$.
3. En los grupos $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ y $(\mathbb{C}, +)$, $\forall x \neq 0$ $\mathrm{ord}(x) = \infty$.
4. En el grupo $\mathbb{Z}/p\mathbb{Z}$ con p primo, $\forall \bar{x} \neq \bar{0}$ $\mathrm{ord}\,(\bar{x}) = p$.
5. En los grupos $\mathbb{Q}^* = \left(\mathbb{Q} \setminus \{0\}, \cdot\right), \mathbb{R}^* = \left(\mathbb{R} \setminus \{0\}, \cdot\right)$, $\mathrm{ord}(-1) = 2$, $\mathrm{ord}(1) = 1$ y $\forall x \notin \{-1, 1\}$ $\mathrm{ord}(x) = \infty$.

6. En el grupo $\mathbb{C}^* = \left(\mathbb{C} \setminus \{0\}, \cdot\right)$, $\forall n \geq 1$ $\operatorname{ord}\left(e^{\frac{2\pi i}{n}}\right) = n$ y $\forall z \in \mathbb{C}$ t. q. $|z| \neq 1$, $\operatorname{ord}(z) = \infty$.

Lema 1.3.5. Sea G un grupo y $x \in G$ con $\operatorname{ord}(x) = n \in \mathbb{N}$. Entonces,

i) $x^m = 1 \iff n|m$.

ii) $x^m = x^{m'} \iff m \equiv m' \pmod{n}$.

iii) $\operatorname{ord}\left(x^m\right) = \frac{n}{\operatorname{mcd}(n,m)} = \frac{\operatorname{ord}(x)}{\operatorname{mcd}\left(\operatorname{ord}(x),m\right)}$.

Demostración.

i) Si $n|m$, entonces $m = n \cdot d$, con lo cual, $x^m = (x^n)^d = 1^d = 1$. Recíprocamente, pongamos $m = nq + r$, con $0 \leq r < n$. Entonces,

$$\left.\begin{array}{l} 1 = x^m = x^{nq+r} = (x^n)^q x^r = x^r \\ 0 \leq r < n \end{array}\right\} \implies r = 0 \implies n|m.$$

ii) $x^m = x^{m'} \iff x^{m-m'} = 1 \iff n|m - m' \iff m \equiv m' \pmod{n}$.

iii) Sean $k = \operatorname{ord}\left(x^m\right)$ y $g = \operatorname{mcd}(n, m)$. Queremos ver que $k = n/g$.

$$(x^m)^{\frac{n}{g}} = x^{\frac{mn}{g}} = (x^n)^{\frac{m}{g}} = 1 \implies k \left| \frac{n}{g} \right. .$$

Por otro lado,

$$1 = (x^m)^k = x^{mk} \implies n|mk \implies \frac{n}{g} \left| \frac{m}{g} k \overset{\substack{n/g \text{ y } m/g \\ \text{primos entre si}}}{\implies} \frac{n}{g} \right| k.$$

Y sumando los dos resultados, tenemos que $\frac{n}{g} = k$.

□

Definición 1.3.6. Diremos que un grupo G es cíclico si está generado por un solo elemento $x \in G$. Escribimos $G = \langle x \rangle$, G generado por x o x generador de G.

Observación 1.3.7. Sea G un grupo cíclico. Si $\operatorname{ord}(G) = n$ (con n finito), entonces

$$G = \left\{1 \left(= x^0\right), x, x^2, \ldots, x^{n-1}\right\}.$$

Lo denotaremos como $G = C_n$ (grupo cíclico de orden n). Si $\operatorname{ord}(G) = \infty$, entonces

$$G = \left\{x^k \mid k \in \mathbb{Z}\right\}.$$

Ejemplo 1.3.8.

1. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
2. $\mathbb{Z}/n\mathbb{Z} = \langle \bar{k} \rangle$ con $\text{mcd}(n, k) = 1$.

Definición 1.3.9. Sea $d \in \mathbb{Z}, d \geq 1$, definimos la función φ de Euler como

$$\varphi(d) = \text{card}\left\{1 \leq k \leq d \mid \text{mcd}(k, d) = 1\right\}.$$

Ejemplo 1.3.10.

$$\begin{array}{llll} \varphi(1) = 1, & \varphi(5) = 4, & \varphi(3) = 2, & \varphi(7) = 6, \\ \varphi(2) = 1, & \varphi(6) = 2, & \varphi(4) = 2, & \varphi(p) = p - 1 \text{ (con } p \text{ primo).} \end{array}$$

Proposición 1.3.11. Sea $G = \langle x \rangle$ un grupo cíclico, con $\text{ord}(x) = n$, entonces

i) $\forall y \in G, \text{ord}(y) | n$,

ii) $\forall d | n$, existen $\varphi(d)$ elementos de $G = C_n$ de orden d. De hecho, son

$$\left\{ x^{\frac{n}{d}k} \,\middle|\, 1 \leq k \leq d \text{ t. q. } \text{mcd}(k, d) = 1 \right\}.$$

Demostración.

i) Por ser y un elemento de G, es de la forma $y = x^m$, $0 \leq m \leq n$. Entonces,

$$\text{ord}(y) = \text{ord}\left(x^m\right) = \frac{\text{ord}(x)}{\text{mcd}\left(\text{ord}(x), m\right)} = \frac{n}{\text{mcd}(n, m)}.$$

Y concluimos $\text{ord}(y) | n$.

ii) Sea $y \in G$ t. q. $\text{ord}(y) = d$, tenemos que

$$y = x^m \implies \text{ord}(y) = d = \frac{n}{\text{mcd}(n, m)} \iff \text{mcd}(n, m) = \frac{n}{d}.$$

Buscamos los m tales que $\text{mcd}(n, m) = \frac{n}{d}$.

$$\text{mcd}(n, m) = \frac{n}{d} \iff \text{mcd}\left(\frac{n}{d}d, \frac{n}{d}k\right) = \frac{n}{d} \iff \text{mcd}(d, k) = 1.$$

Con esta última condición, tenemos que

$$\varphi(d) = \text{card}\left\{k \in \mathbb{Z} \mid \text{mcd}(k, d) = 1 \text{ y } 1 \leq k \leq d\right\} = \text{card}\left\{x^m \mid \text{ord}\left(x^m\right) = d\right\}.$$

□

Corolario 1.3.12. Se tiene que

$$n = \sum_{d|n} \varphi(d).$$

Demostración. Tomamos $G = C_n = \langle x \rangle$. Entonces,

$$n = |G| = \sum_{d|n} \operatorname{card}\left\{x \in G \mid \operatorname{ord}(x) = d\right\} = \sum_{d|n} \varphi(d),$$

ya que

$$G = \bigsqcup_{d|n} \left\{x \in G \mid \operatorname{ord}(x) = d\right\}.$$

□

Proposición 1.3.13. Sea $G = C_n = \langle x \rangle$ (con n finito). Entonces

i) Si $d|n$, entonces $x^{\frac{n}{d}}$ es un elemento de orden d y el subgrupo $H_d := \left\langle x^{\frac{n}{d}} \right\rangle$ es subgrupo cíclico de orden d.

ii) Si H es un subgrupo de G, entonces $\exists! d|n$ tal que $H = H_d$.

Demostración.

i) Se tiene que

$$\mathrm{o}\left(x^{\frac{n}{d}}\right) = \frac{n}{\operatorname{mcd}(n, \frac{n}{d})} = d.$$

Como $x^{\frac{n}{d}}$ tiene orden d, $H_d = \left\langle x^{\frac{n}{d}} \right\rangle$ es un grupo cíclico de orden d.

ii) Sea H un subgrupo de $G = C_n$ y sea $1 \leq t \leq n$ el menor exponente tal que $x^t \in H$. Veremos que $t|n$. Expresamos $n = tk + r$ (con $0 \leq r < t$).

$$1 = x^n = x^{tk+r} = \left(x^t\right)^k x^r.$$

Como $x^t \in H$, se tiene que $\left(x^t\right)^k, \left(\left(x^t\right)^k\right)^{-1} \in H$. Así,

$$x^r = \left(\left(x^t\right)^k\right)^{-1} \left(x^t\right)^k x^r = \left(\left(x^t\right)^k\right)^{-1} \in H.$$

Pero t es el exponente más pequeño (a excepción del 0) tal que $x^t \in H$ y, en consecuencia, como $r < t$, $r = 0$ y $n = tk$. Veremos ahora que $H = H_k$.

Claramente, $\left\langle x^{\frac{n}{k}} \right\rangle = H_k \subseteq H$, ya que $x^{\frac{n}{k}} = x^t \in H$ y, por lo tanto, todos sus múltiplos están en H.

Sea $y = x^m \in H$. Necesariamente, $m \geq t$. Escribimos $m = tq + s$ (con $0 \leq s < t$). Entonces,

$$x^m = x^{tq+s} = \left(x^t\right)^q x^s \implies x^s = \underbrace{\left(\left(x^t\right)^q\right)^{-1}}_{\in H} \cdot \underbrace{x^m}_{\in H} \in H.$$

de nuevo, por la definición de t, $s = 0$ y concluimos que $y = \left(x^t\right)^q \in \left\langle x^{\frac{n}{k}} \right\rangle = H_k$, es decir, $H \subseteq H_k$.

Solo resta ver que k es único, pero es obvio ya que, si $H = H_k = H_e$, entonces,

$$\frac{n}{k} = \mathrm{o}(H_k) = \mathrm{o}(H) = \mathrm{o}(H_e) = \frac{n}{e} \implies k = e.$$

□

Corolario 1.3.14. *Retículo de subgrupo de un grupo cíclico.* Sea $G = C_n = \langle x^n \rangle$ un grupo cíclico de orden $n \geq 1$. Existe una biyección

$$\begin{aligned} \{d \in \mathbb{N} \mid 1 \leq d \leq n,\, d|n\} &\longleftrightarrow \{\text{subgrupos de } G\} \\ d &\longleftrightarrow H_d. \end{aligned}$$

1.4. Morfismos de grupos

Definición 1.4.1. Sean G_1, G_2 dos grupos y sea $f\colon G_1 \to G_2$ una aplicación. Decimos que f es un (homeo)morfismo de grupos si

$$f(xy) = f(x)f(y).$$

Proposición 1.4.2. Si f es un morfismo de grupos, entonces

i) $f(1) = 1$,

ii) $f\left(x^{-1}\right) = \left(f(x)\right)^{-1}$.

