Estructuras Algebraicas

Victoria Torroja Rubio

8/9/2025

Índice general

Profesor: Adrián Barcelo

Correo: abacelo@ucm.es

Despacho: 443

Evaluación

- 15 % Trabajo a entregar
- 20 % Ejercicios/prácticas a entregar/hacer
- 65 % Examen final (hay que sacar al menos un 4 para que haga media con la evaluación continua)

Capítulo 0

Preliminares

Recordamos que $\mathbb{N} = \{1, 2, \ldots\}$ es el conjunto de los **números naturales** y $\mathbb{Z} = \{\ldots, -1, -1, 0, 1, 2, \ldots\}$ es el conjunto de **números enteros**. Tomamos la suma y el producto tal y como los conocemos $(+, \cdot)$. Además, dotas a $\mathbb{N}$ y $\mathbb{Z}$ del orden que conocemos $(<)$. En $\mathbb{N}$, tenemos el **principio del buen orden**.

Teorema 0.1 (Principio del buen orden)**.** Todo subconjunto no vacío de $\mathbb{N}$ tiene un elemento mínimo.

Recordemos también que dado $z \in \mathbb{Z}$, su valor absoluto $|z|$ es asignar el valor positivo de z. En concreto,

$$|z| = \begin{cases} z, & z \geq 0 \\ -z, & z < 0 \end{cases}.$$

Además, se cumple que

$$|z_1| \leq |z_1 \cdot z_2|, \quad \forall z_1, z_2 \in \mathbb{Z} / \{0\}.$$

0.1. Divisibilidad

Teorema 0.2. Sean $n, m \in \mathbb{Z}$ con $m \neq 0$. Así, existen $q, r \in \mathbb{Z}$ únicos tales que $n = mq + r$ y $0 \leq r < |m|$.

Demostración. Estudiemos primero la existencia. Supongamos que $m > 0$ y consideremos el siguiente subconjunto

$$X = \{n - mk \mid k \in \mathbb{Z}, n - mk \geq 0\} \subset \mathbb{N}.$$

Tenemos que este subconjunto es no vacío. En efecto, si $n \geq 0$ tenemos que $n = n - m \cdot 0 \in X$. Si $n < 0$, tenemos que $n(1 - m) \in X$. Así, tenemos que $X \neq \emptyset$. Así, podemos aplicar el principio del bueno orden, por lo que existe un elemento mínimo r. Así, tenemos que existe $q \in \mathbb{Z}$ tal que

$$r = n - mq, \ r \geq 0.$$

Además, tenemos que

$$n-(q+1)\,m=n-qm-m=r-m<r.$$

Por tanto, $n-(q+1)\,m\notin X$ por ser r el mínimo. Entonces, necesariamente tenemos que $n-(q+1)\,m<0$, por lo que $r<m\leq|m|$. Ahora, si $m<0$, hemos visto que $r_1,q_1\in\mathbb{Z}$ tales que $n=(-m)\,q_1+r_1$ con $0\leq r_1<|m|$. Es trivial que esto demuestra el teorema, puesto que $-q_1\in\mathbb{Z}$.
Ahora demostramos la unicidad. Supongamos que existen $q_1,q_2,r_1,r_2\in\mathbb{Z}$ tales que

$$n=mq_1+r_1,\quad n=mq_2+r_2.$$

Supongamos sin pérdida de generalidad que $r_1\leq r_2$. Así, tenemos que

$$(q_1-q_2)\,m=r_2-r_1\Rightarrow|q_1-q_2|\,|m|=r_2-r_1.$$

Así, si $r_1\neq r_2$, tenemos que $|q_1-q_2|\geq 1$. Por tanto, se tiene que

$$|q_1-q_2|\,|m|\geq|m|>r_2\geq r_2-r_1.$$

Así, hemos obtenido una contradicción, por lo que debe ser que $r_1=r_2$ y, consecuentemente, $q_1=q_2$. $\square$

Observación. A los números n,m,q y r los llamamos **dividendo**, **divisor**, **cociente** y **resto**, respectivamente.

Definición 0.1. Dados $a,b\in\mathbb{Z}$, decimos que a divide a b, $a|b$, si existe $c\in\mathbb{Z}$ tal que $b=ac$.

Recordemos que si $c|a$ y $c|b$, entonces $c|a+b$. En efecto,

$$a+b=ck_1+ck_2=c\,(k_1+k_2)\,.$$

Proposición 0.1. Sean $a,b,c\in\mathbb{Z}$,

Reflexiva. $a|a$.

Antisimétrica. $a|b,b|a\Rightarrow a=b$.

Transitiva. $a|b,b|c\Rightarrow a|c$.

Demostración. La propiedad reflexiva es trivial, puesto que $a=a\cdot 1,\forall a\in\mathbb{Z}$. En cuanto a la propiedad antisimétrica, tenemos que si $a|b$ y $b|a$, entonces $a=\lambda_1 b$ y $b=\lambda_2 a$. Así, tenemos que $a\leq b$ pero también tenemos que $b\leq a$, por lo que debe ser que $b=a$. Finalmente, para demostrar la propiedad transitiva basta ver que si $b=\lambda a$ y $c=\mu b$, se tiene que $c=\mu\lambda a$, por lo que $a|c$. $\square$

Observación. Tenemos entonces, que la relación de divisibilidad es una **relación de orden parcial**.

Definición 0.2 (Máximo común divisor). Sean $n, m \in \mathbb{Z}$ y $d \in \mathbb{Z}$. Diremos que d es **divisor común** de n y m si $d|n$ y $d|m$. Llamaremos **máximo común divisor** de n y m, $\operatorname{mcd}(n, m)$ al más grande de los divisores comunes positivos.

Observación. Dado que el máximo común divisor es positivo, es único.

Proposición 0.2. Sean $a, b \in \mathbb{Z}$, entonces se cumple:

1. Existe el máximo común divisor de a y b.
2. **Identidad de Bézout.** Existen $x, y \in \mathbb{Z}$ tales que si $d = \operatorname{mcd}(a, b)$ entonces $d = ax + by$.

Demostración. La demostración de 1 y 2 es la misma. Sean $a, b \in \mathbb{Z}$ y consideremos el siguiente conjunto:

$$S = \{\lambda a + \mu b \ : \ \lambda, \mu \in \mathbb{Z}, \lambda a + \mu b > 0\} \subset \mathbb{N}.$$

Está claro que $S \neq \emptyset$, pues supongamos sin pérdida de generalidad que $a > b$, entonces $a - b > 0 \in S$. Así, por el principio del buen orden, tenemos que existe un elemento mínimo de S al que llamaremos d. Así, existen $x, y \in \mathbb{Z}$ tales que $d = ax + by$. Vamos a ver que $d = \operatorname{mcd}(a, b)$. En primer lugar, vamos a ver que es divisor común de a y b. Tenemos que, por el algoritmo de la divisibilidad, existen $q, r \in \mathbb{Z}$ con $0 \leq r < d$ tales que

$$a = qd + r.$$

Si $r > 0$, tenemos que

$$r = a - qd = a - q(ax + by) = (1 - qx)a + yb \in S.$$

Así, tenemos que $r \geq d$ pero también $r < d$, lo que es una contradicción. Por tanto, debe ser que $r = 0$, por lo que $d|a$. De manera análoga se demuestra que $r|b$. Así, queda demostrado que d es divisor común de a y b. Ahora, supongamos que d' es también divisor común de a y b. Así, existen $k_1, k_2 \in \mathbb{Z}$ tales que $a = k_1 d'$ y $b = k_2 d'$. De esta manera queda que

$$d = xa + yb = xk_1 d' + yk_2 d' = (xk_1 + yk_2) d'.$$

Así, tenemos que $d' \leq d$, por lo que $d = \operatorname{mcd}(a, b)$. $\square$

Así, sabemos que existe el máximo común divisor, pero ahora necesitamos una manera de calcularlo. Para ello haremos uso del algoritmo de Euclides, que nos va a permitir también encontrar una identidad de Bézout.

Lema 0.1. Sean $a, b, r \in \mathbb{Z}$ tales que $0 \leq r < b$. Si existe $q \in \mathbb{Z}$ tal que $a = bq + r$, entonces $\operatorname{mcd}(a, b) = \operatorname{mcd}(b, r)$.

Demostración. Supongamos las condiciones del lema. Tenemos que, claramente $\operatorname{mcd}(a, b)\,|r$. Así, $\operatorname{mcd}(a, b)$ es divisor común de b y r, por lo que $\operatorname{mcd}(a, b) \leq \operatorname{mcd}(b, r)$. Por otro lado, tenemos que $\text{mcd}\,(b,r)\,|a$, por lo que es divisor común de b y a y, consecuentemente, $\text{mcd}\,(b,r) \leq \text{mcd}\,(a,b)$. Así, tenemos que $\text{mcd}\,(a,b) = \text{mcd}\,(b,r)$. $\square$

Teorema 0.3 (Algoritmo de Euclides). Sean $a, b \in \mathbb{Z}$, $a > b$ y vamos a dividir a entre b. Así, $a = bq_1 + r_1$, $q_1 \in \mathbb{Z}$, $0 < r_1 < |b|$.

- Si $r_1 = 0$, entonces $b|a$ y $\text{mcd}\,(a,b) = b$.
- Si $r_1 \neq 0$, entonces aplicando el lema tenemos que $\text{mcd}\,(a,b) = \text{mcd}\,(b,r_1)$. Así, dividimos b entre r_1 y obtenemos $b = r_1q_2 + r_2$, y aplicamos el mismo razonamiento de antes hasta obtener un $r_k = 0$ y tendremos que $r_{k-1} = \text{mcd}\,(a,b)$.

Sabemos que este proceso es finito por el principio del buen orden y porque r_i se hace cada vez más pequeño.

Reconstruyendo las igualdades obtenidas en el algoritmo de Euclides podemos obtener una identidad de Bézout.

0.2. Factorización

Definición 0.3. Sea $a \in \mathbb{Z}/\{-1,0,1\}$.

1. Diremos que a es **primo** si $a|bc \Rightarrow a|b \vee a|c$.
2. Diremos que a es **irreducible** si $a = bc \Rightarrow b = \pm 1 \vee c = \pm 1$.

Observación. Si $a \in \mathbb{N}$, a es irreducible si sus únicos divisores son 1 y a. Además, si $a \in \mathbb{Z}$, entonces a es primo si y solo si es irreducible. En efecto, si a es irreducible y $a|bc$ pero a no divide a b, tenemos que $\text{mcd}\,(a,b) = 1$. Así, existen $\lambda, \mu \in \mathbb{Z}$ tales que

$$1 = \lambda a + \mu b.$$

De esta forma, se tiene que, dado que $bc = ak$ con $k \in \mathbb{Z}$,

$$c = c\lambda a + c\mu b = c\lambda a + k\mu a = (c\lambda + k\mu)\,a.$$

Así, tenemos que a es primo.

Teorema 0.4 (Teorema fundamental de la aritmética). Sea $n \in \mathbb{Z}/\{-1,0,1\}$ [a], entonces n es producto finito de enteros irreducibles de forma única salvo reordenación. Esto es, existen $p_1, \ldots, p_k \in \mathbb{Z}$ y $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$ tales que $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

[a] Si $n < 0$ consideramos la descomposición de $|n|$ y lo multiplicamos por -1.

Corolario 0.1. Sean $a, b \in \mathbb{Z}$ y $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ y $b = q_1^{\beta_1} \cdots q_t^{\beta_t}$, con $p_i, q_i \in \mathbb{Z}$ irreducibles y $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}$. Así, definimos el $\text{mcd}\,(a,b)$ como los enteros irreducibles comunes elevados al menor exponente. Es decir, si $p_i = q_i$ para $i = 1, \ldots, s$ con $s < t, k$, tenemos que

$$\text{mcd}\,(a,b) = p_1^{\text{mín}\{\alpha_1,\beta_1\}} \cdots p_s^{\text{mín}\{\alpha_s,\beta_s\}}.$$

0.3. Aritmética modular

Definición 0.4. Sean $a, m \in \mathbb{Z}$ y $n \in \mathbb{N}$. Diremos que a es **congruente** con m módulo n si $a - m = kn$ para $k \in \mathbb{Z}$, $a \equiv m \mod n$.

Observación. También podemos decir que m es el resto de dividir a entre n.

