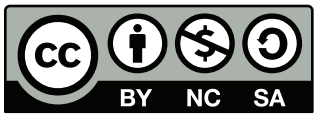
ESTRUCTURAS ALGEBRAICAS

ApuntsFME

Barcelona, Octubre 2018

Última modificación: 2 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 $\mathrm{ord}(\sigma)$ 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

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

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

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

   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,

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

   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

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

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

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

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

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

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

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

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

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

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

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

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

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

iii) Sean $k = \mathrm{ord}\,(x^m)$ y $g = \mathrm{mcd}(n, m)$. 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 $\text{ord}(G) = n$ (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 $\text{ord}(G) = \infty$, entonces

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

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

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

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 $\text{mcd}(m, n) = \frac{n}{d}$.

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

Con esta última condición, tenemos que

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

□

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

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

□

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,

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

□

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

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

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 $x \in G_1$, $f\left(x\right) = f\left(x \cdot 1\right) = f\left(x\right) f\left(1\right) \implies f\left(1\right) = 1$.

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

□

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. $f\left(x\right) = x'$. Sean $f\left(x\right), f\left(y\right) \in G_2$ dos elementos cualesquiera de G_2,

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

□

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

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 $a, b \in f^{-1}\left(K\right)$, entonces $\exists a', b' \in K$ t. q. $f\left(a\right) = a'$, $f\left(b\right) = b'$ y tenemos que $ab = f^{-1}\left(f\left(ab\right)\right) = f^{-1}\left(f\left(a\right)f\left(b\right)\right) = f^{-1}\left(a'b'\right) \in f^{-1}\left(K\right)$, ya que $a'b' \in K$.
   iii) Sea $a \in f^{-1}\left(K\right)$, entonces $\exists a' \in K$ t. q. $f\left(a\right) = a'$, y tenemos que $a^{-1} = f^{-1}\left(f\left(a^{-1}\right)\right) = f^{-1}\left(f\left(a\right)^{-1}\right) = f^{-1}\left(\left(a'\right)^{-1}\right) \in f^{-1}\left(K\right)$, ya que $\left(a'\right)^{-1} \in K$.

□

Observación 1.4.7.

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

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

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

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

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

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

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

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

Teorema de Lagrange (1.5.7)
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

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

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

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

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.

$$H \triangleleft K \triangleleft G \not\Longrightarrow H \triangleleft G.$$

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

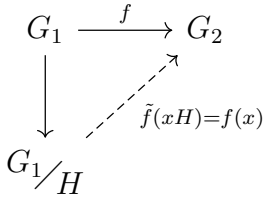
$$\{\text{sg. (normales) de } G \text{ que contienen a } H\} \leftrightarrow \left\{\text{sg. (normales) de } G/H\right\}$$

$$\begin{aligned} K \supset H &\mapsto \Pi(K) \\ \Pi^{-1}(L) &\hookleftarrow L \end{aligned}$$

Demostración. Ejercicio. □

Teorema de isomorfía (primero) (1.6.14)
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

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

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,

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

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

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

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,

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

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

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

$$\mathcal{O}_d(G) = \left\{y \in G \middle| \, \mathrm{o}(y) = d\right\} \subseteq \left\{y \in \Bbbk^* \middle| \, \mathrm{o}(y) = d\right\} = \mathcal{O}_d(\Bbbk^*).$$

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

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

□

Índice alfabético