Demostración.

i) Sea $x \in G_1$, $f(x) = f(x \cdot 1) = f(x)\, f(1) \implies f(1) = 1$.

ii) Sea $x \in G_1$, $f\left(xx^{-1}\right) = f(1) \overset{i)}{=} 1 = f(x)\, f\left(x^{-1}\right) \implies f\left(x^{-1}\right) = f(x)^{-1}$.

□

Observación 1.4.3. Notación:

Nombre	Propiedades
Monomorfismo	Inyectiva
Epimorfismo	Exhaustiva
Isomorfismo	Biyectiva
Endomorfismo	$G_1 = G_2$
Automorfismo	Biyectiva y $G_1 = G_2$

Proposición 1.4.4. Sea $f\colon G_1 \to G_2$ un morfismo biyectivo (isomorfismo). Entonces $f^{-1}\colon G_2 \to G_1$ es un morfismo de grupos.

Demostración. Como f es biyectiva, en particular es exhaustiva y inyectiva y tenemos que $\forall x' \in G_2$, $\exists! x \in G_1$ t. q. $f(x) = x'$. Sean $f(x), f(y) \in G_2$ dos elementos cualesquiera de G_2,

$$f^{-1}\left(f(x) f(y)\right) = f^{-1}\left(f(xy)\right) = xy = f^{-1}\left(f(x)\right) f^{-1}\left(f(y)\right).$$

□

Definición 1.4.5. Sean G_1 y G_2 grupos. Decimos que G_1 y G_2 son isomorfos si $\exists f \colon G_1 \to G_2$ isomorfismo. Lo notaremos como $G_1 \cong G_2$.

Proposición 1.4.6. Sea $f \colon G_1 \to G_2$ un morfismo de grupos.

i) Si H es un subgrupo de G_1, entonces $f(H)$ es subgrupo de G_2.

ii) Si K es un subgrupo de G_2, entonces, $f^{-1}(K)$ es subgrupo de G_1.

Demostración.

i) Veamos que se cumplen las tres propiedades de la definición 1.1.4.

   i) $1 \in H \implies f(1) = 1 \in f(H) \implies f(H) \neq \varnothing$.
   ii) Sean $a, b \in H$. Entonces, $ab \in H$ y $f(a)f(b) = f(ab) \in f(H)$.
   iii) Sea $a \in H$. Entonces, $a^{-1} \in H$ y $f(a)^{-1} = f\left(a^{-1}\right) \in H$.

ii) Veamos que se cumplen las tres propiedades de la definición 1.1.4.

   i) $1 \in K, f(1) = 1 \implies 1 \in f^{-1}(K) \neq \varnothing$.
   ii) Sean $a, b \in f^{-1}(K)$. Entonces, $f(a), f(b), f(a) f(b) \in K$ y tenemos que $ab \in f^{-1}\left(f(ab)\right) = f^{-1}\left(f(a) f(b)\right) \subseteq f^{-1}(K)$.
   iii) Sea $a \in f^{-1}(K)$. Entonces, $f(a) \in K, f(a)^{-1} = f\left(a^{-1}\right) \in K$, y tenemos que $a^{-1} \in f^{-1}\left(f\left(a^{-1}\right)\right) = f^{-1}\left(f(a)^{-1}\right) \subseteq f^{-1}(K)$.

□

Observación 1.4.7.

- $f(G_1) = \mathrm{Im}(f)$.
- $f^{-1}(1) = \ker(f)$.

Proposición 1.4.8. Sean G_1, G_2 grupos y sea $f \colon G_1 \to G_2$ un morfismo de grupos, entonces

i) f inyectiva $\iff \ker(f) = \{1\}$.

ii) f exhaustiva $\iff \mathrm{Im}(f) = G_2$.

Demostración. Ejercicio. □

1.5. Clases laterales

Definición 1.5.1. Sea G un grupo y $H \subseteq G$ un subgrupo. Dados $a, b \in G$, decimos que a está relacionado con b por la izquierda si

$$a^{-1}b \in H.$$

Ejercicio 1.5.2. Demostrar que que la relación definida es una relación de equivalencia. Para ello, hace falta ver que es reflexivo, simétrico y transitivo.

Definición 1.5.3. Con la relación que hemos visto ahora, denotamos la clase de equivalencia de $a \in G$ como

$$\begin{aligned}\bar{a} &= \left\{b \in G \mid a^{-1}b = x,\, x \in H\right\} \\ &= \left\{b \in G \mid b = ax,\, x \in H\right\} \\ &= aH.\end{aligned}$$

y llamaremos a aH clase lateral por la izquierda del elemento a módulo el subgrupo H.

Ejemplo 1.5.4. Si $a = 1$, tenemos que

$$1 \cdot H = \left\{1x \mid x \in H\right\} = H.$$

Observación 1.5.5. Tomamos

$$\begin{aligned} f_a \colon G &\to G \\ x &\mapsto f_a(x) = ax \end{aligned}$$

una aplicación biyectiva ($f_a^{-1} = f_{a^{-1}}$). Notemos, que f no es un morfismo de grupos (en general), ya que $f(1) = a$ (en general $a \neq 1$). Se tiene también que

$$f_a(H) = \left\{f_a(x) \mid x \in H\right\} = \left\{ax \mid x \in H\right\} = aH.$$

Diremos pues que hay una biyección $H \leftrightarrow aH$, en particular, si G es finito, se tiene que $|H| = |aH|$.

Definición 1.5.6. Sea G un grupo y sea H un subgrupo de G. Llamamos conjunto cociente de G módulo H a

$$G/H = \left\{aH \mid a \in G\right\} = \left\{\bar{a} \mid a \in G\right\},$$

es decir, el conjunto de las clases laterales por la izquierda de G módulo H.

Teorema 1.5.7. *Teorema de Lagrange.*
Sea G un grupo finito y sea H un subgrupo de G. Entonces,

$$|G| = |H| \left| G/H \right|.$$

Demostración. Se tiene que

$$G = \bigsqcup \bar{a}H.$$

Por lo tanto,

$$|G| = \left|\bigsqcup \bar{a}H\right| = \sum |\bar{a}H| = \sum_{k=1}^{\left|G/H\right|} |H| = |H| \left|G/H\right|.$$

□

Corolario 1.5.8. Si G es finito y H es subgrupo, entonces $|H|$ divide a $|G|$. Si $x \in G$,

$$\mathrm{o}(x) |\, \mathrm{o}(G) = |G|\,.$$

Demostración. Ya que $\mathrm{o}(x) = \mathrm{o}\left(\langle x \rangle\right)$ y $\mathrm{o}(H) |\, \mathrm{o}(G)$. □

Definición 1.5.9. Sea G un grupo y sea $H \subseteq G$ un subgrupo, decimos que $a, b \in G$ están relacionados por la derecha si

$$ab^{-1} \in H.$$

Ejercicio 1.5.10. Demostrar que se trata de una relación de equivalencia (propiedades simétrica, transitiva y reflexiva).

Definición 1.5.11. Tenemos que

$$\bar{a} = \left\{b \in G \mid ab^{-1} = x,\, y \in H\right\} = \left\{b \in G \mid b = ya,\, y \in H\right\} = Ha.$$

Llamamos clase lateral por la derecha de a módulo H a Ha.

Observación 1.5.12. Sea

$$\begin{aligned} g_a \colon G &\to G \\ x &\mapsto g_a(x) = xa. \end{aligned}$$

Notamos que es una aplicación biyectiva ($g_a^{-1} = g_{a^{-1}}$), pero que no es un morfismo de grupos. Además, $g_a(H) = Ha$ y, por lo tanto, se tiene una biyección $H \leftrightarrow Ha$. En particular, si G es finito, $|H| = |Ha|$.

Proposición 1.5.13. Existe una biyección

$$\begin{aligned} \left\{aH \mid a \in G\right\} &\to \left\{Hb \mid b \in G\right\} \\ xH &\mapsto Hx^{-1}. \end{aligned}$$

Demostración. Ejercicio: demostrar que está bien definida y que es biyectiva. □

Definición 1.5.14. Sea G un grupo y $H \subseteq G$ un subgrupo. Llamamos índice de G en H al cardinal de G/H. Y lo denotamos como

$$[G : H] = \left|G/H\right| \overset{\text{TL}}{=} \frac{|G|}{|H|}.$$

1.6. Subgrupos normales. Grupo cociente

Definición 1.6.1. Sea G un grupo y $H \subseteq G$ un subgrupo. Decimos que H es un subgrupo normal de G si $\forall a \in G$

$$aH = Ha,$$

y lo denotaremos como $H \triangleleft G$.

Observación 1.6.2. $H \triangleleft G$ no quiere decir que $ax = xa$ $(x \in H,\, a \in G)$. Quiere decir que $\forall x \in H,\, a \in G,\, \exists y \in H$ tal que $ax = ya$.

Proposición 1.6.3. Sea G un grupo y $H \subseteq G$ un subgrupo, entonces son equivalentes

(i) $H \triangleleft G$,

(ii) $aH = Ha$, $\forall a \in G$,

(iii) $aH \subseteq Ha$, $\forall a \in G$,

(iv) $aHa^{-1} = H$, $\forall a \in G$,

(v) $aHa^{-1} \subseteq H$, $\forall a \in G$.

Demostración. En primer lugar, (i) $\iff$ (ii) por definición y (ii) $\implies$ (iii) es inmediato.
Veamos que (iii) $\implies$ (v). Sea $x = aba^{-1} \in aHa^{-1}$, de modo que $b \in H$. Por (iii), sabemos que $ab = ca$, con $c \in H$; entonces, $x = aba^{-1} = caa^{-1} = c \in H$.
Veamos que (v) $\implies$ (iv). Basta provar que $\left|aHa^{-1}\right| = |H|$. Tomemos $b, c \in H$ tales que $aba^{-1} = aca^{-1}$. Se tiene que $b = c$ y sigue que $\left|aHa^{-1}\right| = |H|$.
Veamos, por último, que (iv) $\implies$ (ii). Sea $x = ab = aba^{-1}a \in aH$. Por (iv), $aba^{-1} = c \in H$, de modo que $x = ca \in Ha$ y concluimos que $aH \subseteq Ha$. Análogamente, tenemos que $Ha \subseteq aH$. □

Ejemplo 1.6.4.