Las congruencias respetan las operaciones, es decir si $a_1 \equiv m_1 \mod n$ y $a_2 \equiv m_2 \mod n$ tenemos que

$$a_1 + a_2 \equiv m_1 + m_2 \mod n.$$

Con la resta funciona igual. Además, si $b \in \mathbb{Z}$,

$$ba_1 \equiv bm_1 \mod n.$$

Teorema 0.5 (Teorema chino del resto)**.** Sea el sistema de congruencias

$$\begin{cases} x \equiv a_1 \mod n_1 \\ \vdots \\ x \equiv a_t \mod n_t \end{cases},$$

tal que $a_1, \dots, a_t \in \mathbb{Z}$, $n_1, \dots, n_t \in \mathbb{N}$ tal que $\operatorname{mcd}(n_i, n_j) = 1$, $\forall i \neq j$. Entonces, el sistema tiene solución y estas soluciones están en la misma clase de equivalencia módulo $n = n_1 \cdots n_t$.

Capítulo 1

Grupos

Definición 1.1 (Grupo). Sea la terna $(G, \cdot, e)$ donde G es un conjunto no vacío, $\cdot : G \times G \to G$ una operación interna y $e \in G$. Diremos que la terna $(G, \cdot, e)$ es un **grupo** si se cumple:

Asociativa. $\forall a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Elemento neutro. $\forall a \in G$, $a \cdot e = e \cdot a = a$.

Inversa. $\forall a \in G, \exists b \in G$, $a \cdot b = b \cdot a = e$.

Además, diremos que $(G, \cdot, e)$ es **abeliano** si se cumple la propiedad conmutativa, es decir, $\forall a, b \in G$, $a \cdot b = b \cdot a$.

Definición 1.2 (Orden de un grupo). Dado un grupo $(G, \cdot, e)$, llamamos **orden** del grupo a la cardinalidad de G, $|G|$.

Ejemplo. Algunos ejemplos de grupos son:

1. $(\mathbb{R}, +, 0)$ es un grupo abeliano.
2. $(\mathbb{R}/\left\{0\right\}, \cdot, 1)$ es un grupo abeliano.
3. $(\mathbb{Z}, +, 0)$ es un grupo abeliano.
4. $(\mathbb{N} \cup \left\{0\right\}, +, 0)$ no es un grupo por no haber inversos.

Proposición 1.1. Sea $(G, \cdot, e)$ un grupo. Entonces se tiene que:

1. El elemento neutro es único.
2. Dado $a \in G$, existe un único elemento inverso.

Demostración. Demostremos **1**. Supongamos que e y e' son ambos elementos neutros.

Tenemos que

$$e = e \cdot e' = e' \cdot e = e'.$$

Así, hemos visto que $e = e'$. Ahora, demostremos **2**. Si $a \in G$, supongamos que $b, c \in G$ son sus inversos. Entonces tenemos que

$$b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = e \cdot c = c.$$

Así, tenemos que $b = c$. □

Observación. 1. De ahora en adelante, en vez de escribir $(G, \cdot, e)$ para nombrar el grupo, escribiremos sólamente G. De manera similar, no escribiremos $a \cdot b$ sino ab.

2. Dado $a \in G$ finito, a su inverso lo denotaremos por a^{-1}.

3. Dado un grupo G, va a estar totalmente definido por su tabla de multiplicación (tabla de Cayley). Esta será de la forma

	e	a_1	$\cdots$	a_n
e	e	a_1	$\cdots$	a_n
a_1	a_1	a_1^2	$\cdots$	$a_1 a_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_n	a_n	$a_n a_1$	$\cdots$	a_n^2

Ejemplo. Consideremos el grupo $(\mathbb{Z}_5 / \{0\}, \cdot)$. Su tabla de Cayley será:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Proposición 1.2. Sea G un grupo. Entonces,

1. $\forall a \in G$, $\left(a^{-1}\right)^{-1} = a$.
2. $\forall a, b, c \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
3. $\forall a, b, c \in G$, si $ba = ca$ o $ab = ac$, entonces $b = c$.

Demostración. Demostramos **1**. Si $a \in G$, tenemos que

$$a^{-1}a = a \cdot a^{-1} = e.$$

Dado que el inverso es único, tenemos que $\left(a^{-1}\right)^{-1} = a$. Ahora demostramos **2**. Si $a, b \in G$,

$$(ab)\left(b^{-1}a^{-1}\right) = aea^{-1} = aa^{-1} = e.$$

Por la inversa del inverso, tenemos que $(ab)^{-1} = b^{-1}a^{-1}$. Finalmente, demostramos **3**. Si $a, b, c \in G$ y, sin pérdida de generalidad, $ba = ca$, dado que existe $a^{-1} \in G$, tenemos

que
$$ba = ca \iff baa^{-1} = caa^{-1} \iff be = ce \iff b = c.$$

□

Ejemplo. 1. Consideremos un conjunto $X \neq \emptyset$ y el conjunto de sus biyecciones $\text{Biy}(X) = \{f : X \to X \ : \ f \text{ biyección}\}$. Como operación tomamos la composición de funciones. Entonces, $(\text{Biy}(X), \circ)$ es un grupo. En efecto:

Asociativa. La composición de funciones es asociativa.

Elemento neutro. Tomamos como elemento neutro la función identidad. En efecto, $id \in \text{Biy}(X)$ y $\forall f \in \text{Biy}(X)$,
$$(f \circ id)(x) = f(id(x)) = f(x).$$
$$(id \circ f)(x) = id(f(x)) = f(x).$$

Inverso. Si $f \in \text{Biy}(X)$, sabemos que por ser f biyectiva existe $f^{-1} \in \text{Biy}(X)$ tal que $f \circ f^{-1} = id$ y $f^{-1} \circ f = id$.

Así, hemos visto que $(\text{Biy}(X), \circ)$ es un grupo, pero no tiene por qué ser abeliano.

2. Sea $\mathcal{M}_n(\mathbb{R})$, $n \geq 1$, el conjunto de matrices reales cuadradas con coeficientes en $\mathbb{R}$, y consideremos el producto de matrices usual. El par $(\mathcal{M}_n, \cdot)$ no es un grupo, puesto que las matrices con determinante nulo no tienen inverso.
Tomemos así solo las matrices cuyo determinante es distinto de cero, y por tanto sabemos que tienen inverso. A este conjunto lo llamamos **grupo lineal general**, $\text{GL}_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) \ : \ |A| \neq 0\}$. Así, $(\text{GL}_n(\mathbb{R}), \cdot)$ forma un grupo.
De manera similar, el conjunto $\text{SL}_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) \ : \ |A| = 1\}$, al que llamamos **grupo lineal especial**, también forma un grupo con la multiplicación.

Observación. Se puede ver que $\text{SL}_n(\mathbb{R}) \subset \text{GL}_n(\mathbb{R})$.

1.1. Subgrupos

Definición 1.3 (Subgrupo)**.** Sea G un grupo y $H \subset G$. Diremos que H es **subgrupo** de G, $H \leq G$, si H es cerrado para la operación de G, esto es

- $H \neq \emptyset$.
- $\forall a, b \in H$, $ab \in H$.
- $\forall a \in H$, $a^{-1} \in H$.

Ejemplo. **(i)** Sea G un grupo. Tenemos que $\{e\} \leq G$ es el **subgrupo trivial** .

(ii) $\text{SL}_n(\mathbb{R}) \leq \text{GL}_n(\mathbb{R})$.

(iii) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

(iv) $\mathbb{Q}/\{0\} \leq \mathbb{R}/\{0\} \leq \mathbb{C}/\{0\}$.

Proposición 1.3. Sea G un grupo y $H \subset G$. Así, $H \leq G$ si y solo si $e \in H$ y $\forall a, b \in H$ se cumple que $ab^{-1} \in H$.

Demostración. Demostremos la primera implicación. Si $H \leq G$, tenemos que $H \neq \emptyset$ por lo que existe $a \in H$, por lo que $a^{-1} \in H$ y $e = aa^{-1} \in H$. Ahora, si $a, b \in H$, tenemos que $b^{-1} \in H$, por lo que $ab^{-1} \in H$.
Recíprocamente, $H \neq \emptyset$ puesto que $e \in H$. Sea $a \in H$. Tenemos que $a^{-1} = e \cdot a^{-1} \in H$. Falta que si $a, b \in H$, entonces $ab \in H$. Sean $a, b \in H$, entonces $a^{-1}, b^{-1} \in H$. Entonces $ab = a\left(b^{-1}\right)^{-1} \in H$. Así, demostramos las tres propiedades. $\square$

Ejemplo (Producto cartesiano de dos grupos)**.** Sean $(G_1, \cdot_{G_1}, e_{G_1})$ y $(G_2, \cdot_{G_2}, e_{G_2})$ dos grupos. Vamos a ver que su producto cartesiano también es un grupo. Definimos la siguiente operación para el producto cartesiano:

$$\begin{aligned} \cdot : (G_1 \times G_2) \times (G_1 \times G_2) &\to G_1 \times G_2 \\ (g_1, g_2) \times (g_1', g_2') &\to (g_1 \cdot_{G_1} g_1', g_2 \cdot_{G_2} g_2') . \end{aligned}$$

Está claro que $G = G_1 \times G_2 \neq \emptyset$ y que se trata de una operación interna.

Asociatividad. Si $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$, tenemos que

$$\begin{aligned} ((a_1, a_2) \cdot (b_1, b_2)) \cdot (c_1, c_2) &= (a_1 \cdot b_1, a_2 \cdot b_2) \cdot (c_1, c_2) = (a_1 \cdot b_1 \cdot c_1, a_2 \cdot b_2 \cdot c_2) \\ &= (a_1, a_2)(b_1 \cdot c_1, b_2 \cdot c_2) = (a_1, a_2) \cdot ((b_1, b_2) \cdot (c_1, c_2)) . \end{aligned}$$

Elemento neutro. Tenemos que $e = (e_{G_1}, e_{G_2})$. En efecto, si $(g_1, g_2) \in G_1 \times G_2$, tenemos que

$$\begin{aligned} (e_{G_1}, e_{G_2}) \cdot (g_1, g_2) &= (g_1, g_2) \\ (g_1, g_2) \cdot (e_{G_1}, e_{G_2}) &= (g_1, g_2) . \end{aligned}$$

Inverso. Si $(g_1, g_2) \in G_1 \times G_2$, tenemos que su inverso será $\left(g_1^{-1}, g_2^{-1}\right) \in G_1 \times G_2$. En efecto,

$$\begin{aligned} (g_1, g_2) \cdot \left(g_1^{-1}, g_2^{-1}\right) &= (e_{G_1}, e_{G_2}) \\ \left(g_1^{-1}, g_2^{-1}\right) \cdot (g_1, g_2) &= (e_{G_1}, e_{G_2}) . \end{aligned}$$

Así, está claro que $G_1 \times G_2$ es un grupo.

Definición 1.4. Sea G un grupo. Entonces,

(a) Llamamos **centro** de G al conjunto

$$Z(G) = \{a \in G \; : \; ax = xa, \forall x \in G\} .$$

(b) Llamamos **centralizador** de $x \in G$ al conjunto

$$C_G(x) = \{a \in G \; : \; ax = xa\} .$$

Observación. Los conjuntos $Z(G)$ y $C_G(x)$ son subgrupos. En efecto:

(i) Tenemos que $e \in Z(G)$ y si $a \in Z(G)$, también tenemos que $a^{-1} \in Z(G)$. En efecto,

$$a^{-1}x = xa^{-1} \iff aa^{-1}x = axa^{-1} \iff x = xaa^{-1} = xe = x.$$

Así, si $a, b \in Z(G)$, tenemos que $b^{-1} \in Z(G)$ y $\forall x \in G$,

$$ab^{-1}x = axb^{-1} = xab^{-1}.$$

Por lo que $ab^{-1} \in Z(G)$ y se trata de un subgrupo.

(ii) El argumento para demostrar que $C_G(x)$ es un subgrupo de G es análogo al anterior.

Observación. Se puede comprobar que $Z(G) = \bigcap\limits_{x\in G} C_G(x)$. En efecto:

(i) Si $x \in Z(G)$ tenemos que $\forall g \in G$, $xg = gx$, por lo que $\forall g \in G$, $x \in C_G(g) \iff x \in \bigcap\limits_{g\in G} C_G(g)$.

(ii) Si $x \in \bigcap\limits_{g\in G} C_G(g)$, $x \in C_G(g)$, $\forall g \in G$. Por lo que $xg = gx$, $\forall g \in G$ y $x \in Z(G)$.