1. Tomamos $G = \mathcal{S}_3 = \{\mathrm{Id}, (12), (13), (23), (123), (132)\}$ y $H = A_3 = \{\mathrm{Id}, (123), (132)\}$. Sabemos ahora que

$$|G| = |H|\left|G/H\right| \implies \frac{|G|}{|H|} = \frac{6}{3} = 2 = \left|G/H\right|.$$

   Como $\forall x \in H$, $xH = H = Hx$, H es un grupo normal, ya que solo existen 2 clases.

2. Tomamos $G = D_{2\cdot 4} = \{\mathrm{Id}, r, r^2, r^3, s, rs, r^2s, r^3s\}$ y $H = \{\mathrm{Id}, r, r^2, r^3\}$.

Proposición 1.6.5. Sea G un grupo finito y $H \subseteq G$ un subgrupo,

$$[G : H] = 2 \implies H \triangleleft G$$

Demostración. Por ser H un grupo, se tiene que $aH = H = Ha$, $\forall a \in H$. Además, como solamente hay dos clases laterales, se tiene que $aH = G \setminus H = Ha$, $\forall a \in G \setminus H$. □

Ejemplo 1.6.6. Tomamos $G = \mathcal{S}_3$ y $H = \{\mathrm{Id}, (1,2)\}$. Tenemos que

$$(1,3)H = (1,3)\{\mathrm{Id}, (1,2)\} = \{(1,3), (1,2,3)\},$$
$$H(1,3) = \{\mathrm{Id}, (1,2)\}(1,3) = \{(1,3), (1,3,2)\}.$$

Lema 1.6.7. Sean G_1, G_2 grupos, sean H, K subgrupos de G_1 y G_2 respectivamente y sea $f\colon G_1 \to G_2$ un morfismo de grupos, entonces

i) $H \triangleleft G_1 \implies f(H) \triangleleft f(G_1)$.

ii) $K \triangleleft G_2 \implies f^{-1}(K) \triangleleft G_1$.

Demostración.

i) Sea $f(x) \in f(H)$ y sea $f(a) \in f(G_1)$. Entonces,

$$f(a)f(x)f(a)^{-1} = f(a)f(x)f\left(a^{-1}\right) = f\left(axa^{-1}\right) \in f(H),$$

puesto que $axa^{-1} \in H$.

ii) Sea $x \in f^{-1}(K)$ y sea $a \in G_1$. Entonces,

$$axa^{-1} \in f^{-1}\left(f\left(axa^{-1}\right)\right) = f^{-1}\left(f(a)f(x)f(a)^{-1}\right) \subseteq f^{-1}(K),$$

puesto que $f(x) \in K$, $f(a), f^{-1}(a) \in G_2$ y $K \triangleleft G_2$.

□

Observación 1.6.8. Si G es un grupo conmutativo, entonces todo subgrupo es normal.

Observación 1.6.9. Sea G un grupo. G y $\{\mathrm{Id}\}$ son subgrupos normales.

Proposición 1.6.10. Sea G un grupo y sean $H \subseteq K \subseteq G$ subgrupos.

$$H \triangleleft G \implies H \triangleleft K.$$

Demostración. Para todo $a \in K$ y $x \in H$ se tiene que $axa^{-1} \in H$ y, por lo tanto, $H \triangleleft K$. □

Observación 1.6.11.

$$H \triangleleft K \triangleleft G \implies H \triangleleft G.$$

Ejemplo 1.6.12. Sean

$$\begin{aligned} G &= \mathcal{S}_4, \\ H &= \left\{\mathrm{Id}, (1,2)(3,4)\right\}, \\ K &= \left\{\mathrm{Id}, (1,2)(3,4), (1,3)(2,4), (2,3)(1,4)\right\}. \end{aligned}$$

Tenemos que $[K : H] = 2$, lo cual implica que $H \triangleleft K$. También es cierto que $K \triangleleft G$:

$$\sigma(1,2)(3,4)\sigma^{-1} = \sigma(1,2)\sigma^{-1}\sigma(3,4)\sigma^{-1} = (\sigma(1)\,\sigma(2))(\sigma(3)\,\sigma(4)) \in K$$

y análogamente para el resto de permutaciones de K. Sin embargo, $H \not\triangleleft G$:

$$\begin{aligned} (1,2,3)H &= \left\{(1,2,3), (1,3,4)\right\}, \\ H(1,2,3) &= \left\{(1,2,3), (2,4,3)\right\}. \end{aligned}$$

Proposición 1.6.13. Sea G un grupo, y sea $H \triangleleft G$ un subgrupo normal, entonces

i) En G/H existe una estructura de grupo definida por

$$(xH)(yH) = (xy)H.$$

ii) La función

$$\begin{aligned} \Pi\colon G &\to G/H \\ x &\mapsto xH = \bar{x} \end{aligned}$$

es un morfismo de grupos exhaustivo y de núcleo H.

iii) Existe una biyección entre

$$\begin{aligned} \{\text{sg. (normales) de } G \text{ que contienen a } H\} &\leftrightarrow \left\{\text{sg. (normales) de } G/H\right\} \\ K \supseteq H &\mapsto \Pi(K) \\ \Pi^{-1}(L) &\hookleftarrow L \end{aligned}$$

Demostración.

i) Sean $x \sim x'$ y $y \sim y'$, queremos ver que $xy \sim x'y'$.

$$\left.\begin{aligned} x \sim x' &\implies x^{-1}x' \in H \\ y \sim y' &\implies y^{-1}y' \in H \end{aligned}\right\} \implies (xy)^{-1}\left(x'y'\right) = y^{-1}\underbrace{\left(x^{-1}x'\right)}_{\in H}y' \overset{H\triangleleft G}{=} \underbrace{y^{-1}y'}_{\in H}t \in H.$$

Comprovamos las propiedades de la operación de un grupo:

- *Associativa*: $(xH)\,(yHzH) = (xH)\left((yz)\,H\right) = \left(x\,(yz)\right)H = \left((xy)\,z\right)H = (xyH)\,(zH) = \left((xH)\,(yH)\right)(zH)$.

- *Elemento neutro*:

$$H(xH) = (1H)(xH) = (1x)H = xH,$$
$$(xH)H = (xH)(1H) = (x1)H = xH.$$

- *Elemento inverso*: $(xH)\left(x^{-1}H\right) = \left(xx^{-1}\right)H = 1H = H$.

ii) Sean $x, y \in G$. Entonces, $\Pi(xy) = (xy)H = (xH)(yH) = \Pi(x)\Pi(y)$, con lo que Π es un morfismo de grupos. Ver que es un morfismo exhaustivo es inmediato, puesto que, dada una clase, cualquiera de sus respresentates la tiene por imagen. Su núcleo es $\Pi^{-1}(H)$, es decir los elementos que tienen H por imagen. Sabemos que $xH = H$, $\forall x \in H$ y que $y \notin H \implies y1 \notin H \implies \Pi(y) = yH \neq H$, de modo que $\text{Nuc}(\Pi) = H$.

iii) Demostraremos primero que Π define un morfismo biyectivo entre los subgrupos de G que contienen H y los subgrupos de G/H. Sea $K \supseteq H$ un subgrupo de G. Veamos que $\Pi(K)$ es un subgrupo de G/H.

- $H = \Pi(H) \subseteq \Pi(K)$, así que $\Pi(K)$ tiene elemento neutro.
- Sea $a \in \Pi(K)$. Entonces, $a = xH$, para algún $x \in K$, de modo que $x^{-1} \in K$ y concluimos que $x^{-1}H \in \Pi(K)$, es decir, a tiene elemento inverso en $\Pi(K)$.
- Sean $a, b \in \Pi(K)$. Entonces, $a = xH$ y $b = yH$, para algún par $x, y \in K$, de modo que $xy \in K$ y concluimos que $(xy)H \in \Pi(K)$, es decir, $\Pi(K)$ es cerrado por la operación.

Sea L un subgrupo de G/H. Veamos que $\Pi^{-1}(L)$ es un subgrupo de G que contiene H.

- $1 \in H = \Pi^{-1}(H) \subseteq \Pi^{-1}(L)$, es decir, $\Pi^{-1}(L)$ contiene a H y, por ende, tiene elemento neutro.
- $x \in \Pi^{-1}(L) \implies \Pi(x) = xH \in L \implies x^{-1}H \in L \implies x^{-1} \in \Pi^{-1}(L)$, es decir, todo elemento de $\Pi^{-1}(L)$ tiene inverso en $\Pi^{-1}(L)$.
- $x, y \in \Pi^{-1}(L) \implies \Pi(x) = xH, \Pi(y) = yH \in L \implies (xH)(yH) = (xy)H \in L \implies xy \in \Pi^{-1}(L)$, es decir, $\Pi^{-1}(L)$ es cerrado por la operación.

Para acabar, basta ver que Π restringida a los subgrupos de G que contienen H es inyectiva. Sean K_1, K_2 subgrupos de G que contienen H tales que $\Pi(K_1) = \Pi(K_2)$. Supongamos que $K_1 \neq K_2$. Sin pérdida de generalidad, $\exists x \in K_1$ tal que $x \notin K_2$. Puesto que $xH \in \Pi(K_1) = \Pi(K_2)$, necesariamente $\exists y \in K_2$ tal que $yH = xH$. Entonces, $x \in xH = yH \implies y^{-1}x \in H \subseteq K_2 \implies yy^{-1}x = x \in K_2$ e incurrimos en una contradicción. Por consiguiente, $K_1 = K_2$ y sigue que Π restringida a los subgrupos de G que contienen H es inyectiva.

Para demostrar que Π define un morfismo biyectivo entre los subgrupos normales de G que contienen H y los subgrupos normales de G/H, es suficiente comprobar que la imagen y la antiimagen de subgrupos normales (que, como ya hemos visto, son subgrupos) son normales. Sea $K \supseteq H$ un subgrupo normal de G. Veamos que

$\Pi(K) \triangleleft {}^{G}\!/_{H}$. Sea $xH \in {}^{G}\!/_{H}$. Entonces, se tiene que

$$\begin{aligned}(xH)\,\Pi(K) &= \bigcup_{yH\in\Pi(K)} \{(xH)(yH)\} = \bigcup_{y\in K} \{(xH)(yH)\} = \\ &= \bigcup_{y\in K} \{(xy)H\} = \bigcup_{y\in K}\bigcup_{z\in H} \{xyz\} = \bigcup_{z\in H}\bigcup_{y\in K} \{xyz\} = \\ &= \bigcup_{z\in H} \{(xK)z\} = \bigcup_{z\in H} \{(Kx)z\} = \bigcup_{z\in H}\bigcup_{y\in K} \{yxz\} = \\ &= \bigcup_{y\in K}\bigcup_{z\in H} \{yxz\} = \bigcup_{y\in K} \{(yx)H\} = \bigcup_{y\in K} \{(yH)(xH)\} = \\ &= \bigcup_{yH\in\Pi(K)} \{(yH)(xH)\} = \Pi(K)(xH),\end{aligned}$$

de modo que $\Pi(K)$ es un subgrupo normal de ${}^{G}\!/_{H}$. Por otro lado, sea L un subgrupo normal de ${}^{G}\!/_{H}$. Veamos que $\Pi^{-1}(L) \triangleleft G$. Sea $x \in G$. Se tiene que $x\Pi^{-1}(L)\,x^{-1}$ es un grupo, de lo que sigue

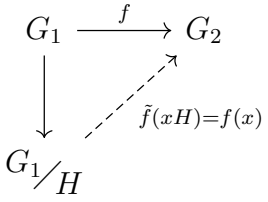
$$\begin{aligned}x\Pi^{-1}(L)\,x^{-1} &= \Pi^{-1}\left(\Pi\left(x\Pi^{-1}(L)\,x^{-1}\right)\right) = \\ &= \Pi^{-1}\left((xH)\,L\left(x^{-1}H\right)\right) = \\ &= \Pi^{-1}\left((xH)\left(x^{-1}H\right)L\right) = \\ &= \Pi^{-1}(HL) = \\ &= \Pi^{-1}(L).\end{aligned}$$

Así pues, $\Pi^{-1}(L)$ es un subgrupo normal de G y hemos terminado.

□

Teorema 1.6.14. *Primer teorema de isomorfía.*
Sean G_1, G_2 grupos, sea $f\colon G_1 \to G_2$ un morfismo de grupos. Sea $H \triangleleft G_1$ un subgrupo normal. Definimos

$$\begin{aligned}\tilde{f}\colon {}^{G_1}\!/_{H} &\to G_2 \\ xH &\mapsto \tilde{f}(xH) = f(x).\end{aligned}$$



Entonces,

i) $\tilde{f}$ está bien definida $\iff H \subseteq \ker(f)$.

Si $\tilde{f}$ está bien definida, se cumple que

ii) $\tilde{f}$ es un morfismo de grupos,

iii) $xH \in \ker\left(\tilde{f}\right) \iff x \in \ker(f)$,

iv) $\operatorname{Im}\left(\tilde{f}\right) = \operatorname{Im}(f)$.

Demostración.

i)

$$\begin{aligned}
\tilde{f} \text{ está bien definida} &\iff \left(xH = yH \implies f(x) = f(y)\right) \iff \\
&\iff \left(x^{-1}y \in H \implies f(x) = f(y)\right) \iff \\
&\iff \left(x^{-1}y \in H \implies f(x) f^{-1}(y) = 1\right) \iff \\
&\iff \left(x^{-1}y \in H \implies f(x) f\left(y^{-1}\right) = 1\right) \iff \\
&\iff \left(x^{-1}y \in H \implies f\left(xy^{-1}\right) = 1\right) \iff \\
&\iff H \subseteq \ker(f).
\end{aligned}$$

ii) $\tilde{f}(xH)\,\tilde{f}(yH) = f(x) f(y) = f(xy) = \tilde{f}\left((xy)H\right)$.

iii) $xH \in \ker\left(\tilde{f}\right) \iff \tilde{f}(xH) = f(x) = 1 \iff x \in \ker(f)$.

iv) $\operatorname{Im}\left(\tilde{f}\right) = \left\{\tilde{f}(xH) \mid x \in G_1\right\} = \left\{f(x) \mid x \in G_1\right\} = \operatorname{Im}(f)$.

□

Corolario 1.6.15. En particular $\tilde{f}\colon {}^{G_1}\!/_{\ker(f)} \to f(G_1)$ es un morfismo de grupos biyectivo (isomorfismo).

Corolario 1.6.16. Hay un único grupo cíclico de orden n (salvo isomorfismos).

Demostración. Sea $G = C_n(x) = \left\{1, x, \ldots, x^{n-1}\right\} = \langle x \rangle$, tomamos

$$\begin{aligned} f\colon \mathbb{Z} &\to C_n(x) \\ k &\mapsto x^k \end{aligned}$$

que es un morfismo de grupos exhaustivo, $\ker(f) = n\mathbb{Z}$. Por el primer teorema de isomorfía (1.6.14),

$${}^{\mathbb{Z}}\!/_{\mathbb{Z}_n} \cong C_n.$$

□

1.7. El grupo multiplicativo de un cuerpo finito

Observación 1.7.1. *Notación.* Sea G un grupo finito con $\mathrm{o}(G) = n$ y $d|n$, notaremos

$$\mathcal{O}_d = \left\{y \in G \mid \mathrm{o}(y) = d\right\}.$$

Sea $x \in G$ con $\mathrm{o}(x) = m$, notaremos

$$C_m(x) = \langle x \rangle = \left\{1, x, \ldots, x^{m-1}\right\}$$

Observación 1.7.2. *Notación.* Dado un cuerpo $\Bbbk$, notaremos $\Bbbk^* = \Bbbk \setminus \{0\}$.

Lema 1.7.3. Sea $\Bbbk$ un cuerpo y sea $p(T) \in \Bbbk[T]$ un polinomio de grado n. Entonces,

$$\left|\{\text{raíces de } p(T)\}\right| \leq n.$$

Demostración. Pongamos $p\,(T) = a_n T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0$. Entonces, si t es una raíz de p o, dicho de otro modo, $p\,(t) = 0$, se tiene que

$$p\,(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 = 0,$$

de modo que

$$\begin{aligned} p\,(T) &= p\,(T) - p\,(t) = \\ &= a_n T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0 - a_n t^n - a_{n-1}t^{n-1} - \cdots - a_1 t - a_0 = \\ &= (T-t)\left[a_n\left(T^{n-1} + T^{n-2}t + \cdots + Tt^{n-2} + t^{n-1}\right) + \cdots + a_1\right] = \\ &= (T-t)\,q\,(T)\,, \end{aligned}$$

donde $q\,(T)$ es un polinomio de grado $n-1$. Así pues, las demás raíces de $p\,(T)$ dividen $q\,(T)$ y así sucesivamente. Entonces, si $p\,(T)$ tubiera más de n raíces, sería de la forma $(T-t_1)\cdots(T-t_{n+1})\,q\,(T)$ y tendría, almenos, grado $n+1$, lo cual supone una contradicción. □

Lema 1.7.4. Sea $\Bbbk$ un cuerpo y sea $x \in \Bbbk^*$, $\mathrm{o}(x) = n$. Entonces,

$$\mathcal{O}_n\,(\Bbbk^*) \subseteq \{\text{raíces de } T^n - 1\} = C_n(x) \subseteq \Bbbk^*.$$

Además, $\left|\mathcal{O}_n\,(\Bbbk^*)\right| = \varphi(n)$.

Demostración. Sea $y \in \mathcal{O}_n(\Bbbk^*)$. Se tiene que $y^n = 1 \implies y^n - 1 = 0 \implies y$ es raíz de $T^n - 1$, y tenemos la primera inclusión $\mathcal{O}_n\,(\Bbbk^*) \subseteq \{\text{raíces de } T^n - 1\}$.
Ahora, veamos que $\{\text{raíces de } T^n - 1\} = C_n(x)$. Por un lado,

$$y \in C_n(x) \implies y = x^k \implies y^n = \left(x^k\right)^n = (x^n)^k = 1,$$

con lo que $C_n(X) \subseteq \{\text{raíces de } T^n - 1\}$. Por otro lado,

$$\left|\{\text{raíces de } T^n - 1\}\right| \leq n = \left|C_n\,(x)\right|,$$

y concluimos que $\{\text{raíces de } T^n - 1\} = C_n(x)$.
El último resultado sigue inmediatamente de la inclusión $\mathcal{O}_n\,(\Bbbk^*) \subseteq C_n\,(x)$ y de la proposición 1.3.11. □

Teorema 1.7.5. Sea $\Bbbk$ un cuerpo y sea G un subgrupo finito de $\Bbbk^*$. Entonces, G es un grupo cíclico. En particular, si $\Bbbk$ es finito, $\Bbbk^*$ es un grupo cíclico.

Demostración. Sea $|G| = n$ y sea $d|n$. Tenemos que

$$\mathcal{O}_d(G) = \{y \in G \mid \mathrm{o}(y) = d\} \subseteq \{y \in \Bbbk^* \mid \mathrm{o}(y) = d\} = \mathcal{O}_d(\Bbbk^*).$$

Definimos $m_d = |\mathcal{O}_d(G)| \leq |\mathcal{O}_d(\Bbbk^*)| \leq \varphi(d)$. Entonces,

$$n = \sum_{d|n} m_d \leq \sum_{d|n} \varphi(d) = n \implies m_d = \varphi(d).$$

Tomamos ahora $d = n$, se tiene que

$$\left.\begin{array}{l} m_n = \varphi(n) \geq 1 \implies \exists y \in G \text{ t. q. } \mathrm{o}(y) = n \\ |G| = n \end{array}\right\} \implies G = C_n(y).$$

□

1.8. Grupos simples

Definición 1.8.1. Sea G un grupo no trivial ($G \neq \{1\}$). Decimos que G es simple si los únicos subgrupos normales de G son $\{1\}$ y G.

Teorema 1.8.2. Sea G un grupo. Son equivalentes

(i) G es simple y abeliano,

(ii) $|G| = p$, con p primo,

(iii) $G \cong \mathbb{Z}/p\mathbb{Z}$ con p primo.