1.2. Homomorfismos

Definición 1.5 (Homomorfismo)**.** Sean G_1 y G_2 grupos tales que $\cdot_{G_1}$ y $\cdot_{G_2}$ son sus operaciones y e_{G_1} y e_{G_2} sus elementos neutros. Entonces, $f : G_1 \to G_2$ es un **homomorfismo** de grupos si $\forall a, b \in G_1$,

$$f(a \cdot_{G_1} b) = f(a) \cdot_{G_2} f(b).$$

Observación. Si $f_1 : G_1 \to G_2$ y $f_2 : G_2 \to G_3$ son homomorfismos de grupos, entonces $f_2 \circ f_1$ es un homomorfismo de grupos. Es decir, la composición de homomorfismos de grupos sigue siendo homomorfismo de grupos. En efecto, si $a, b \in G_1$,

$$f_2 \circ f_1(ab) = f_2(f_1(ab)) = f_2(f_1(a) f_1(b)) = f_2(f_1(a)) f_2(f_1(b)) = f_2 \circ f_1(a) f_2 \circ f_1(b).$$

Ejemplo. Consideremos la aplicación

$$\begin{aligned} f : \mathbb{R}/\{0\} &\to \mathrm{GL}_n(\mathbb{R}) \\ t &\to \begin{pmatrix} t & 0 & \cdots & 0 \\ 0 & t & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & t \end{pmatrix} = t \cdot I_n. \end{aligned}$$

Está aplicación es un homomorfismo de grupos.

Definición 1.6. Sea $f : G_1 \to G_2$ homomorfismo de grupos. Entonces:

(a) Llamamos **núcleo** de f al conjunto

$$\operatorname{Ker}(f) = \{a \in G_1 \ : \ f(a) = e_{G_2}\}.$$

(b) Llamamos **imagen** de f al conjunto

$$\operatorname{Im}(f) = \{b \in G_2 \ : \ \exists a \in G_1, f(a) = b\}.$$

Proposición 1.4. Sea $f : G_1 \to G_2$ un homomorfismo de grupos. Entonces:

1. $f(e_{G_1}) = e_{G_2}$.
2. $\forall a \in G_1$, $f\left(a^{-1}\right) = f(a)^{-1}$.
3. Si $H \leq G_1$, entonces $f(H) \leq G_2$. En particular, tenemos que $\operatorname{Im}(f) \leq G_2$.
4. f es inyectiva si y solo si $\operatorname{Ker}(f) = \{e_{G_1}\}$.
5. Si $N \leq G_2$, entonces $f^{-1}(N) \leq G_1$ que contiene a $\operatorname{Ker}(f)$.

Demostración.

1. Sabemos que $e_{G_1} = e_{G_1} \cdot e_{G_1}$, por lo que:

$$f(e_{G_1}) = f(e_{G_1} \cdot e_{G_1}) = f(e_{G_1}) f(e_{G_1}).$$

Así, tenemos que

.

$$\begin{aligned} e_{G_2} &= f(e_{G_1})^{-1} f(e_{G_1}) = f(e_{G_1})^{-1} \left(f(e_{G_1}) f(e_{G_1})\right) \\ &= \left(f(e_{G_1})^{-1} f(e_{G_1})\right) f(e_{G_1}) = e_{G_2} f(e_{G_1}) = f(e_{G_1}). \end{aligned}$$

2. Sea $a \in G_1$, entonces por la unicidad del inverso y por **1**:

$$f(a) f\left(a^{-1}\right) = f\left(aa^{-1}\right) = f(e_{G_1}) = e_{G_2}.$$

3. Si $H \leq G_1$, tenemos que $e_{G_1} \in H$, por lo que $e_{G_2} \in f(H)$. Además, tenemos que $\forall a, b \in H$ se cumple que $ab^{-1} \in H$. Por tanto, si $x, y \in f(H)$, $\exists a, b \in H$ tales que $x = f(a)$ y $y = f(b)$, de esta manera, tenemos que $ab^{-1} \in H$, por lo que $f\left(ab^{-1}\right) \in f(H)$. Así,

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

Así, queda demostrado que $f(H) \leq G_2$.

4. Si $\operatorname{Ker}(f) = \{e_{G_1}\}$ y $f(a) = f(b)$, tenemos que

$$f(a) f(b)^{-1} = e_{G_2} \iff f\left(ab^{-1}\right) = e_{G_2}.$$

Por tanto, $ab^{-1} = e_{G_1}$, por lo que $a = b$. Así, hemos visto que f es inyectiva. Supongamos que f es inyectiva y que $a \in \operatorname{Ker}(f)$. Entonces, tenemos que $f(a) = f(e_{G_1}) = e_{G_2}$, por lo que $a = e_{G_1}$ y $\operatorname{Ker}(f) = \{e_{G_1}\}$.

5. Supongamos que $N \leq G_2$. Tenemos que $e_{G_2} \in N$, por lo que $e_{G_1} \in f^{-1}(N)$. Si $x, y \in f^{-1}(N)$ tenemos que $f(x), f(y) \in N$, así,

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

Por tanto, $\forall x, y \in f^{-1}(N)$, tenemos que $xy^{-1} \in f^{-1}(N)$, por lo que $f^{-1}(N) \leq G_1$. Ahora, si $x \in \operatorname{Ker}(f)$, tenemos que $f(x) = e_{G_2} \in N$, por lo que $x \in f^{-1}(N)$ y consecuentemente $\operatorname{Ker}(f) \leq f^{-1}(N)$.

$\square$

Ejemplo.
1. Consideremos $f_m : \mathbb{Z} \to \mathbb{Z}$ con $m \in \mathbb{Z}$, con la suma, tal que $f(z) = mz$. Tenemos que f_m es un homomorfismo de grupos. Por proposición anterior, tenemos que
$$m\mathbb{Z} := f(\mathbb{Z}) = \{z \in \mathbb{Z} \ : \ z = km, k \in \mathbb{Z}\} \leq \mathbb{Z}.$$
Similarmente, tenemos que $\operatorname{Ker}(f_m)$ es el subgrupo trivial si $m \neq 0$ y es $\mathbb{Z}$ si $m = 0$.
2. Es homomorfismo la aplicación $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}/\{0\} : M \to \det(M)$. En concreto, se trata de un homomorfismo sobreyectivo. Además, podemos ver que $\operatorname{Ker}(\det) = \mathrm{SL}_n(\mathbb{R})$.

Definición 1.7 (Isomorfismo y automorfismo)**.** Sea $f : G_1 \to G_2$ un homomorfismo de grupos. Si f es biyectiva, entonces f es un **isomorfismo** y lo escribimos $G_1 \cong G_2$. Si $f : G_1 \to G_1$ es un isomorfismo, se llama **automorfismo**.

Observación.
1. Si $G_1 \cong G_2$ tenemos que $|G_1| = |G_2|$ y tienen la misma tabla de Cayley.
2. Si $f : G_1 \to G_2$ es un isomorfismo, tenemos que $f^{-1} : G_2 \to G_1$ también lo es. En efecto, Si $x, y \in G_2$ existen $a, b \in G_1$ tales que $x = f(a)$ e $y = f(b)$. Así,
$$f^{-1}(xy) = f^{-1}(f(a) f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x) f^{-1}(y).$$
3. Si $f : G_1 \to G_2$ es un homomorfismo sobreyectivo, tenemos que $f(G_1) \cong G_2$, es decir, $\operatorname{Im}(f) \cong G_2$.
4. Si $f : G_1 \to G_2$ es un homomorfismo inyectivo, entonces $G_1 \cong \operatorname{Im}(f)$.
5. La relación de ser isomorfo es una relación de equivalencia.
6. El conjunto de automorfismos de G, $\operatorname{Aut}(G)$, es un subgrupo de $\operatorname{Biy}(G)$.

1.3. Grupos cíclicos

Notación. Sea $(G, \cdot)$ un grupo, $a \in G$ y $k \in \mathbb{Z}$. Entonces utilizaremos la siguiente notación:

$$a^0 = e, \quad a^n = \underbrace{a \cdot a \cdots a}_{n \text{ veces}}, \quad a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n \text{ veces}}.$$

Lema 1.1. Sea $(G, \cdot)$ un grupo, $a \in G$ y $k, l \in \mathbb{Z}$. Entonces $a^{l+k} = a^l a^k$ y $\left(a^{-1}\right)^k = a^{-k} = \left(a^k\right)^{-1}$.

Demostración. Está claro que, por la propiedad asociativa, si $l, k \in \mathbb{N}$ (o $l, k \leq 0$, se procede igual):

$$a^{l+k} = \underbrace{a \cdot a \cdots a}_{l+k \text{ veces}} = \underbrace{a \cdot a \cdots a}_{l \text{ veces}} \cdot \underbrace{a \cdot a \cdots a}_{k \text{ veces}} = a^l a^k.$$

Sin pérdida de generalidad, supongamos que $l \leq 0$ y $k > 0$. Entonces, es evidente que

$$a^l a^k = a \cdots a \cdot a^{-1} \cdots a^{-1} = a^{l-k}.$$

Por otro lado, tenemos que

$$\left(a^{-1}\right)^k a^k = \left(a^{-1} \cdots a^{-1}\right) \cdot (a \cdots a) = a^{-1} \cdots a^{-1} \cdot \left(a^{-1} \cdot a\right) \cdot a \cdots a = e.$$

Al haber el mismo número de a^{-1} que de a, está claro que el resultado será el elemento neutro. Por la unicidad del inverso, tenemos que $\left(a^k\right)^{-1} = \left(a^{-1}\right)^k$. □

Notación. Dado un grupo $(G, \cdot)$ y $a \in G$, utilizaremos la siguiente notación:

$$\langle a \rangle = \left\{ a^k \ : \ k \in \mathbb{Z} \right\}.$$

Proposición 1.5. Si G es un grupo y $a \in G$, se tiene que $\langle a \rangle \leq G$ y $\langle a \rangle$ es abeliano.

Demostración. Dado que G es un grupo, su operación es cerrada, por lo que $\langle a \rangle \subset G$. Tenemos que $e \in \langle a \rangle$. Por otro lado, si $x, y \in \langle a \rangle$, existen $n, m \in \mathbb{Z}$ tales que $x = a^n$ e $y = a^m$. Así, tenemos que $y^{-1} = a^{-m}$, así, $xy^{-1} = a^n a^{-m} = a^{n-m} \in \langle a \rangle$, puesto que $n - m \in \mathbb{Z}$. Además, es abeliano, puesto que

$$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx.$$

□

Notación. Si la operación del grupo fuera aditiva, en lugar de a^k escribiríamos ka.

Observación. Está claro que $\langle a \rangle = \left\langle a^{-1} \right\rangle$. En efecto,

$$x \in \langle a \rangle \iff x = a^n, n \in \mathbb{Z} \iff x = \left(a^{-1}\right)^{-n}, n \in \mathbb{Z} \iff x \in \left\langle a^{-1} \right\rangle.$$

Definición 1.8 (Grupo cíclico)**.** Un grupo G es **cíclico** si existe $a \in G$ tal que $G = \langle a \rangle$. Decimos que a es **generador** de G o que G **está generado** por a.

Ejemplo. Consideremos el grupo $(\mathbb{Z}, +)$. Tenemos que este grupo es cíclico y tiene dos generadores, 1 y -1. En efecto, se cumple que $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

Proposición 1.6. Si G es un grupo cíclico, cualquier subgrupo $H \leq G$ también es cíclico.

Demostración. Supongamos que $H \neq \{e\}$ y $H \neq G$, puesto que estos casos son triviales. Sea $k \in \mathbb{N}$ el más pequeño tal que $a^k \in H$. Podemos observar que dado que $H \leq G$, tenemos que $a^{-k} \in H$. Vamos a ver que $H = \langle a^k \rangle$.

(i) Si $x \in H$, tenemos que existe $l \in \mathbb{Z}$ tal que $x = a^l$. Por el algoritmo de la división, tenemos que existen $q, r \in \mathbb{Z}$ tales que

$$l = qk + r, \quad 0 \leq r < k.$$

Entonces, tenemos que

$$a^l = a^{qk+r} = \left(a^k\right)^q a^r.$$

Dado que $a^l, \left(a^k\right)^q \in H$, debe ser que $a^r \in H$. Como $k \in \mathbb{N}$ era el menor tal que $a^k \in H$ y $r < k$, debe ser que $r = 0$, por lo que $x = a^l = \left(a^k\right)^q \in H$. Así, hemos visto que $H \leq \langle a^k \rangle$.

(ii) Por otro lado, si $x \in \langle a^k \rangle$, tenemos que existe $n \in \mathbb{Z}$ tal que $x = \left(a^k\right)^l \in H$. Así, tenemos que $\langle a^k \rangle \subset H$.

Así, hemos visto que $H = \langle a^k \rangle$, por lo que es cíclico. □

Corolario 1.1. Todo $H \leq \mathbb{Z}$ es un subgrupo cíclico, es decir, existe $m \in \mathbb{Z}$ tal que $H = \langle m \rangle$.

Demostración. Se deduce fácilmente a partir de la proposición y de la observación anterior. □

Ejemplo.