Demostración. Empecemos probando que (i) $\implies$ (ii). Como $G \neq \{1\}$, $\exists x \in G$ con $x \neq 1$. Veamos que $\mathrm{o}(x) = \infty \implies \langle x^2 \rangle \subsetneq G$. Supongamos que $\mathrm{o}(x) = \infty$. Entonces, $\langle x^2 \rangle = G \implies x \in \langle x^2 \rangle \implies x = \left(x^2\right)^n = x^{2n} \implies x^{-1}x = x^{-1}x^{2n} \implies 1 = x^{2n-1} \implies \mathrm{o}(x) \leq 2n - 1$ lo cual contradice la hipótesis $\mathrm{o}(x) = \infty$. Tenemos ahora que $\langle x^2 \rangle$ es subgrupo propio de G. Pero G es abeliano y, por lo tanto, $\langle x^2 \rangle \triangleleft G$, cosa que supone una contradicción con la hipótesis de que G es simple. Así pues, $\mathrm{o}(x) = n > 1$. Tomamos $p|n$, con p primo. Sabemos que

$$\mathrm{o}\left(x^{\frac{n}{p}}\right) = \frac{n}{\mathrm{mcd}\left(n, \frac{n}{p}\right)} = \frac{n}{\frac{n}{p}} = p.$$

Es decir, $x^{\frac{n}{p}}$ tiene orden p. Tomamos $H = \langle x^{\frac{n}{p}} \rangle \neq \{1\}$. H es un subgrupo de G y G es abeliano, de modo que $H \triangleleft G$. Sin embargo, G es simple, con lo cual $H = G$ y concluimos que $|G| = |H| = p$.

Veamos ahora que (ii) $\implies$ (iii). Suponemos que $|G| = p$ con p primo, y sigue que $\exists x \in G$, $x \neq 1$. En particular $\mathrm{o}(x) | \mathrm{o}(G) = p$ y, puesto que p es primo, $\mathrm{o}(x) = p$. Ahora se tiene que $\langle x \rangle \subseteq G$, pero los órdenes de los grupos son iguales y, por consiguiente,

$G = \langle x \rangle \cong \mathbb{Z}/p\mathbb{Z}$.

Por último, veamos que (iii) $\Longrightarrow$ (i). $G \cong \mathbb{Z}/p\mathbb{Z}$ es el grupo cíclico de p elementos y es abeliano. Además, vimos que los siguientes conjuntos están en biyección:

$$\left\{ d \in \mathbb{Z} \;\middle|\; d|n,\ 1 \leq d \leq n \right\} \leftrightarrow \left\{ H \mid H \text{ sg. de } G, |H| = d \right\}$$
$$d \mapsto \langle y^{\frac{n}{d}} \rangle.$$

Como n es primo, los únicos subgrupos de G son $\{1\}$ y G y, en particular, son los únicos normales. Concluimos que G es simple. □

Teorema 1.8.3. *Teorema de Feit-Thompson.*
Sea G un grupo simple tal que $|G| = n \in \mathbb{N}$, con n non. Entonces, n es un número primo.

Demostración. La demostración es demasiado larga y complicada como para abarcarla en esta asignatura. □

Corolario 1.8.4. Sea G un grupo simple tal que $|G| = n \in \mathbb{N}$, con n non. Se tiene que

$$G \equiv \mathbb{Z}/p\mathbb{Z},$$

con $p = n$ primo.

Demostración. El resultado es una consecuencia inmediata de los teoremas 1.8.3 y 1.8.2. □

Teorema 1.8.5. Sea $n \geq 5$, entonces A_n es simple.

Demostración. Sabemos (por problemas) que $A_n = \langle 3\text{-ciclos} \rangle$. Sean ahora (a_1, a_2, a_3) y (b_1, b_2, b_3) dos 3-ciclos, veremos que $\exists \sigma \in A_n$ tal que $\sigma\,(a_1, a_2, a_3)\,\sigma^{-1} = (b_1, b_2, b_3)$. Tomamos σ la permutación que envía a_1 a b_1, a_2 a b_2, a_3 a b_3 y el resto a donde sea. Si $\sigma \in A_n$ ya hemos acabado. Si $\sigma \notin A_n$, tomamos

$$\tilde{\sigma} = \sigma\,(a_4, a_5)$$

con todos los a_i diferentes entre ellos (a_4 y a_5 existen porque $n \geq 5$). Entonces se tiene que

$$\begin{aligned} \tilde{\sigma}\,(a_1, a_2, a_3)\,\tilde{\sigma}^{-1} &= \sigma\,(a_4, a_5)\,(a_1, a_2, a_3)\,(a_4, a_5)\,\sigma^{-1} \\ &= \sigma\,(a_1, a_2, a_3)\,\cancel{(a_4, a_5)}\cancel{(a_4, a_5)}\sigma^{-1} \\ &= \sigma\,(a_1, a_2, a_3)\,\sigma^{-1} = (b_1, b_2, b_3) \end{aligned}$$

y $\tilde{\sigma} \in A_n$. Tomamos $H \triangleleft A_n$, con H no trivial. Veamos que H contiene un 3-ciclo. Tomamos $\sigma \in H$, con $\sigma \neq \mathrm{Id}$. Por el ejercicio 20 se tiene que o bien

$$\exists \tau \in A_n \text{ t. q. } \tau\sigma\tau^{-1}\sigma^{-1} \text{ es un 3-ciclo,}$$

o bien

$$\exists \tau_1\tau_2 \in A_n \text{ t. q. } \tau_2\tau_1\sigma\tau_1^{-1}\sigma^{-1}\tau_2^{-1}\sigma\tau_1\sigma^{-1}\tau_1^{-1} \text{ es un 3-ciclo.}$$

Ahora queremos ver que $H = A_n$. Acabamos de ver que $\exists \sigma \in H$ 3-ciclo y que todo τ 3-ciclo es el conjugado de σ por un elemento $\rho \in A_n$. Por lo tanto, $\tau \in H$, lo que nos dice que $A_n = \langle \text{3-ciclos} \rangle \subseteq H$ y hemos acabado. □

Lema 1.8.6. Sea G un grupo no trivial y sea H un subgrupo normal a G. Entonces, G/H es simple si y solo si H es un elemeno maximal del conjunto $\{K \mid K \triangleleft G, K \neq G, H \subseteq K\}$.

Demostración. Como establece la proposición 1.6.13, existe una biyección entre los subgrupos normales de G/H y los subgrupos normales de G que contien H. Por definición, G/H es simple si y solo su tiene exactamente dos subgrupos normales. Así, si G/H es simple, $H \neq G$ y hay exactamente dos subgrupos normales de G: H y G. Entonces, H es el elemento maximal de los subgrupos propios de G que contienen H. Recíprocamente, si H es un elemeno maximal del conjunto $\{K \mid K \triangleleft G, K \neq G, H \subseteq K\}$, entonces $\{K \mid K \triangleleft G, H \subseteq K\} = \{K \mid K \triangleleft G, K \neq G, H \subseteq K\} \cup \{G\} = \{H, G\}$. Por consiguiente, G/H tiene exactamente dos subgrupos normales, es decir, es simple. □

Definición 1.8.7. Sea G un grupo. Llamamos torre normal de G a una cadena de subgrupos de G tal que

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\},$$

es decir, que G_i es un subgrupo normal de G_{i+1}. Decimos que los grupos

$$G_0/G_1, G_1/G_2, \ldots, G_{n-1}/G_n$$

son los cocientes de la torre y que la longitud de la torre es n.

Definición 1.8.8. Sea G un grupo. Decimos que una torre normal de G es una torre normal abeliana de G si todos los grupos

$$G_0/G_1, G_1/G_2, \ldots, G_{n-1}/G_n$$

son abelianos.

Definición 1.8.9. Sea G un grupo. Decimos que es resoluble si tiene una torre normal abeliana.

Definición 1.8.10. Sea G un grupo. Decimos que una torre normal de G es una serie de composición de G si todos los grupos

$$G_0/G_1, G_1/G_2, \ldots, G_{n-1}/G_n$$

son simples.

Ejemplo 1.8.11.

1. Todo grupo tiene, almenos, una torre normal. En particular, $G = G_0 \triangleright G_1 = \{1\}$ es una torre normal. Además, es una torre abeliana si y solo si G es abeliano, y es simple si y solo si G es simple. Así pues, si G es abeliano, es resoluble porque $G \triangleright \{1\}$ es una torre normal abeliana.

2. Consideremos $G = D_{2n}$. Se tiene que $D_{2n} \triangleright \langle r \rangle \triangleright \{1\}$ es una torre normal. Veamos que es abeliana.
$$\langle r \rangle / \{1\} = \langle r \rangle \cong \mathbb{Z}/n\mathbb{Z},$$
que es abeliano, y
$$D_{2n}/\langle r \rangle \cong C_2,$$
que es abeliano. Por lo tanto, D_{2n} es resoluble. Además, puesto que C_2 es simple, $D_{2n} \triangleright \langle r \rangle \triangleright \{1\}$ es una serie de composición si y solo si n es primo.

3. Consideremos $G = \mathcal{S}_4$. Se tiene que $\mathcal{S}_4 \triangleright V_4 = \left\{\mathrm{Id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\right\} \triangleright \{\mathrm{Id}\}$ es una torre normal. Para ver que $\mathcal{S}_4 \triangleright V_4$, observamos que $\sigma(a,b)(c,d)\sigma^{-1} = \sigma(a,b)\sigma^{-1}\sigma(c,d)\sigma^{-1} = \left(\sigma(a)\sigma(b)\right)\left(\sigma(c)\sigma(d)\right) \in V_4$. Veamos que G_4/V_4 no conmuta.
$$\begin{aligned}(1,2,3)V_4(1,4)V_4 &= (1,2,3)(1,4)V_4 = \\ &= (1,4,2,3)V_4 \neq \\ &\neq (1,2,3,4)V_4 = \\ &= (1,4)(1,2,3)V_4 = \\ &= (1,4)V_4(1,2,3)V_4.\end{aligned}$$
Así pues, la torre no es abeliana y no es una serie de composición porque V_4 no es simple.

4. Podemos refinar la torre anterior para que sea abeliana y serie de composición. Consideremos la torre
$$\mathcal{S}_4 \triangleright A_4 \triangleright V_4 \triangleright \left\{\mathrm{Id}, (1,2)\right\} \triangleright \{\mathrm{Id}\}.$$
Veamos que efectivamente es una torre. $\mathcal{S}_4 \triangleright A_4$ porque A_4 es un subgrupo y $[\mathcal{S}_4 : A_4] = 2$. $A_4 \triangleright V_4$ porque $\mathcal{S}_4 \triangleright V_4$. $V_4 \triangleright \left\{\mathrm{Id}, (1,2)\right\}$ porque $\left\{\mathrm{Id}, (1,2)\right\}$ es un subgrupo y $\left[V_4 : \left\{\mathrm{Id}, (1,2)\right\}\right] = 2$.
Veamos ahora que cada uno de los cocientes de la torre son simples y conmutativos.
$$\begin{aligned}\mathcal{S}_4/A_4 &\cong \mathbb{Z}/2\mathbb{Z}, \\ A_4/V_4 &\cong \mathbb{Z}/3\mathbb{Z}, \\ V_4/\left\{\mathrm{Id}, (1,2)\right\} &\cong \mathbb{Z}/2\mathbb{Z}, \\ \left\{\mathrm{Id}, (1,2)\right\}/\{\mathrm{Id}\} &\cong \mathbb{Z}/2\mathbb{Z},\end{aligned}$$
que son todos simples y conmutativos.

5. $\mathbb{Z}$ no tiene serie de composición. En primer lugar, observamos que $\mathbb{Z}$ no es simple porque $2\mathbb{Z} \triangleleft \mathbb{Z}$. Sea G un subgrupo de $\mathbb{Z}$ (en particular, será un subgrupo normal porque $\mathbb{Z}$ es conmutativo). El máximo común divisor m de todos los elementos de G es un elemento de G porque de obtiene sumando (finitos) elementos de G. Entonces, $G = \langle m \rangle = m\mathbb{Z} \cong \mathbb{Z}$, y deducimos que todos los elementos de cualquier torre normal de $\mathbb{Z}$ serán de la forma $n\mathbb{Z}$. Pero ${}^{n\mathbb{Z}}\!/_{0} = n\mathbb{Z} \cong \mathbb{Z}$ no es simple, de manera que siempre habrá un cociente de la torre que no es simple. Por lo tanto, $\mathbb{Z}$ no tiene serie de composición.

Proposición 1.8.12. Todo grupo finito tiene una serie de composición.

Demostración. Sea G un grupo finito y supongamos que no tiene serie de composición. De entre sus torres normales (el primer ejemplo nos muestra que hay, almenos, una) tomemos una que no pueda ser refinada, es decir, que para todo par de grupos consecutivos G_i y G_{i+1} de la torre, no exista un grupo H (distinto de G_i y G_{i+1}) con $G_i \triangleright H \triangleright G_{i+1}$. Sabemos que una tal torre normal existe porque, de no ser así, podríamos encontrar una torre normal con un número arbitrario de grupos de distinto cardinal, lo cual supondría una contradicción con la finitud de G. Entonces, la torre en cuestión tiene un par de grupos consecutivos G_k y G_{k+1} tales que ${}^{G_k}\!/_{G_{k+1}}$ no es simple ya que, de lo contrario, seria una serie de composición. Sin embargo, el lema 1.8.6 nos asegura que G_{k+1} no es un elemento maximal del conjunto de grupos $\{H \mid H \triangleleft G_k, H \neq G_k, G_{k+1} \subseteq H\}$. Por lo tanto, existe un grupo H (distinto de G_k y G_{k+1}) con $G_k \triangleright H \supseteq G_{k+1}$. Pero $G_k \triangleright G_{k+1}$, y necesariamente $H \triangleright G_{k+1}$. Esto contradice la suposición de que no existía un tal H y concluimos que G tiene serie de composición. □

Teorema 1.8.13. *Segundo teorema de isomorfía.*
Sea G un grupo y sean H, K subgrupos de G con $H \triangleleft G$. Entonces,

i) $(H \cap K) \triangleleft K$,

ii) HK es un subgrupo de G,

iii) $H \triangleleft HK$.

Además, se tiene que

$$ {}^{K}\!/_{H \cap K} \cong {}^{HK}\!/_{H}. $$

Demostración.

i) Sean $x \in H \cap K$, $a \in K$. Entonces, $axa^{-1} \in K$ trivialmente. Además, puesto que $H \triangleleft G$ y $a \in K \subseteq G$, $axa^{-1} \in H$. Así pues, $axa^{-1} \in H \cap K$ y $(H \cap K) \triangleleft K$.

ii) Naturalmente, $HK \subseteq G$. Veamos que HK es un grupo. $1 \in H, K \implies 1 \in HK$. Sean $h_1, h_2 \in H$ y sean $k_1, k_2 \in K$. Entonces, como que $H \triangleleft G \implies aH = Ha$, $h_1k_1h_2k_2 = h_1h_3k_1k_2$, para algún $h_3 \in H$. Por ser H y K grupos, $h_1k_1h_2k_2 = h_1h_3k_1k_2 \in HK$. Finalmente, sea $hk \in HK$. Entonces, $(hk)^{-1} = k^{-1}h^{-1} \in k^{-1}H = Hk^{-1}$. Así pues, existe $\overline{h} \in H$ tal que $(hk)^{-1} = \overline{h}k^{-1} \in HK$.

iii) Sea $a \in H$ y sea $hk \in HK$. Entonces, $hka\,(hk)^{-1} = hkak^{-1}h^{-1}$. Puesto que $H \triangleleft G$, $kak^{-1} = \overline{a} \in H$ y concluimos que $hka\,(hk)^{-1} = hkak^{-1}h^{-1} = h\overline{a}h^{-1} \in H$, de modo que $H \triangleleft HK$.

Sea $\varphi\colon K \overset{i}{\hookrightarrow} HK \overset{\pi}{\to} {}^{HK}\!/_{H}$. El cociente ${}^{HK}\!/_{H}$ es un grupo porque HK es un grupo y $H \triangleleft HK$. La composición de morfismos de grupos es un morfismo de grupos, de manera que φ es un morfismo de grupos.

Veamos que φ es exhaustivo. Sea $\overline{hk} = hkH \in {}^{HK}\!/_{H}$ la clase de $hk \in HK$. Por ser H un subgrupo normal de G, existe algún $h' \in H$ tal que $hk = kh'$. Entonces, $\overline{hk} = hkH = kh'H = kH = \overline{k}$. Así pues, $\overline{hk} = \overline{k} = \varphi(k)$, $\forall \overline{hk} \in {}^{HK}\!/_{H}$, y concluimos que φ es exhaustivo.

Veamos que $\ker(\varphi) = H \cap K$. Sea $k \in \ker(\varphi)$, es decir, $k \in K$ tal que $\varphi(k) = \overline{1} = H$. Entonces, $\varphi(k) = \overline{k} = kH = H$, lo cual implica que $k \in H$, de modo que $k \in H \cap K$ y sigue que $\ker(\varphi) \subseteq H \cap K$. Sea ahora $k \in H \cap K$. Puesto que $k \in K$, k es del dominio de φ y tenemos que $\varphi(k) = \overline{k} = kH = H = \overline{1}$, por ser k de H. Finalmente, $\ker(\varphi) \supseteq H \cap K$ y se da la igualdad.

Para terminar, ${}^{K}\!/_{H \cap K}$ es un grupo porque $(H \cap K) \triangleleft K$ y podemos aplicar el primer teorema de isomorfía para deducir que

$$ {}^{K}\!/_{H \cap K} \cong {}^{K}\!/_{\ker(\varphi)} \cong {}^{HK}\!/_{H}. $$

□

Teorema 1.8.14. *Teorema de Jordan-Hölder.*
Sea G un grupo y sean

$$ G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}, $$
$$ G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_m = \{1\} $$

dos series de composición de G. Entonces $n = m$ y $\exists \sigma \in \mathcal{S}_n$ tal que

$$ {}^{H_{i-1}}\!/_{H_i} \cong {}^{G_{\sigma(i)-1}}\!/_{G_{\sigma(i)}},\ \forall 1 \leq i \leq n. \tag{1.1} $$

Demostración. Aunque el teorema es cierto para cualquier grupo, realizaremos la demostración para grupos finitos solamente, por inducción sobre $|G|$. Para simplificar la notación, diremos que dos series de composición son equivalentes si satisfacen 1.1.

Sea G un grupo finito y sean $\{G_i\}_{i=0,\ldots,n}$ y $\{H_i\}_{i=0,\ldots,m}$ series de composición de G.

La hipóteis de inducción dice que si H es un grupo con $|H| < |G|$, entonces dos series de composición cualesquiera de H son equivalentes.

Si $H_1 = G_1$ entonces $|G_1| = |H_1| < |G|$, ya que ${}^{G_0}\!/_{G_1}$ es simple. Tenemos entonces que $n - 1 = m - 1$ y las series de composición $\{G_i\}_{i=1,\ldots,n}$ y $\{H_i\}_{i=1,\ldots,n}$ son equivalentes. Por lo tanto, $n = m$ y las series de composición completas son equivalentes.

Consideremos ahora el caso $H_1 \neq G_1$. Sabemos que $G_1, H_1 \triangleleft G$, lo que implica que $G_1H_1 \triangleleft G$. Como ${}^{G}\!/_{G_1}$ es simple y $H_1G_1 \supset G_1$, se tiene que $G_1H_1 = G$. Definamos el grupo $K_2 = H_1 \cap G_1$ y veamos que $K_2 \triangleleft H_1$. Sea $x \in K_2$ y sea $a \in H_1$, entonces

$$ x \in G_1, a \in H_1 \subset G \overset{G_1 \triangleleft G}{\Longrightarrow} axa^{-1} \in G_1. $$

Además, claramente $axa^{-1} \in H_1$, de modo que $K_2 \triangleleft H_1$. Análogamente, se demuestra que $K_2 \triangleleft G_1$. Por el segundo teorema del isomorfismo (1.8.13), tenemos que

$$ {}^{G_1}\!/_{K_2} = {}^{G_1}\!/_{H_1 \cap G_1} \cong {}^{G_1H_1}\!/_{H_1} = {}^{G}\!/_{H_1}. $$

Por el mismo razonamiento, $H_1/K_2 \cong G/G_1$. Por ser serie de composición, K_2 tiene serie de composición $K_2 \triangleright K_3 \triangleright \cdots \triangleright K_p = \{1\}$. Hasta ahora tenemos las series

$$G_1 \triangleright K_2 \triangleright \cdots \triangleright K_p = \{1\}, \qquad G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{1\},$$
$$H_1 \triangleright K_2 \triangleright \cdots \triangleright K_p = \{1\}, \qquad H_1 \triangleright H_2 \triangleright \cdots \triangleright H_m = \{1\}.$$

Puesto que $|G_1| < |G| \implies$, podemos afirmar que, en virtud de la hipótesis de inducción, $n - 1 = p - 1$ y que la series de composición

$$G_1 \triangleright K_2 \triangleright \cdots \triangleright K_p = \{1\},$$
$$G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{1\}$$

son equivalentes. Análogamente,

$$H_1 \triangleright K_2 \triangleright \cdots \triangleright K_p = \{1\},$$
$$H_1 \triangleright H_2 \triangleright \cdots \triangleright H_m = \{1\}$$

también son series de composición equivalentes. En particular, $n = m$. Recordemos las series de composición originales

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\},$$
$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n = \{1\}.$$

Debido a que $G_1/K_2 \cong G/H_1$ y que $H_1/K_2 \cong G/G_1$, concluimos que las dos series de composición de G son equivalentes. □

Proposición 1.8.15. Sea G un gupo y H un subgrupo. Entonces,

i) Si G es resoluble, H es resoluble.

ii) Si $H \triangleleft G$ y G es resoluble, G/H es resoluble.

iii) Si $H \triangleleft G$ y H, G/H son resolubles, G es resoluble.