1. El conjunto $U_n = \{z \in \mathbb{C} : z^n = 1\}$, de las raíces n-ésimas de la unidad, es un grupo cíclico con la multiplicación. Recordamos que $w_k = e^{i\frac{2\pi k}{n}}$, para $k = 0, \ldots, n-1$. Es sencillo ver que $(U_n, \cdot, 1) \leq (\mathbb{C}/\{0\}, 1)$. En efecto,

$$e^{i\frac{2\pi \cdot 0}{n}} = e^0 = 1.$$

Ahora, si $w_1, w_2 \in U_n$, tenemos que si $k_1 > k_2$:

$$w_1 w_2^{-1} = e^{i\frac{2\pi k_1}{n}} e^{i\frac{2\pi(-k_2)}{n}} = e^{i\frac{e\pi(k_1-k_2)}{n}} \in U_n.$$

Así, está claro que $(U_n, \cdot, 1) \leq (\mathbb{C}/\{0\} \ \cdot, 1)$. Para ver que es cíclico basta con ver que $U_n = \left\langle e^{i\frac{2\pi}{n}} \right\rangle$.

2. En $\mathbb{Z}$, tenemos que $\forall m \in \mathbb{Z}, m\mathbb{Z} \leq \mathbb{Z}$. Sabemos que $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$. Podemos definir la operación:

$$\begin{aligned} + : \mathbb{Z}_m \times \mathbb{Z}_m &\to \mathbb{Z}_m \\ ([a]_m, [b]_m) &\to [a+b]_m. \end{aligned}$$

Vamos a ver que está operación está bien definida. Si $x \in [a]_m$ e $y \in [b]_m$, tenemos que

$$m | x - a \quad \text{y} \quad m | y - b.$$

Así, existen $\lambda, \mu \in \mathbb{Z}$ tales que $x = a + \lambda m$ e $y = b + \mu m$. Por tanto, obtenemos que

$$x+y = a+\lambda m+b+\mu m = (a+b)+(\lambda+\mu)\,m \iff x+y \equiv a+b \mod m \iff [x+y]_m = [a+b]_m.$$

Queremos ver ahora que $(Z_m, +, [0]_m)$ es un grupo. Está claro que $\mathbb{Z}_m \neq \emptyset$ y que el elemento neutro es $[0]_m$. Ahora comprobamos que hay inversos. Si $[a]_m \in \mathbb{Z}_m$, tenemos que $[-a]_m \in \mathbb{Z}_m$ y, por definición, $[a]_m + [-a]_m = [0]_m$. También se puede ver que $\mathbb{Z}_m$ es cíclico, es decir, que $\mathbb{Z}_m = \langle [1]_m \rangle$.

Lema 1.2. Sea G un grupo cíclico, por lo que $G = \langle a \rangle$. Entonces si $a^k \neq e$, $\forall k \in \mathbb{N}$, tenemos que G tiene orden infinito. En caso contrario, si $m = \text{mín}\left\{k \in \mathbb{N} \,:\, a^k = e\right\}$ tenemos que $G = \langle a \rangle = \left\{e, a, \dots, a^{m-1}\right\}$. Además, $a^k = e$ si y solo si $m|k$.

Demostración. **(i)** Sea $a^k \neq e$, $\forall k \in \mathbb{N}$. Entonces, $a^k \neq e$, $\forall \mathbb{Z}/\left\{0\right\}$, por lo que el orden de G es infinito. En efecto, si existieran $i, j \in \mathbb{Z}$ distintos tales que $a^i = a^j$, tendríamos que $a^{i-j} = e$, lo que es una contradicción.

(ii) Por otro lado, sea $m = \text{mín}\left\{k \in \mathbb{N} \,:\, a^k = e\right\}$. Vamos a ver que $G = \langle a \rangle = \left\{e, a, \dots, a^{m-1}\right\}$. Es trivial que $\left\{e, a, \dots, a^{m-1}\right\} \subset G$. Recíprocamente, si $g \in G$, tenemos que existe $l \in \mathbb{Z}/\left\{0\right\}$ tal que $g = a^l$. Por el algoritmo de la división, tenemos que existen $q, r \in \mathbb{Z}$ tales que

$$l = mq + r,\ 0 \leq r < m.$$

Así, tenemos que

$$a^l = a^{mq+r} = (a^m)^q\, a^r = a^r.$$

Así, como $0 \leq r < m$, debe ser que $g \in \left\{e, a, \dots, a^{m-1}\right\}$, por lo que $G \subset \left\{e, a, \dots, m-1\right\}$. Consecuentemente, $G = \left\{e, a, \dots, a^{m-1}\right\}$.
Finalmente, como $l = qm + r$, es trivial que $a^l = e \iff r = 0$.

$\square$

Observación. En el lema podemos ver que $m = \text{mín}\left\{k \in \mathbb{N} \,:\, a^k = e\right\}$ es también el orden de G.

Proposición 1.7. Dos grupos G y H cícliclos del mismo orden son isomorfos.

Demostración. Sea $G = \langle a \rangle$ y $H = \langle b \rangle$. Consideremos la aplicación

$$\begin{aligned} f : G &\to H \\ a^k &\to b^k. \end{aligned}$$

Vamos a ver que se trata de un homomorfismo de grupos:

$$f\left(a^k\right) f\left(a^t\right) = b^k b^t = b^{k+t} = f\left(a^{k+t}\right) = f\left(a^k a^t\right).$$

Ahora vamos a ver que es biyectiva.

Inyectiva. Si $|G| > k \geq t$ y $f\left(a^k\right) = f\left(a^t\right)$, tenemos que $f\left(a^{k-t}\right) = b^{k-t} = e$. Como $|G| > k - t \geq 0$, debe ser que $k - t = 0$, por lo que $a^k = a^t$.

Sobreyectiva. Si $c \in H$ con $c = b^k$ para algún $k = 0, \ldots, |H| - 1$, tenemos que $f\left(a^k\right) = b^k = c$.

Así, está claro que f es un isomorfismo. $\square$

Notación. Vamos a llamar C_n al grupo cíclico con la multiplicación y $\mathbb{Z}_n$ al grupo cíclico con la suma.

Definición 1.9 (Orden de un elemento)**.** Sea G un grupo y $a \in G$. Llamaremos **orden** de a, $o(a)$, al cardinal del grupo que genera, es decir, $o(a) = |\langle a \rangle|$.

Observación. Sean G y H grupos.

1. Si G es finito y $a \in G$, tenemos que
$$o(a) = m = \min\left\{k \in \mathbb{N} \ : \ a^k = e\right\}.$$
Si $\langle a \rangle$ es finito, entonces se aplica de igual forma. En particular, $o(a) | k \iff a^k = e$, para $k \in \mathbb{Z} / \{0\}$.

2. Supongamos que G y H son finitos. Sea $f : G \to H$ un homomorfismo y sea $x \in G$. Entonces $o(f(x)) | o(x)$. En efecto, tenemos que
$$f(x)^{o(x)} = f\left(x^{o(x)}\right) = f(e_G) = e_H \iff o(f(x)) | o(x).$$
Además, si $f : G \to H$ es isomorfismo, entonces sabemos que existe $f^{-1} : H \to G$ que también es isomorfismo. De aquí, obtenemos que $o(x) | o(f(x))$, por lo que $o(x) = o(f(x))$.

Ejemplo.

1. Consideremos los grupos $C_2 \times C_4$ y C_8. Ambos tienen orden 8, sin embargo no son isomorfos. En C_8 hay elementos de orden 8, puesto que $C_8 = \langle a \rangle$ tal que $a^8 = e$, pero en $C_2 \times C_4$ no hay elementos de orden 8, lo más que hay es de orden 4. En efecto, si $(a, b) \in C_2 \times C_4$ tenemos que
$$(a, b)^4 = \left(a^4, b^4\right) = \left(e_{C_2}, e_{C_4}\right) \in C_2 \times C_4.$$
Tenemos que $C_8 = \left\{e, a, \ldots, a^{n-1}\right\}$ y
$$C_2 \times C_4 = \left\{(e, e), (e, b), \left(e, b^2\right), \left(e, b^3\right), (c, e), (c, b), \left(c, b^2\right), \left(c, b^3\right)\right\}.$$

2. Tomemos los grupos $(\mathbb{C}, +, 0)$ y $(\mathbb{C} / \{0\}, \cdot, 1)$. Supongamos que existe un homomorfismo de grupos, $f : \mathbb{C} / \{0\} \to \mathbb{C}$. Esta aplicación nunca podrá ser inyectiva. En efecto, tenemos que $i \in \mathbb{C} / \{0\}$ y $o(i) = 4$, pero si $z \in \mathbb{C}$, tenemos que $o(z)$ no es finito.

Lema 1.3. Sea G un grupo y sea $a \in G$ tal que $o(a)$ es finito. Entonces,

1. $o(a) = o\left(a^{-1}\right)$.
2. $\forall k \in \mathbb{N}$, si $\operatorname{mcd}(o(a), k) = 1$, entonces $o\left(a^k\right) = o(a)$. En general,
$$o\left(a^k\right) = \frac{o(a)}{\operatorname{mcd}(o(a), k)}.$$
3. Si $b \in G$ con $o(b)$ finito tal que $ab = ba$ y $\operatorname{mcd}(o(a), o(b)) = 1$, entonces $o(ab) = o(a)\, o(b)$.

Demostración. 1. Como $\langle a \rangle = \left\langle a^{-1} \right\rangle$, tenemos que
$$o(a) = |\langle a \rangle| = \left|\left\langle a^{-1} \right\rangle\right| = o\left(a^{-1}\right).$$

2. Fijemos $k \in \mathbb{N}$. Sea $r \geq 1$ con $r \in \mathbb{N}$, entonces tenemos que
$$\begin{aligned} a^{kr} = e &\iff o(a) \,|kr \iff o(a) \,|\operatorname{mcd}(o(a)\, r, kr) \\ &\iff o(a) \,|r \cdot \operatorname{mcd}(o(a), k) \iff \frac{o(a)}{\operatorname{mcd}(o(a), k)} |r. \end{aligned}$$
Así, tenemos que $o\left(a^k\right) = \dfrac{o(a)}{\operatorname{mcd}(o(a), k)}$.

3. Supongamos que $ab = ba$ y que $\operatorname{mcd}(o(a), o(b)) = 1$. Tenemos que
$$(ab)^{o(a)o(b)} = a^{o(a)o(b)} b^{o(a)o(b)} = \left(a^{o(a)}\right)^{o(b)} \left(b^{o(b)}\right)^{o(a)} = e \cdot e = e.$$
Tenemos que $o(ab) \,|o(a)\, o(b)$. Por otro lado, tenemos que
$$a^{o(ab)} b^{o(ab)} = (ab)^{o(ab)} = e.$$
Así, tenemos que $a^{o(ab)} = b^{-o(ab)}$ y por **(1)** tenemos que $o\left(a^{o(ab)}\right) = o\left(b^{o(ab)}\right)$. Por **(2)** tenemos que
$$\frac{o(a)}{\operatorname{mcd}(o(a), o(ab))} = o\left(a^{o(ab)}\right) = o\left(b^{o(ab)}\right) = \frac{o(b)}{\operatorname{mcd}(o(b), o(ab))}.$$
Sabemos que los órdenes son números naturales y que $\operatorname{mcd}(o(a), o(b)) = 1$, por tanto debe ser que
$$\frac{o(a)}{\operatorname{mcd}(o(a), o(ab))} = \frac{o(b)}{\operatorname{mcd}(o(b), o(ab))} = 1.$$

Así, obtenemos que $o(a) = \text{mcd}(o(a), o(ab))$ y $o(b) = \text{mcd}(o(b), o(ab))$, por lo que $o(a) | o(ab)$ y $o(b) | o(ab)$. Como $\text{mcd}(o(a), o(b)) = 1$, tenemos que $o(a) o(b) | o(ab)$. Así, podemos concluir que $o(a) o(b) = o(ab)$.

$\square$

Corolario 1.2. Sean $n, m \geq 1$ enteros naturales tales que $\text{mcd}(n, m) = 1$. Entonces, el grupo $C_n \times C_m \cong C_{nm}$ es el único grupo cíclico de orden $n \cdot m$ salvo isomorfía.