Demostración. Ejercicio. □

1.9. Acción de un grupo sobre un conjunto

Definición 1.9.1. Sea X un conjunto y G un grupo. Llamamos acción de G en X a una aplicación

$$G \times X \to X$$
$$(a, x) \mapsto ax$$

que verifica

i) $a(bx) = (ab)x$, $\forall a, b \in G$, $\forall x \in X$,

ii) $1x = x$.

Decimos que G opera en X o bien que X es un G-conjunto.

Observación 1.9.2. Una acción de G en X define, $\forall a \in G$, una aplicación

$$\begin{aligned} m_a \colon X &\to X \\ x &\mapsto m_a(x) = ax. \end{aligned}$$

Además, m_a es biyectiva y tenemos $(m_a)^{-1} = m_{a^{-1}}$ ya que $a^{-1}(ax) = \left(a^{-1}a\right) x = 1x = x$.

Es decir, una acción de G en X, nos define una aplicación

$$\begin{aligned} G &\to \mathrm{Perm}(X) = \left\{ f \colon X \to X \mid f \text{ biyectiva} \right\} \\ a &\mapsto m_a. \end{aligned}$$

Esta aplicación es un morfismo de grupos, ya que

$$m_a m_b\,(x) = abx = m_{ab}\,(x)\,,\ \forall x \in X.$$

Recíprocamente, sea $f \colon G \to \mathrm{Perm}(X)$ un morfismo de grupos. Podemos definir una acción

$$\begin{aligned} \tilde{f} \colon G \times X &\to X \\ (a, x) &\mapsto \tilde{f}(a, x) = f(a)(x), \end{aligned}$$

que está bien definida porque

i) $a(bx) = f(a)\left(f(b)(x)\right) = \left(f(a)f(b)\right)(x) = f(ab)(x) = (ab)x$,

ii) $1x = f(1)x = \mathrm{Id}(x) = x$.

Por lo tanto, podremos afirmar que existe una biyección

$$\{\text{acciones } G \times X \to X\} \leftrightarrow \left\{\text{morfismo de grupos } G \to \mathrm{Perm}(X)\right\}$$

si demostramos que es una inyección en alguna de las direcciones.

Definición 1.9.3. Sea G un grupo y X un G-conjunto. Llamamos órbita de $x \in X$ a

$$Gx = \left\{ ax \mid a \in G \right\} \subseteq X.$$

Proposición 1.9.4. Sean $x, y \in X$. La relación $x \sim y \iff \exists a \in G$ tal que $y = ax$ es una relación de equivalencia.

Observación 1.9.5. Si tenemos la relación de equivalencia anterior, entonces

$$\bar{x} = \left\{ y \in X \mid x \sim y \right\} = \left\{ y \in X \mid \exists a \in G \text{ t. q. } y = ax \right\} = \left\{ ax \mid a \in G \right\} = Gx,$$

que es la órbita de x. El conjunto de órbitas se escribe como $G \setminus X$ ó $X/\sim$.

Definición 1.9.6. Sea G un grupo y X un G-conjunto. Llamamos estabilizador de $x \in X$ o grupo de isotopía de x a

$$G_x = \left\{ a \in G \mid ax = x \right\} \subseteq G.$$

Proposición 1.9.7. G_x es un subgrupo.

Demostración. Veamos las tres propiedades de la definición 1.1.4.

i) $1x = x \implies 1 \in G_x$.

ii) Sean $a, b \in G$ tales que $ax = x$, $bx = x$. Entonces, $(ab)x = a(bx) = ax = x$ y por lo tanto $ab \in G_x$.

iii) Sea $a \in G$ tal que $ax = x$. Entonces, $x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}x$ y por lo tanto $a^{-1} \in G_x$.

□

Lema 1.9.8. Sea G un grupo y X un G-conjunto. Sean $x, y \in X$, si $x \sim y$, entonces G_x y G_y son subgrupos conjugados.

Demostración. $x \sim y \implies y = ax$ para algún $a \in G$. Veremos que $G_y = aG_xa^{-1}$.
Veamos que $G_y \subseteq aG_xa^{-1}$. Sea $\alpha \in G_y$

$$\begin{aligned}
\alpha \in G_y &\implies \alpha y = y \implies \\
&\implies \alpha ax = ax \implies \\
&\implies \left(a^{-1}\alpha a\right) x = x \implies \\
&\implies a^{-1}\alpha a \in G_x \implies \\
&\implies \alpha a \in aG_x \implies \\
&\implies \alpha \in aG_xa^{-1}.
\end{aligned}$$

La otra inclusión resta como ejercicio. □

Proposición 1.9.9. Sea G un grupo y X un G-conjunto. Entonces, $\forall x \in X$, tenemos que

$$\begin{aligned}
Gx &\to {}^{G}\!/_{G_x} \\
ax &\mapsto aG_x
\end{aligned}$$

es una aplicación bien definida y biyectiva. En particular,

i) $|Gx| = \left|{}^{G}\!/_{G_x}\right| = [G : G_x] = \frac{|G|}{|G_x|}$. Es decir, $|G_x||Gx| = |G|$.

ii) Si X es finito, entonces $X = \bigsqcup_{i=1}^{r} Gx_i$ y, por consiguiente,

$$|X| = \sum_{i=1}^{r} |Gx_i| = \sum_{i=1}^{r} \left[G : G_{x_i}\right],$$

que es lo que conocemos como fórmula de órbitas.

iii)

Demostración. Veamos que si $ax = bx$, entonces $aG_x = bG_x$. En efecto,

$$ax = bx \implies b^{-1}ax = x \implies b^{-1}a \in G_x \implies aG_x = bG_x.$$

Veamos ahora que la aplicación es inyectiva. Supongamos que $aG_x = bG_x$, entones

$$aG_x = bG_x \implies b^{-1}a \in G_x \implies b^{-1}ax = x \implies ax = bx.$$

La aplicación es evidentemente exhaustiva por construcción. El punto i) es una consecuencia inmediata del teorema de Lagrange (1.5.7) y el punto ii) sigue del i).

□

Definición 1.9.10. Sea G un grupo y X un G-conjunto. Diremos que $x \in X$ es un punto fijo si

$$ax = x \quad \forall a \in G.$$

Observación 1.9.11. x es un punto fijo $\iff Gx = \{x\} \iff G_x = G$.

Definición 1.9.12. Sea G un grupo, X un conjunto y $G \times X \to X$ una acción de G en X. Diremos que esta acción es transitiva si, $\forall x, y \in X$, se tiene que $x \sim y$.

Observación 1.9.13. Una acción es transitiva si y solo si $X = Gx$, $\forall x \in X$, es decir, si hay una sola órbita.

Definición 1.9.14. Sea G un grupo, X un conjunto y $G \times X \to X$ una acción de G sobre X. Diremos que esta acción es fiel si $\forall a, b \in G$ tales que $a \neq b$, se tiene que $m_a \neq m_b$, es decir,

$$G \to \mathrm{Perm}(X)$$
$$a \mapsto m_a$$

es un morfismo inyectivo de grupos.

Definición 1.9.15. Sea G un grupo y sea $a \in G$. Definimos el centralizador de a, $Z_G(a)$, como

$$Z_G(a) = \left\{b \in G \mid ab = ba\right\},$$

es decir, el conjunto de elementos que conmutan con a. Sea $S \subseteq G$. Definimos el centralizador de S, $Z_G(S)$, como

$$Z_G(S) = \left\{b \in G \mid ab = ba, \forall a \in S\right\},$$

es decir, la intersección de los centralizadores de todos sus elementos. Definimos el centro de G, $Z(G)$ como

$$Z(G) = Z_G(G),$$

es decir, el conjunto de elementos que conmutan con cualquier otro elemento.

1.9.1. Acción por traslación de G en $X = G$

Definición 1.9.16. Sea G un grupo. Definimos la acción por traslación de G como la aplicación

$$\begin{aligned} G \times G &\to G \\ (a, x) &\mapsto a \cdot x = ax. \end{aligned}$$

Observación 1.9.17. Las acciones por traslación son transitivas y fieles.

Teorema 1.9.18. *Teorema de Carley.*
Sea G un grupo finito con $|G| = n$. Entonces, G es isomorfo a un subgrupo de $\mathcal{S}_n$.

Demostración. Tomamos la acción de G en $X = G$ por traslación. Puesto que de trata de una acción fiel, la aplicación

$$\begin{aligned} m\colon G &\to \mathcal{S}_n \\ a &\mapsto m_a \end{aligned}$$

es inyectiva. Veamos que $\operatorname{Im}(m)$ es un grupo.

- $m_1 = \mathrm{Id} \in \operatorname{Im}(m)$,
- $m_a m_b(x) = abx = m_{ab}(x) \in \operatorname{Im}(m)$,
- $m_{a^{-1}} m_a(x) = a^{-1}ax = x \implies m_a^{-1} \in \operatorname{Im}(m)$.

Así pues, la aplicación

$$\begin{aligned} \widetilde{m}\colon G &\to \operatorname{Im}(m) \\ a &\mapsto m_a \end{aligned}$$

es un morfismo biyectivo de grupos de G a un subgrupo de $\mathcal{S}_n$. □

1.9.2. Acción por conjugación de G en $X = G$

Definición 1.9.19. Sea G un grupo. Definimos la acción por conjugación de G como la aplicación

$$\begin{aligned} G \times G &\to G \\ (a, x) &\mapsto axa^{-1}. \end{aligned}$$

Proposición 1.9.20. Sea G un grupo. Si $x \in G$ es punto fijo por conjugación, entonces $x \in Z(G)$.