Demostración. La unicidad ya la hemos visto. Lo único que falta por ver es que $C_n \times C_m$ es cíclico. Supongamos que $C_n = \langle a \rangle$ y $C_m = \langle b \rangle$. Tenemos que $(a, 1_m) \in C_n \times C_m$ y $o(a, 1_m) = n$. De forma análoga se puede ver que $o(1_n, b) = m$. Tenemos que

$$o((a, 1_m)(1_n, b)) = o(a, 1_m) o(1_n, b) = nm.$$

Así, tenemos que $\langle (a, b) \rangle \subset C_n \times C_m$ y $|C_n \times C_m| = o(a, b)$, por lo que debe ser que $C_n \times C_m = \langle (a, b) \rangle$ y $C_n \times C_m$ es cíclico. $\square$

Proposición 1.8. Sea G un grupo cíclico tal que $G = \langle a \rangle$, y sea $d > 0$ de forma que $d | o(a) = n$. Entonces existe un único subgrupo $H \leq G$ de orden d tal que $H = \left\langle a^{\frac{n}{d}} \right\rangle$.

Demostración. Sea $k = \dfrac{n}{d}$. Vamos a considerar el homomorfismo de grupos $f : G \to G : x \to x^d$. Cogemos

$$H = \text{Ker}(f) = \left\{ x \in G \ : \ x^d = e \right\} \leq G.$$

Como H es subgrupo de un grupo cíclico, tenemos que H también es cíclico. Así, para un $r \in \mathbb{N}$, $H = \langle a^r \rangle$. Tenemos que $(a^r)^d = e$, por lo que $n | rd$. En particular, tenemos que $kd | rd$, por lo que $k | r$. Así, nos queda que $a^r \in \left\langle a^k \right\rangle$, por lo que $H \subset \left\langle a^k \right\rangle$. Recíprocamente, tenemos que $k = \text{mcd}(k, n)$, por lo que

$$o\left(a^k\right) = \frac{o(a)}{\text{mcd}(k, o(a))} = \frac{n}{k} = d.$$

Entonces, tenemos que $\left(a^k\right)^d = e$, por lo que $a^k \in H$. Así, tenemos que $\left\langle a^k \right\rangle \subset H$. Así, hemos desmostrado que $H = \left\langle a^k \right\rangle$.
Demostramos ahora la unicidad. Sea K un subgrupo de orden d. Como $K \leq G$, que es cíclico, sabemos que K es cíclico, y está generado por un elemento $a^r = b$. Sabemos que $b^d = e$, por lo que $b \in H$ y $K \subset H$. Como ambos grupos son del mismo orden, debe ser que $H = K$. $\square$

1.4. Grupos finitamente generados

Definición 1.10. Sea G un grupo y $S \subset G$ con $S = \{s_1, \ldots, s_k\}$ finito. Llamamos **subgrupo generado por** S al conjunto

$$\langle S \rangle = \left\{ s_1^{t_1} s_2^{t_2} \cdots s_k^{t_k} \ : \ t_i \in \mathbb{Z}, s_i \in S, k \in \mathbb{N} \right\}.$$

Definición 1.11 (Grupo finitamente generado)**.** Sea G un grupo. Diremos que G es **finitamente generado** si $G = \langle s_1, \ldots, s_k \rangle$ para algún $S = \{s_1, \ldots, s_k\} \subset G$ finito.

Observación. Se cumple que $\langle S \rangle = \bigcap\limits_{S \subset H \leq G} H$. En efecto:

(i) Si $x \in \langle S \rangle$, tenemos que $x = s_1^{t_1} \cdots s_k^{t_k}$ para $s_i \in S$ y $t_i \in \mathbb{Z}$. Entonces, si $S \subset H \leq G$, como H es subgrupo la operación está cerrada en H, por lo que $x = s_1^{t_1} \cdots s_k^{t_k} \in H$. Así, $\langle S \rangle \subset \bigcap\limits_{S \subset H \leq G} H$.

(ii) Supongamos que $x \in \bigcap\limits_{S \subset H \leq G} H$ pero $x \notin \langle S \rangle$. Esto es una contradicción, pues es fácil comprobar que $\langle S \rangle \leq G$ y $S \subset \langle S \rangle$. Por tanto, debe ser que $\bigcap\limits_{S \subset H \leq G} H \subset \langle S \rangle$.

Ejemplo.

1. Los grupos cíclicos son finitamente generados puesto que son generados por un único elemento.
2. Todos los grupos finitos están finitamente generados.
3. El grupo de los cuaterniones, Q, tiene orden 8 y tenemos que $Q = \langle i, j, k \rangle = \langle i, j \rangle$.

Proposición 1.9. Sea G un grupo y $\emptyset \neq S \subset G$, con $S = \{s_1, \ldots, s_k\}$. Sea $f : G \to H$ un homomorfismo de grupos. Entonces $f(\langle S \rangle) = \langle f(S) \rangle$.

Demostración. Sea $\langle S \rangle = \left\{ s_1^{t_1} \cdots s_k^{t_k} \ : \ t_i \in \mathbb{Z}, s_i \in S, k \in \mathbb{N} \right\}$. Tenemos que

$$f\left(s_1^{t_1} \cdots s_k^{t_k}\right) = f\left(s_1^{t_1}\right) \cdots f\left(s_k^{t_k}\right) = f(s_1)^{t_1} \cdots f(s_k)^{t_k}.$$

□

1.4.1. Grupo diédrico D_n

Sea $n \geq 3$ y consideremos $U_n = \left\langle e^{\frac{2\pi i}{n}} \right\rangle$[1]. Pensemos en la representación de U_n en el plano, que forma un polígono de n lados. Tenemos que si $u = e^{\frac{2\pi i}{n}}$, entonces

$$U_n = \left\{1, u, u^2, \ldots, u^{n-1}\right\}.$$

Sea τ la simetría en el plano respecto del eje horizontal. Entonces, tenemos que $\tau : U_n \to U_n : z \to z^{-1}$, que es una biyección. Sea ρ el giro en sentido antihorario de ángulo $\frac{2\pi}{n}$.

[1] Recordamos que este es el grupo formado por las raíces n-ésimas de la unidad.

Tenemos que $\rho : U_n \to U_n : z \to z \cdot u$, que también es una biyección. Definimos el grupo diédrico de orden n como

$$D_n = \langle \tau, \rho \rangle .$$

Estudiemos el orden de τ y ρ. Por ser τ una simetría tenemos que $\forall z \in U_n$,

$$\tau^2 (z) = \tau \left(z^{-1} \right) = z.$$

Así, tenemos que $o(\tau) = 2$. Por otro lado,

$$\rho^k (z) = zu^k.$$

Tenemos que $u^k = 1 \iff n|k$, por tanto $o(\rho) = n$. Así podemos asegurar que

$$\left\{1, \tau, \rho, \rho^2, \ldots, \rho^{n-1}, \tau\rho, \ldots, \tau\rho^{n-1}\right\} \subset D_n.$$

Por un lado sabemos que $\rho^i \neq \rho^j$ si $i \neq j$ con $i, j < n$, y $\tau \neq \rho^k$, $\forall k \leq n$, puesto que tienen imagen distinta en 1. Por tanto, tenemos que $|D_n| \geq 2n$. Veamos que efectivamente $|D_n| = 2n$ y que D_n coincide con el conjunto de arriba. Veamos que $\tau \cdot \rho$ tiene orden dos:

$$(\tau \cdot \rho)^2 (z) = \tau (\rho (\tau (\rho (z)))) = \tau (\rho (\tau (z \cdot u))) = \tau \left(\rho \left(u^{-1} z^{-1} \right) \right) = \tau \left(u^{-1} z^{-1} u \right) = u^{-1} zu = z.$$

Así, obtenemos que $\tau \cdot \rho = \rho^{-1} \cdot \tau$ y $o(\tau \cdot \rho) = 2$. En particular tenemos que $\forall k \in \mathbb{N}$, $\tau\rho^k = \rho^{-k}\tau$. Así, tenemos que $|D_n| = 2n$ y D_n es el conjunto que hemos visto anteriormente. Podemos hacer un par de observaciones:

- Todos los elementos de D_n pueden ser expresados como una potencia de τ por una potencia de ρ.
- No es un grupo abeliano, puesto que $\tau \cdot \rho \neq \rho \cdot \tau$.

Proposición 1.10. Sea G un grupo finito tal que $G = \langle s, t \rangle$, donde s tiene orden 2, t tiene orden n y st tiene orden 2. Entonces, $G \cong D_n$.

Demostración. Como $(st)^2 = e$, tenemos que $st = t^{-1}s$. Así, es fácil ver que $st^k = t^{-k}s$, $\forall k \in \mathbb{N}$. Si repetimos el argumento dado en la construcción del grupo diédrico, tenemos que

$$G = \left\{1, s, t, t^2, \ldots, t^{n-1}, st, \ldots, st^{n-1}\right\} .$$

Consideremos la aplicación $f : D_n \to G : \tau^i\rho^j \to s^i t^j$ para $i \in \{0,1\}$ y $j \in \{0, 1, \ldots, n-1\}$. Se trata de un homomorfismo de grupos puesto que

$$f\left(\left(\tau^i\rho^j\right)\left(\tau^k\rho^m\right)\right) = f\left(\tau^{i+k}\rho^{m-j}\right) = s^{i+k}t^{m-j} = s^i s^k t^{-j} t^m = s^i t^j s^k t^m = f\left(\tau^i\rho^j\right) f\left(\tau^k\rho^m\right).$$

Veamos que es una biyección. Tenemos que

$$\operatorname{Im}(f) = \langle f(\tau), f(\rho) \rangle = \langle s, t \rangle = G.$$

Por tanto, f es sobreyectiva. Como G y D_n tienen el mismo orden, tenemos que f es un isomorfismo y $G \cong D_n$. □

1.4.2. Generadores en grupos de congruencias

Vamos a considerar $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$. Sea

$$\begin{aligned} \cdot : \mathbb{Z}_m \times \mathbb{Z}_m &\to \mathbb{Z}_m \\ ([a]_m, [b]_m) &\to [a \cdot b]_m. \end{aligned}$$

Veamos que la aplicación está bien definida. Supongamos que $[a]_m = [a']_m$ y $[b]_m = [b']_m$. Tenemos que $a - a' = km$ y $b - b' = k'm$ para $k, k' \in \mathbb{Z}$. Así,

$$ab = (km + a')(k'm + b') = kk'm^2 + kb'm + a'k'm + a'b' \Rightarrow ab - a'b' = Cm,\ C \in \mathbb{Z}.$$

Por tanto, $[ab]_m = [a'b']_m$. Consideremos el neutro $[1]_m$. Vamos a estudiar si $(\mathbb{Z}_m / \{[0]_m\}, \cdot, [1]_m)$ es un grupo. Para que lo sea, basta estudiar la propiedad de los inversos y que la operación sea interna. Para que este conjunto sea grupo debe darse que m es primo.

Definición 1.12. Sea $\mathbb{Z}_m$ con $m \in \mathbb{N}$ y vamos a definir las **unidades de** $\mathbb{Z}_m$ como $\mathcal{U}(\mathbb{Z}_m) = \{[a]_m \ : \ \operatorname{mcd}(a, m) = 1\}$.

Observación. El conjunto está bien definido ya que si $[a]_m = [b]_m$, tenemos que $b = a + km$ con $k \in \mathbb{Z}$. Como $\operatorname{mcd}(a, m) = 1$, debe ser que $\operatorname{mcd}(b, m) = 1$.

Lema 1.4. Dado $a \in \mathbb{Z}$, $[a]_m \in \mathcal{U}(\mathbb{Z}_m)$ si y solo si tiene inverso multiplicativo en $\mathbb{Z}_m^*$.

Demostración. **(i)** Supongamos que $[a]_m \in \mathcal{U}(\mathbb{Z}_m)$, por lo que $\operatorname{mcd}(a, m) = 1$. Por la identidad de Bézout, existen $\lambda, \mu \in \mathbb{Z}$ tales que

$$1 = \lambda a + \mu m.$$

Por tanto, tenemos que $[1]_m = [\lambda a]_m = [\lambda]_m [a]_m$. Para ver que $[\lambda]_m$ es el inverso multiplicativo de $[a]_m$ falta ver que $[\lambda]_m \in \mathcal{U}(\mathbb{Z}_m)$. En efecto, tenemos que $\operatorname{mcd}(\lambda, m) \,|1$ por lo que $\operatorname{mcd}(\lambda, m) = 1$ y $[\lambda]_m \in \mathcal{U}(\mathbb{Z}_m)$.

(ii) Supongamos que $[a]_m$ tiene inverso multiplicativo. Entonces, exsite $[b]_m \in \mathbb{Z}_m^*$ tal que $[a]_m \cdot [b]_m = [a \cdot b]_m = [1]_m$. Por tanto, $1 = ab - km$. Sea $d = \operatorname{mcd}(a, m)$, entonces $d|a$ y $d|m$, por lo que $d|1$ y tenemos que $d = 1$. Así, nos queda que $[a]_m \in \mathcal{U}(\mathbb{Z}_n)$.

□

Observación. Los elementos de $\mathcal{U}(\mathbb{Z}_m)$ son los generadores de $\mathbb{Z}_m$. En efecto, si $[a]_m \in \mathcal{U}(\mathbb{Z}_m)$ tenemos que $\operatorname{mcd}(a, m) = 1$, por lo que $o([a]_m) = m$.

Proposición 1.11. El conjunto $(\mathcal{U}(\mathbb{Z}_m), \cdot, [1]_m)$ es un grupo abeliano.

Demostración. **(i)** Veamos que la operación está cerrada. Si $[a]_m, [b]_m \in \mathcal{U}(\mathbb{Z}_m)$ tenemos que si $\operatorname{mcd}(ab, m) > 1$, entonces existe un primo p tal que $p|m$ y $p|ab$, por lo que $p|a$ o $p|b$, que es una contradicción. Por tanto, tenemos que $[ab]_m \in \mathcal{U}(\mathbb{Z}_m)$[a].

(ii) Veamos que se cumple la propiedad asociativa. Está claro que

$$([a]_m \cdot [b]_m)\,[c]_m = [ab]_m \cdot [c]_m = [abc]_m = [a]_m \cdot [bc]_m = [a]_m\,([b]_m \cdot [c]_m)\,.$$

(iii) Está claro que el elemento neutro es $[1]_m$.

(iv) Por lo visto en el lema anterior, los elementos de $\mathcal{U}(\mathbb{Z}_m)$ tienen inversos multiplicativos en $\mathcal{U}(\mathbb{Z}_m)$.

□

[a]Esta parte también se puede demostrar directamente utilizando la identidad de Bézout para a, m y b, m y haciendo el producto de las dos.

Definición 1.13 (Función de Euler). La **función de Euler**, φ, se define como

$$\varphi : \mathbb{N}/\{0\} \to \mathbb{N} : m \to \varphi(m) = |\mathcal{U}(\mathbb{Z}_m)|\,.$$

Es decir, $\varphi(m)$ es el número de generadores de $\mathbb{Z}_m$.

Proposición 1.12. Sea φ la función de Euler.

1. Si p es primo con $p \geq 2$, entonces $\varphi(p) = p - 1$.
2. Si p es primo y $k \geq 2$ entero, entonces $\varphi\left(p^k\right) = (p-1)\,p^{k-1}$. En particular, si $k \geq 3$, $\varphi\left(p^k\right) = \varphi\left(p^{k-1}\right)p$.
3. Si $n, m \in \mathbb{N}$ tales que $\mathrm{mcd}\,(n, m) = 1$, entonces $\varphi(nm) = \varphi(n)\,\varphi(m)$.

Demostración. 1. Es trivial.

2. El grupo $\mathcal{U}\left(\mathbb{Z}_{p^k}\right)$ está formado por las clases $[a]_{p^k} \in \mathbb{Z}_{p^k}$ tales que $\mathrm{mcd}\left(a, p^k\right) = 1$, es decir, $\mathrm{mcd}\,(a, p) = 1$. Por tanto,

$$\mathcal{U}\left(\mathbb{Z}_{p^k}\right) = \mathbb{Z}_{p^k} / \underbrace{\left\{[pi]_{p^k} \;:\; 0 \leq i < p^k\right\}}_{p\mathbb{Z}_{p^k}}.$$

Podemos observar que $p\mathbb{Z}_{p^k} = \left\langle [p]_{p^k} \right\rangle = \left\langle p \cdot [1]_{p^k} \right\rangle$, por lo que tiene orden $\dfrac{p^k}{p} = p^{k-1}$. Por tanto, tenemos que

$$\varphi\left(p^k\right) = p^k - p^{k-1} = (p-1)\,p^{k-1}.$$

Finalmente, está claro que la ecuación $\varphi\left(p^k\right) = \varphi\left(p^{k-1}\right)p$ es trivial para $k = 2$. Si $k > 2$, tenemos que

$$\varphi\left(p^{k-1}\right)p = (p-1)\,p^{k-2}p = (p-1)\,p^{k-1} = \varphi\left(p^k\right).$$

□

Capítulo 2

Cocientes y homomorfismos

Definición 2.1. Sea G un grupo, $H \leq G$ y $a \in G$. Definimos los conjuntos

$$aH = \{ah \ : \ h \in H\}, \quad Ha = \{ha \ : \ h \in H\}.$$

Lema 2.1. Sea G un grupo, $H \leq G$ y $a \in G$. Las aplicaciones

$$f_1 : H \to aH : h \to ah, \quad f_2 : H \to Ha : h \to ha$$

son biyecciones. En particular, si $a \in H$, $aH = Ha = H$.

Demostración. Demostramos sólamente que f_1 es biyección, puesto que la demostración de f_2 es análoga.

- Veamos que f_1 es sobreyectiva. Tenemos que si $x \in aH$, entonces $\exists h \in H$ tal que $x = ah$, por lo que $f_1(h) = x$.
- Para ver que f_1 es inyectiva, supongamos que $f_1(h_1) = f_1(h_2)$, por lo que $ah_1 = ah_2$. Multiplicando por el inverso de a en la izquierda de ambos lados obtenemos que $h_1 = h_2$.

Ahora, si $a \in H$, tenemos que $aH, Ha \subset H$. Sea $h \in H$, por tanto

$$h = \underbrace{a^{-1}(ah)}_{\in aH} = \underbrace{\left(ha^{-1}\right)a}_{\in Ha} \in H.$$

Así, tenemos que $H \subset aH, Ha$, por lo que $H = aH = Ha$. □

Definición 2.2. Sea G un grupo y $H \leq G$. Sean $a, b \in G$ y vamos a definir la relación de equivalencia $\sim_H$:

$$a \sim_H b \iff Ha = Hb.$$

Entonces diremos que a y b son **congruentes por la derecha módulo** H. El **índice** $[G : H]$ de H en G es el número de G módulo H. Es decir,

$$[G : H] := |G/ \sim_H| .$$

Lema 2.2. Sean $a, b \in G$ y $H \leq G$. Entonces $a \sim_H b$ si y solo si $ab^{-1} \in H$.

Demostración. **(i)** Si $a \sim_H b$ tenemos que $Ha = Hb$. Por tanto, $a = e \cdot a \in Hb$, por lo que existe $h \in H$ tal que $a = hb$, así tenemos que $ab^{-1} = h \in H$.

(ii) Si $ab^{-1} \in H$, tenemos que existe $h \in H$ tal que $ab^{-1} = h$ por lo que $a = hb$ y $a \in Hb$. Sea $xa \in Ha$, tenemos que $xa = xhb \in Hb$, por lo que $Ha \subset Hb$. Recíprocamente, tenemos que $b = h^{-1}a$. Tomamos $h' = h^{-1} \in H$. Entonces, si $xb \in Hb$ tenemos que $xb = xh'a \in Ha$, por lo que $Hb \subset Ha$. Así, nos queda que $Ha = Hb$.

□

Observación. Si $a \in G$, tenemos que $[a]_{\sim_H} = Ha$. Lo llamamos la clase de equivalencia de a módulo H o la clase lateral derecha de a por H. En efecto,

$$b \in [a]_m \iff ab^{-1} \in H \iff ba^{-1} \in H \iff b \in Ha.$$

Proposición 2.1 (Fórmula de Lagrange)**.** Sea G un grupo y $H \leq G$. Entonces, $|G| = |G : H| \, |H|$.

Demostración. Sea $[G : H] = k$, entonces sean $a_1, \ldots, a_k$ representantes de las k distintas clases de equivalencia. Así,

$$G = Ha_1 \sqcup \cdots \sqcup Ha_k.$$

Dado que se trata de uniones disjuntas obtenemos que

$$|G| = |Ha_1 \sqcup \cdots \sqcup Ha_k| = \sum_{i=1}^{k} |Ha_i| = \sum_{i=1}^{k} |H| = k\, |H| .$$

La segunda igualdad la hemos obtenido del primer lema del tema. □

Observación. 1. Sea G un grupo finito y $a \in G$. Entonces por la fórmula de Lagrange sabemos que $o(a) \mid |G|$. Basta ver que hemos tomado $H = \langle a \rangle$.

2. Se puede definir la relación de equivalencia también por la izquierda:

$$a \sim^H b \iff aH = bH \iff b^{-1}a \in H.$$

Podemos observar que $\sim_H$ y $\sim^H$ son en general distintos pero $G/ \sim_H$ y $G/ \sim^H$ están en biyección. En efecto, la aplicación $[a]_{\sim_H} \to [a^{-1}]_{\sim^H}$ es una biyección. Así, el índice de un subgrupo no depende de si trabajamos por la izquierda o por la derecha.

Proposición 2.2 (Transitividad del índice). Sean G un grupo finito y $H, K \leq G$ tales que $K \leq H$. Así,

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

Demostración. Sea $m = [G : H]$ y $n = [H : K]$. Sean $a_1, \ldots, a_m$ representantes de las clases de equivalencia de $[G : H]$ y sean $b_1, \ldots, b_n$ representantes de las clases de equivalencia $[H : K]$. Así, tenemos que

$$G = Ha_1 \sqcup \cdots \sqcup Ha_m, \quad H = Kb_1 \sqcup \cdots \sqcup Kb_n.$$

Por tanto, $Ha_i = Kb_1a_i \sqcup \cdots \sqcup Kb_na_i$, $\forall i = 1, \ldots, n$. Así, nos queda que

$$G = \bigsqcup_{i=1}^{m} Ha_i = \bigsqcup_{i=1}^{m} \left(\bigsqcup_{j=1}^{n} Kb_ja_i \right).$$

Así queda demostrado el resultado. □

Corolario 2.1. Sea $K \leq H \leq G$ tales que $[G : K] = p$, con p primo. Entonces o $H = K$ o $H = G$.

Demostración. Tenemos que

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

Hay dos posibles casos:

- Si $[G : H] = p$, entonces $[H : K] = 1$ y $H = K$.
- Si $[H : K] = p$, entonces $[G : H] = 1$ y $H = G$.

□

Corolario 2.2. Sea G un grupo finito.

1. Si $H, K \leq G$ con órdenes coprimos entre ellos, entonces $H \cap K = \{e\}$.
2. Si G tiene orden primo, entonces G es cíclico y está generado por $a \in G/\{e\}$.

Demostración. 1. Sabemos que $H \cap K \leq G, K, H$. Por la fórmula de Lagrange tenemos que $|H \cap K|$ divide a $|H|$ y a $|K|$, pero $\text{mcd}(|H|, |K|) = 1$, por lo que $|K \cap H| = 1$ y necesariamente $H \cap K = \{e\}$.

2. Supongamos que $|G| = p$, con p primo, y $a \in G/\{e\}$. Por la fórmula de Lagrange, sabemos que $o(a)$ divide a $|G|$. Por ser $|G|$ primo, debe ser que $o(a) = p$, por lo que $G = \langle a \rangle$.

□

Teorema 2.1 (Teorema de Euler). Sea $m \geq 1$ un entero natural. Para cada $a \in \mathbb{Z}$ tal que $\operatorname{mcd}(a, m) = 1$ se cumple que $a^{\varphi(m)} \equiv 1 \mod m$, donde $\varphi(m)$ es la función de Euler.

Demostración. Recordamos que $\mathcal{U}(\mathbb{Z}_m)$ son las unidades de $\mathbb{Z}_m$ y $\varphi(m) = |\mathcal{U}(\mathbb{Z}_m)|$. Sea $a \in \mathbb{Z}$ con $[a]_m \in \mathcal{U}(\mathbb{Z}_m)$. Así

$$\left[a^{\varphi(m)}\right]_m = [a]_m^{\varphi(m)} = [1]_m,$$

puesto que $\varphi(m) = |\mathcal{U}(\mathbb{Z}_m)|$ y $o([a]_m) | \varphi(m)$. $\square$

Corolario 2.3 (Pequeño teorema de Fermat). Sea $p \geq 2$ primo y $a \in \mathbb{Z}$ entonces $a^p \equiv a \mod p$ [a].

[a] Para que se cumpla el teorema debe darse que $\operatorname{mcd}(a, p) = 1$.

Demostración. Usando lo anterior, tenemos que

$$a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \mod p \Rightarrow a^p \equiv a \mod p.$$

$\square$

Ejemplo (Grupos de orden 4). Vamos a considerar grupos de orden 4. Sea $G = \{e, a, b, ab\}$. Como $|G| = 4$, el orden de sus elementos es 2 o 4. Podemos considerar varios casos:

- Puede suceder que todos los elementos tengan orden 2. Tendríamos entonces que $G \cong C_2 \times C_2$.
- Puede suceder que exista un elemento de orden 4. Entonces existe otro elemento de orden 4 que es su inverso. Por tanto, el otro elemento que sobra debe tener orden 2. Tendríamos entonces que $C \cong C_4$.