Demostración. x punto fijo $\iff axa^{-1} = x, \forall a \in G \iff ax = xa, \forall a \in G \iff x \in Z(G)$. □

Proposición 1.9.21. Sea G un grupo. Si consideramos la acción por conjugación de G, entonces $G_x = Z_G(x)$.

Demostración. $G_x = \{a \in G \mid axa^{-1} = x\} = \{a \in G \mid ax = xa\} = Z_G(x)$. □

Proposición 1.9.22. *Fórmula de órbitas de la acción por conjugación de G en G.* Sea G un grupo, y sean $x_1, \ldots, x_r$ representantes de órbitas no puntuales. Entonces,

$$|G| = \left|Z(G)\right| + \sum_{i=1}^{r} \left[G : Z_G(x_i)\right].$$

Demostración. Se tiene que

$$|G| = \sum_{i=1}^{s} |Gx_i| = \left|Z(G)\right| + \sum_{i=1}^{r} \left[G : G_{x_i}\right].$$

□

Teorema 1.9.23. *Teorema de Cauchy.*
Sea G un grupo finito de orden n y sea $p|n$ un número primo. Entonces, existe algún $x \in G$ tal que $\mathrm{o}(x) = p$.

Demostración. Si G es un grupo abeliano, procederemos a demostrar el enunciado por inducción sobre n. Los casos $n = 2$ y $n = 3$ son grupos conocidos. Suponemos $n \geq 4$ y tomamos $x \in G$. Por el teorema de Lagrange tenemos que $\mathrm{o}(x) = m|n$. Separamos ahora en dos casos.

Si $p|m$, entonces $\mathrm{o}\left(x^{\frac{m}{p}}\right) = p$ y hemos acabado.

Si $p \not| m$, tenemos que $\langle x \rangle \triangleleft G$ (por ser G abeliano), de modo que $G/\langle x \rangle$ es un grupo cociente. Así pues,

$$\left|G/\langle x \rangle\right| = \frac{|G|}{\left|\langle x \rangle\right|} = \frac{n}{m}.$$

Como $p|n$ y $p \not| m$, se tiene que $p|\left|G/\langle x \rangle\right| < n$ y, por hipótesis de inducción, $\exists \bar{y} \in G/\langle x \rangle$ tal que $\mathrm{o}(\bar{y}) = p$. Esto quiere decir que $(\bar{y})^p = \bar{1} = \langle x \rangle$, cosa que implica que $y^p = x^r$ para algún $1 \leq r \leq m$. Entonces,

$$(y^m)^p = (y^p)^m = (x^r)^m = (x^m)^r = 1^r = 1,$$

y necesariamente $\mathrm{o}(y^m)|p$. Puesto que p es primo, solo existen las posibilidades $\mathrm{o}(y^m) = 1$ y $\mathrm{o}(y^m) = p$. Si se da el primer caso,

$$\mathrm{o}(y^m) = 1 \implies y^m = 1 \implies \overline{y^m} = \bar{1} \implies (\bar{y})^m = 1 \implies p|m,$$

lo cual supone una contradicción. Por lo tanto, $\mathrm{o}(y^m) = p$ y hemos acabado.

En el caso de que G no sea abeliano, aplicamos la fórmula de órbitas (1.9.22), que establece que

$$|G| = \left|Z(G)\right| + \sum_{i=1}^{r} \left[G : G_{x_i}\right].$$

Podemos separar los dos casos siguientes.

- Si $\exists i \in \{1,\dots,r\}$ tal que $\operatorname{mcd}\left(p, \left[G : G_{x_i}\right]\right) = 1$. Entonces, $p \nmid \left[G : G_{x_i}\right] = \frac{|G|}{\left|G_{x_i}\right|}$, pero p divide $|G|$, de manera que p divide también $\left|G_{x_i}\right| \leq n$. Aplicando ahora la hipótesis de inducción, se tiene que $\exists x' \in G_{x_i} \subset G$ tal que $\mathrm{o}(x') = p$.
- Si $\forall i \in \{1,\dots,r\}$ se tiene que $p \mid \left[G : G_{x_i}\right]$. Entonces, p divide $\left|Z(G)\right|$, pero $Z(G)$ es un subgrupo propio de G, de modo que $\left|Z(G)\right| < n$. Finalmente, aplicando de nuevo la hipótesis de inducción, $\exists x \in Z(G)$ tal que $\mathrm{o}(x) = p$.

□

1.10. Grupos de Sylow

Definición 1.10.1. Un p-grupo G es un grupo de orden $|G| = p^r$ con p primo y $r \geq 0$.

Observación 1.10.2. $\{1\}$ es un p-grupo para todo primo p. $(r = 0)$.

Teorema 1.10.3. Sea G un p-grupo de orden p^r. Entonces:

i) G es trivial $\iff$ $Z(G)$ es trivial.

ii) G es resoluble.

iii) Si G es simple, entonces $G \cong \mathbb{Z}/p\mathbb{Z}$.

Demostración.

i) La implicación directa es inmediata. Veamos la inversa. Supongamos que G es no trivial y separemos casos en función de la conmutatividad de G. Si G es abeliano, entonces $Z(G) = G$ y $Z(G)$ es no trivial. Recordemos la fórmula de órbitas (1.9.22)

$$|G| = \left|Z(G)\right| + \sum_{i=1}^{s} \left[G : G_{x_i}\right] = \left|Z(G)\right| + \sum_{i=1}^{s} \left[G : Z_G\left(x_i\right)\right],$$

donde $x_1, \dots, x_s$ son representantes de las órbitas no puntuales de G. En particular, $Z_G\left(x_i\right) \subsetneq G$ y tenemos que para todo $1 \leq i \leq s$

$$\left[G : Z_G\left(x_i\right)\right] = \frac{|G|}{\left|Z_G\left(x_i\right)\right|} = \frac{p^r}{p^{r_i}} = p^{t_i},$$

con $t_i \geq 1$, ya que $t_i = 0 \implies r_i = r \implies Z_G\left(x_i\right) = G$, lo cual no puede ser. Entonces, p divide todos los sumandos $\left[G : Z_G\left(x_i\right)\right]$ de la fórmula de órbitas y divide también a $|G|$, así que necesariamente divide a $|Z_G|$, de lo que deducimos que $Z(G)$ es no trivial.

ii) Procederemos por inducción sobre $|G|$. Si $|G| = 1$, G es trivialmente abeliano. Supongamos ahora que G no es abeliano y que $|G| > 1$. En virtud del primer apartado, $Z(G)$ es no trivial y $Z(G) \subsetneq G$ porque no es abeliano. $G \triangleright Z(G) \triangleright \{1\}$ es una torre

normal porque los elementos de $Z(G)$ conmutan con todos los de G y, en particular, entre ellos. Se tiene que $\left|{}^{G}\!/_{Z(G)}\right| = \frac{p^r}{p^s}$ con $0 < s < r$, ya que $Z(G)$ es no trivial y $G \neq Z(G)$. Aplicando ahora la hipótesis de inducción, ${}^{G}\!/_{Z(G)}$ es resoluble. Finalmente, la proposición (1.8.15) afirma que

$${}^{G}\!/_{Z(G)} \text{ es resoluble y } Z(G) \text{ es resoluble } \Longrightarrow G \text{ es resoluble.}$$

iii) Sea G un p-grupo simple. En virtud del apartado anterior, G tiene una torre normal abeliana. Como G es simple, no tiene subgrupos normales propios y $G \triangleright \{1\}$ es la única torre normal abeliana posible. Así pues, ${}^{G}\!/_{\{1\}}$ es abeliano y simple y concluimos $G \cong {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$.

□

El Teorema de Lagrange (1.5.7) nos dice que si H es un subgrupo de un grupo finito G, el cardinal de H divide al de G. Lo natural es preguntarse si el recíproco es cierto, es decir, si para cada divisor n del orden de G existe un subgrupo H de G con $|H| = n$. Si $n = p$ primo, es cierto, el Teorema de Cauchy (1.9.23) nos asegura que $\left|\langle x\rangle\right| = p$ para algún $x \in G$. Veamos que, en general, este enunciado es falso.

Ejemplo 1.10.4. Sea $G = \mathcal{A}_5, |G| = 60$ y sea $n = 30$. No existe ningún subgrupo H con $|H| = 30$ debido a que, de lo contrario,

$$[G : H] = \frac{|G|}{|H|} = \frac{60}{30} = 2, \Longrightarrow H \triangleleft G.$$

lo cual supone una contradicción con que $G = \mathcal{A}_5$ es simple.

Teorema 1.10.5. *Primer teorema de Sylow.*
Sea G un grupo finito y sea p un primo tal que p^r divide $|G|$. Entonces existe un subgrupo H de G tal que $|H| = p^r$.

Demostración. Realizaremos la demostración por inducción sobre $|G|$. El caso $|G| = 1$ es trivial y para $|G| = p$ el teorema de Cauchy (1.9.23) nos proporciona el resultado. Dividiremos la demostración en dos casos.

- $p \not| \left|Z(G)\right|$. Por la fórmula de órbitas (1.9.22), y teniendo en cuenta que p divide $|G|$, existe almenos un representante x_i de una órbita no puntual tal que

$$p \not| \left[G : Z_G(x_i)\right] = \frac{|G|}{\left|Z_G(x_i)\right|},$$

de modo que p^r divide $\left|Z_G(x_i)\right| < |G|$. Por hipótesis de inducción, existe un subgrupo H de $Z_G(x_i) \subseteq G$ con $|H| = p^r$.

- p divide $\left|Z(G)\right|$. Por el Teorema de Cauchy (1.9.23), existe un $x \in Z(G)$ tal que $o(x) = p$. Sea $L = \langle x\rangle$. Como $x \in Z(G)$, $L \triangleleft G$, de modo que ${}^{G}\!/_{L}$ es un grupo y tiene orden

$$\left|{}^{G}\!/_{L}\right| = \frac{|G|}{|L|} = \frac{|G|}{p}.$$

Como p^r divide $|G|$, p^{r-1} divide $\left|{}^{G}\!/_{L}\right| < |G|$ y, por la hipótesis de inducción, existe un subgrupo K de ${}^{G}\!/_{L}$ tal que $|K| = p^{r-1}$. Entonces, $K = {}^{H}\!/_{L}$, para algún subgrupo H de G, con $L \subseteq H$. Finalmente,

$$p^{r-1} = |K| = \left|{}^{H}\!/_{L}\right| = \frac{|H|}{|L|} = \frac{|H|}{p} \implies |H| = p.$$

□

Índice alfabético