2.1. Subgrupos normales

Definición 2.3. Sea G un grupo, $H \leq G$ y $a \in G$. Definimos el subgrupo $a^{-1}Ha = \left\{a^{-1}ha \ : \ h \in H\right\}$ como el **conjugado** de H por a.

Observación. Comprobemos que verdaderamente $a^{-1}Ha$ es un subgrupo. Está claro que $e \in a^{-1}Ha$, puesto que $e = a^{-1}ea$. Ahora, si $x, y \in H$, existen $h_1, h_2 \in H$ tales que $x = a^{-1}h_1a$ e $y = a^{-1}h_2a$. Así, tenemos que

$$xy^{-1} = \left(a^{-1}h_1a\right)\left(a^{-1}h_2a\right) = a^{-1}h_1h_2a \in a^{-1}Ha.$$

Así, nos queda que $a^{-1}Ha \leq G$.

Observación.

1. Si G es abeliano, tenemos que $a^{-1}ha = h$, por lo que $a^{-1}Ha = H$, $\forall a \in G$.
2. Si $a \in H$, entonces $a^{-1}Ha = H$.

3. $a^{-1}Ha$ y H están en biyección, por tanto si H es finito, el orden de $a^{-1}Ha$ no depende del a escogido.

Definición 2.4 (Subgrupo normal)**.** Sea G un grupo y $H \leq G$. Diremos que H es **subgrupo normal**, $H \lhd G$, si $a^{-1}Ha = H$, $\forall a \in G$.

Observación. 1. Siempre hay subgrupos normales: $\{e\}$ y G.

2. Si G es abeliano, todo subgrupo es normal.

Lema 2.3. Sea $H \leq G$. Son equivalentes:

1. $H \lhd G$.
2. $\forall a \in G$, $\forall h \in H$ tal que $a^{-1}ha \in H$.
3. $aH = Ha$, $\forall a \in G$.

Demostración. **(1) $\Rightarrow$ (2)** Es trivial por la definición.

(2) $\Rightarrow$ (3) Sea $h_1 \in H$ tal que $a^{-1}ha = h_1$. Así, tenemos que $ha = ah_1 \in aH$. Por otro lado, sea $h_2 \in H$ tal que $aha^{-1} = h_2$, por lo que $ah = h_2a \in Ha$.

(3) $\Rightarrow$ (1) Como $aH = Ha$, tenemos que $H = a^{-1}Ha$, $\forall a \in G$ por lo que $H \lhd G$.

$\square$

Proposición 2.3. Sean G_1 y G_2 grupos y f un homomorfismo de grupos.

1. Si $H \lhd G_1$, entonces $f(H) \lhd \operatorname{Im}(f)$.
2. Si $K \lhd \operatorname{Im}(f)$, entonces $f^{-1}(K) \lhd G_1$. En particular, $\operatorname{Ker}(f) \lhd G_1$.

Demostración. 1. Sabemos que si $H \leq G_1$ entonces $f(H) \leq \operatorname{Im}(f)$. Falta ver que es subgrupo normal, es decir, $\forall y \in \operatorname{Im}(f)$, $y^{-1}f(H)y = f(H)$. Sea $y \in \operatorname{Im}(f)$ y $h' \in f(H)$, sea $x \in G_1, h \in H$ tales que $f(x) = y$ y $f(h) = h'$. Tenemos que

$$y^{-1}h'y = f\left(x^{-1}\right) f(h) f(x) = f\left(x^{-1}hx\right) \in f(H).$$

2. Si $K \leq \operatorname{Im}(f)$, entonces $f^{-1}(K) \leq G_1$. Tenemos que ver que $f^{-1}(K) \lhd G_1$, es decir, $\forall x \in G_1$, $x^{-1}f^{-1}(K)x = f^{-1}(K)$. Sea $x \in G_1$, $k \in f^{-1}(K)$, entonces existe $y \in \operatorname{Im}(f)$ y $k' \in K$ tales que $f(x) = y$ y $f(k) = k'$. Así, nos queda que

$$x^{-1}kx = f^{-1}(y)^{-1} f^{-1}(k') f^{-1}(y) = f^{-1}\left(y^{-1}k'y\right) \in f^{-1}(K).$$

$\square$

Ejemplo. Consideremos la aplicación $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$. Tenemos que $\operatorname{Ker}(\det) = \mathrm{SL}_n(\mathbb{R}) \lhd \mathrm{GL}_n(\mathbb{R})$.

Proposición 2.4. Sea G un grupo.

1. Si $H \leq G$ y $[G : H] = 2$, entonces $H \lhd G$.
2. Si $K, H \leq G$ y $H \lhd G$, entonces $HK \leq G$. Además, si $K \lhd G$, $HK \lhd G$.
3. Si $K, H \lhd G$ con $H \cap K = \{e\}$, entonces $\forall k \in K, \forall h \in H$ se tiene que $hk = kh$.

Demostración.

1. Como $[G : H] = 2$, solo existen dos clases de equivalencia, $[e]_{\sim_H}$ y $[a]_{\sim_H}$, con $a \in G/H$. Así, $G = H \sqcup Ha = H \sqcup aH$, por lo que $Ha = aH$ y $H \lhd G$.

2. Es trivial que $e \in HK$. Sean $x, y \in HK$, entonces existen $h_1, h_2 \in H$, $k_1, k_2 \in K$ tales que $x = h_1k_1$ e $y = h_2k_2$. Tenemos que
$$xy^{-1} = (h_1k_1)(h_2k_2)^{-1} = h_1\left(k_1k_2^{-1}\right)h_2^{-1} \in h_1\left(k_1k_2^{-1}\right)H = h_1H\left(k_1k_2^{-1}\right).$$
Así, tenemos que $h_1H\left(k_1k_2^{-1}\right) \subset H\left(k_1k_2^{-1}\right) \subset HK$, por lo que $xy^{-1} \in HK$. Si se cumple también que $K \lhd G$ entonces dados $g \in G$ y $hk \in HK$,
$$g^{-1}(hk)g = \left(g^{-1}hg\right)\left(g^{-1}kg\right) \in HK.$$

3. Tenemos que ver que si $k \in K$ y $h \in H$, entonces $hk = kh$, que es equivalente a ver que $h^{-1}k^{-1}hk = e$. Tenemos que
$$h^{-1}k^{-1}hk = h^{-1}k^{-1}hkh^{-1}h = h^{-1}\left(k^{-1}hkh^{-1}\right)h \in H.$$
$$h^{-1}k^{-1}hk = k^{-1}kh^{-1}k^{-1}hk = k^{-1}\left(kh^{-1}k^{-1}h\right)k \in K.$$
Así, $h^{-1}k^{-1}hk \in H \cap K$, por lo que $h^{-1}k^{-1}hk = e$, que es lo que queríamos demostrar.

□

Observación. Sea G grupo y $H, K \lhd G$ con $H \cap K = \{e\}$, y la aplicación $f : H \times K \to G : (h, k) \to hk$. Entonces f es un homomorfismo inyectivo y $\operatorname{Im}(f) = HK$. Además si H y K son finitos, entonces $|HK| = |H|\,|K|$.

Ejemplo. Tomamos $D_4 = \langle \tau, \rho \rangle = \left\{e, \tau, \rho, \rho^2, \rho^3, \tau\rho, \tau\rho^2, \tau\rho^3\right\}$. Estudiemos los subgrupos de D_4. Sabemos que todos los subgrupos, a excepción de los triviales, van a tener orden dos o cuatro.

- Calculamos los subgrupos de orden 4:
$$H_1 = \langle \rho \rangle,\ H_2 = \left\langle \tau, \rho^3 \right\rangle,\ H_3 = \left\langle \tau\rho, \rho^2 \right\rangle.$$
- Calculamos los subgrupos de orden 2:
$$H_4 = \langle \tau \rangle,\ H_5 = \left\langle \rho^2 \right\rangle,\ H_6 = \langle \tau\rho \rangle,\ H_7 = \left\langle \tau\rho^2 \right\rangle,\ H_8 = \left\langle \tau\rho^3 \right\rangle.$$

Estudiemos cuáles de estos son normales. Por la proposición anterior, tenemos que todos los subgrupos de orden 4 son normales porque su índice es dos. Entre los grupos de orden dos el único normal es H_5. Es fácil ver que el resto no son normales.

Observación. En general si $K \lhd H$ y $H \lhd G$ no implica que $K \lhd G$. Por ejemplo, en D_4 tenemos que $\langle \tau \rangle \lhd \langle \tau, \rho^2 \rangle \lhd D_4$ pero $\langle \tau \rangle$ no es subgrupo normal de D_4.

Definición 2.5 (Grupo simple)**.** Llamamos **grupos simples** a los grupos, G, cuyos únicos subgrupos normales son $\{e\}$ y G.

Ejemplo. El grupo $\mathbb{Z}_p$ con p primo es un grupo simple.

2.2. Grupo cociente

Sea G un grupo y $H \lhd G$. Así, $\forall a \in G$, $aH = Ha$. Entonces $\sim_H$ y $\sim^H$ son las mismas relaciones y escribimos G/H para denotar al conjunto $G/\sim_H = G/\sim^H$. Los elementos de G/H son $[a] = aH$. Vamos a dotar de estructura de grupo a G/H con la operación:

$$\begin{aligned} \cdot : G/H \times G/H &\to G/H \\ ([a]_H, [b]_H) &\to [a \cdot b]_H. \end{aligned}$$

Veamos que la aplicación está bien definida. Sean $[a] = [a_1]$ y $[b] = [b_1]$. Sabemos que $aa_1^{-1} \in H$ y $bb_1^{-1} \in H$ por darse que $H \lhd G$. Tenemos que

$$ab\left(a_1 b_1\right)^{-1} = abb_1^{-1}a_1^{-1} = a\left(bb_1^{-1}\right)a^{-1}aa_1^{-1} = \left(a\left(bb_1^{-1}\right)a^{-1}\right)\left(aa_1^{-1}\right) \in H.$$

Nuevamente hemos utilizado que $H \lhd G$. Así la operación está bien definida.
La operación es asociativa por ser asociativa la operación de G. El elemento neutro es $[e]_H$ y el inverso de un elemento $[a]_H$ es $[a^{-1}]_H$. Así, hemos visto que $(G/H, \cdot)$ tiene estructura de grupo. Diremos que G/H es el **grupo cociente** de G entre H. Su orden será $[G : H] = \dfrac{|G|}{|H|}$.

Ejemplo.

1. La construcción del grupo cociente no es más que la generalización del grupo de las congruencias. En efecto, sea $(\mathbb{Z}, +)$ como grupo G y $H = m\mathbb{Z}$ con $m \in \mathbb{Z}$ por lo que $H \leq G$. Tenemos que $H \lhd G$ puesto que G es abeliano y $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$, que tiene estructura de grupo (con la operación ya vista y las clases de equivalencia módulo m).

2. Sea $G = D_4$ y $H = \langle \rho^2 \rangle \lhd G$. Tenemos que G/H tiene estructura de grupo y $[G : H] = 4$, por lo que $\left|D_4/\rho^2\right| = 4$. Veamos si $G/H \cong C_4$ o $G/H \cong C_2 \times C_2$. Tenemos que $[\tau] \neq [\rho^2]$ ya que $\tau \notin \langle \rho^2 \rangle$. Como $[\tau]^2 = [\tau^2] = [e]$, concluimos que $D_4/\langle \rho^2 \rangle \cong C_2 \times C_2$. En efecto, podemos tomar la aplicación

$$f : D_4 \to \langle \tau \rangle \times \langle \rho^2 \rangle : \tau^i \rho^j \to \left(\tau^i, \rho^{2j}\right).$$

Tenemos que es un homomorfismo de grupos cuyo núcleo es $\operatorname{Ker}(f) = \langle \rho^2 \rangle$.

Proposición 2.5. Sea G un grupo y $H \leq G$. Entonces $H \lhd G$ si y solo si H es el núcleo de un homomorfismo de grupos.

Demostración. **(i)** Sea $H \lhd G$ y consideremos G/H. Vamos a definir la aplicación

$$\pi : G \to G/H : g \to [g].$$

Veamos que $\operatorname{Ker}(\pi) = H$. Primero, demostremos que π es un homomorfismo. Si $x, y \in G$,

$$\pi(xy) = [xy] = [x][y] = \pi(x)\pi(y).$$

Además, sabemos que es sobreyectivo, puesto que si $[y] \in G/H$ basta con tomar $y \in G$ y tendremos que $\pi(y) = [y]$. Ahora, tenemos que

$$x \in \operatorname{Ker}(f) \iff [x] = [e] \iff x \in H.$$

Así, tenemos que $\operatorname{Ker}(\pi) = H$.

(ii) Ya vimos que $\operatorname{Ker}(f) \lhd G$.

□

Observación. El homomorfismo $\pi : G \to G/H$ se le llama **homomorfismo cociente** o **proyección**.

Proposición 2.6. Sea $f : G_1 \to G_2$ un homomorfismo de grupos. Entonces, la siguiente aplicación es una biyección:

$$\phi : \{K \leq G_1 \ : \ \operatorname{Ker}(f) \leq K\} \to \{N \ : \ N \leq \operatorname{Im}(f)\} : H \to f(H).$$

Además, $K \lhd G$ si y solo si $f(K) \lhd \operatorname{Im}(f)$.

Demostración. Veamos que la aplicación está bien definida. Si $H \leq G_1$ tenemos que $f(H) \leq \operatorname{Im}(f)$.
Veamos ahora que la aplicación es inyectiva. Supongamos que existen $K_1, K_2 \in \{K \leq G_1 \ : \ \operatorname{Ker}(f) \leq K\}$ con $\phi(K_1) = \phi(K_2)$. Si tomamos $k_1 \in K_1$, existe $k_2 \in K_2$ con $f(k_1) = f(k_2)$. Así, tenemos que

$$f(k_1) = f(k_2) \iff f(k_1) f(k_2)^{-1} = e \iff f\left(k_1 k_2^{-1}\right) = e \iff k_1 k_2^{-1} \in \operatorname{Ker}(f).$$

Así, tenemos que $k_1 k_2^{-1} \in K_1$, por lo que $x_1 \in K_2$ y $K_1 \subset K_2$. De forma análoga se demuestra que $K_2 \subset K_1$.
Veamos ahora que la aplicación es sobreyectiva. Sea $N_1 \in \{N \ : \ N \leq \operatorname{Im}(f)\}$. Sabemos que $f^{-1}(N_1) \leq G_1$ y $\operatorname{Ker}(f) \leq f^{-1}(N_1)$, por lo que $f^{-1}(N_1) \in \{K \leq G_1 \ : \ \operatorname{Ker}(f) \leq K\}$. Es fácil ver que $f\left(f^{-1}(N_1)\right) = N_1$. El resultado final viene dado por una proposición anterior. □

Observación. Este resultado nos permite establecer una biyección entre el número de subgrupos (normales) de G que contienen a H y los subgrupos (normales) de G/H (con $H \lhd G$).

2.3. Teoremas de isomorfía

Ejemplo. 1. Sea $f_n : (\mathbb{Z}, +) \to (\mathbb{C}^*, \cdot) : k \to e^{\frac{2k\pi i}{n}}$. Tenemos que f_n es un homomorfismo de grupos,

$$f_n(t+k) = e^{\frac{e\pi i}{n}(t+k)} = e^{\frac{2t\pi i}{n}} e^{\frac{2k\pi i}{n}} = f_n(t) f_n(k).$$

Tenemos que $\operatorname{Im}(f_n) = U_n$, que son las raíces n-ésimas de la unidad. Calculemos el núcleo:

$$x \in \operatorname{Ker}(f_n) \iff f_n(x) = 1 \iff e^{\frac{2\pi i}{n}x} = 1 \iff n|x.$$

Así, tenemos que $\operatorname{Ker}(f_n) = n\mathbb{Z}$. Sabemos que $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n \cong U_n = \operatorname{Im}(f_n)$.

2. En D_4 podemos considerar la aplicación anterior $f : D_4 \to C_2 \times C_2$. Recordamos que $\operatorname{Ker}(f) = \langle \rho^2 \rangle$. Así, tenemos que $D_4/\langle \rho^2 \rangle \cong C_2 \times C_2 = \operatorname{Im}(f)$.

Teorema 2.2 (Primer teorema de isomorfía)**.** Sea $f : G_1 \to G_2$ un homomorfismo de grupos. Entonces la aplicación

$$\overline{f} : G_1/\operatorname{Ker}(f) \to \operatorname{Im}(f) : [g] \to \overline{f}([g]) = f(g),$$

es un isomorfismo de grupos. En particular, $G_1/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$.

Demostración. Veamos que está bien definida y que es inyectiva. Dados $x_1, x_2 \in G_1$,

$$\begin{aligned}[x_1] = [x_2] &\iff x_1x_2^{-1} \in \operatorname{Ker}(f) \iff f\left(x_1x_2^{-1}\right) = e \\ &\iff f(x_1)\, f(x_2)^{-1} = e \iff f(x_1) = f(x_2).\end{aligned}$$

Veamos que se trata de un homomorfismo. Si $[g_1], [g_2] \in G_1/\operatorname{Ker}(f)$,

$$\overline{f}([g_1][g_2]) = \overline{f}([g_1g_2]) = f(g_1g_2) = f(g_1)\, f(g_2) = \overline{f}([g_1])\, \overline{f}([g_2]).$$

Veamos que es sobreyectiva. Sea $y \in \operatorname{Im}(f)$, por definición existe $x \in G_1$ tal que $f(x) = y$. Basta con tomar $[x] \in G_1/\operatorname{Ker}(f)$, por lo que $\overline{f}([x]) = f(x) = y$. Así, hemos visto que $\overline{f}$ es un isomorfismo y $G_1/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$. □

Ejemplo. 1. Consideremos $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^* : A \to \det(A)$. Ya vimos que $\operatorname{Ker}(\det) = \mathrm{SL}_n(\mathbb{R})$. Además, $\operatorname{Im}(\det) = \mathbb{R}^*$. Por el teorema anterior, tenemos que $\mathrm{GL}_n(\mathbb{R}) / \mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$.

2. Consideremos $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n : (x, y) \to ([x]_m, [y]_n)$. Tenemos que $\operatorname{Ker}(f) = m\mathbb{Z} \times n\mathbb{Z}$ e $\operatorname{Im}(f) = \mathbb{Z}_m \times \mathbb{Z}_n$. Por el teorema anterior, tenemos que $\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times n\mathbb{Z} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Teorema 2.3 (Segundo teorema de isomorfía)**.** Sea G un grupo y $H, N \leq G$ con $N \lhd G$. Así, $H/H \cap N \cong HN/N$.

Teorema 2.4 (Tercer teorema de isomorfía)**.** Sea G un grupo y $H, N \lhd G$ tal que $N \subset H$. Así, $G/N \cong (G/N) / (H/N)$.

Capítulo 3

Grupos finitos abelianos

Definición 3.1 (Exponente de un grupo)**.** Se define **exponente** de un grupo finito G, $\exp(G)$, como el mínimo común múltiplo de los órdenes de los elementos de G.

Observación. El exponente de un grupo divide al orden del grupo.

Lema 3.1. En un grupo finito abeliano el exponente coincide con el orden del elemento de mayor orden.

Demostración. Sea $a \in G$ de tal forma que a tiene orden máximo, por lo que $o(a) \leq \exp(G)$. Supongamos que $o(a) < \exp(G)$, entonces existe $b \in G$ tal que $o(b) \not| o(a)$, es decir, $b^{o(a)} \neq e$. Así existe un primo p y un $k \geq 1$ tal que $p^k | o(b)$ pero $p^k \not| o(a)$. Escribimos

$$o(a) = p^i m, \ i < k, \ \text{mcd}(m, p) = 1.$$

Tenemos que $m | o(a)$ y $p^k | o(b)$, por tanto existen $x \in \langle a \rangle$ e $y \in \langle b \rangle$ tales que $o(x) = m$ y $o(y) = p^k$. Como el grupo es abeliano x, y conmutan y $\text{mcd}(o(x), o(y)) = 1$, podemos escribir

$$o(xy) = o(x)\, o(y) = m \cdot p^k > o(a).$$

Esto es una contradicción puesto que $o(a)$ era el máximo, por lo que debe ser que $\exp(G) = o(a)$. □

Observación.

1. Dos grupos finitos isomorfos tienen el mismo exponente.
2. Si G no es abeliano no se cumple en general el lema anterior. Por ejemplo, si consideramos D_3, tenemos que $\exp(D_3) = 6$ y todos sus elementos tienen órdenes 2 o 3, por lo que no se cumple el lema.

Lema 3.2. Sea G un grupo finito abeliano. Sea $a \in G$ tal que $o(a) = \exp(G)$. Entonces, existe un subgrupo $K \leq G$ tal que $G \cong \langle a \rangle \times K$.

Demostración. Basta probar la existencia de un subgrupo $K \leq G$ tal que $G = \langle a \rangle \cdot \mathbb{K}$

y $\langle a\rangle \cap K = \{e\}$. Procedemos por inducción en $|G|$, siendo el caso $|G| = 1$ trivial. Sea $H = \langle a\rangle$ y observemos que si $G = H$, el enunciado es trivial. Por tanto, supongamos que $G - H$ es no vacío, y de entre todos sus elementos escogemos un elemento $x \in G - H$ de orden minimal. Es obvio que $x \neq e$.
Veamos que $o(x)$ es primo. Para todo número primo p que sea divisor de $o(x)$ tenemos que $o(x^p) = \dfrac{o(x)}{p} < o(x)$, por el lema anterior. En particular, por minimalidad de $o(x)$ deducimos que $x^p \in H$ y por tanto, como $o(x^p) \,|\, \exp(G) = o(a) = |H|$, deducimos que $\langle x^p\rangle$ es el único subgrupo de H de orden $o(x^p)$. Por otro lado, como $o(x) \,|\, \exp(G) = o(a)$, el lema anterior también implica que $o(a) = o(a^p) \cdot p$, con lo que $o(x^p) \,| o(a^p)$, por lo que $\langle a^p\rangle \leq H$ posee un subgrupo de orden $o(x^p)$. $\square$

Teorema 3.1 (Teorema de caracterización de grupos finitos abelianos)**.** Sea G un grupo finito abeliano. Entonces existe $m_1, \ldots, m_k$ tales que m_i divide a m_{i-1} enteros con $k \geq 1$ natural tal que

$$G \cong \mathbb{Z}_{m_1} \times Z_{m_2} \times \cdots \times \mathbb{Z}_{m_k}.$$

Además, $m_1, \ldots, m_k$ son únicos con esta propiedad.

Definición 3.2 (Coeficientes de torsión)**.** Los números $m_1, \ldots, m_k$ son los **coeficientes de torsión** de G.

Observación. 1. Sabemos que $|G| = m_1 \cdots m_k$.

2. Como $m_i|m_{i-1}$, tenemos que $\exp(G) = m_1$.

Ejemplo. Sea $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2} \times \mathbb{Z}_{5^2} \times \mathbb{Z}_5 \times \mathbb{Z}_2$. Tenemos que $|G| = 2^3 \cdot 5^5$. Queremos expresar G de la forma del teorema anterior. Sabemos que si tienen órdenes coprimos entre ellos, son isomorfos al grupo cíclico que es producto de esos órdenes. Así,

$$G \cong \mathbb{Z}_{5^2 \cdot 2} \times \mathbb{Z}_{5^2 \cdot 2} \times \mathbb{Z}_{5 \cdot 2}.$$

Así, tenemos que los coeficientes de torsión serán $\left(5^2 \cdot 2, 5^2 \cdot 2, 5 \cdot 2\right)$.

Proposición 3.1. Sea G un grupo abeliano finito de orden n. Sea m un divisor de n. Entonces existe un $H \leq G$ con $|H| = m$. En particular, si m es primo, entonces existe en G un elemento de orden m.

Demostración. Como G es un grupo abeliano finito, existen $m_1, \ldots, m_k \in \mathbb{N}$ tales que $G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$. Sabemos que $n = m_1 \cdots m_k$. Como $m|n$, entonces existen $n_1, \ldots, n_k \in \mathbb{N}$ con $n_i|m_i$, $\forall i = 1, \ldots, k$ tal que $m = n_1 \cdots n_k$. Por ser $(\mathbb{Z}, +)$ cíclico, tenemos que para cada i existe $H_i \leq \mathbb{Z}_{m_i}$ de orden n_i. Así, tenemos que existe $H \leq G$ con $H \cong H_{n_1} \times \cdots \times H_{n_k}$ donde $H_{n_i} \leq \mathbb{Z}_{n_i}$. Además obtenemos que $|H| = n_1 \cdots n_k = m$. $\square$

Ejemplo. Vamos a construir, dado un orden n, los distintos grupos finitos abelianos de ese orden.

1. Consideremos $n = 24$. Podemos considerar varios casos:

   Caso 1. Consideremos que $m_1 = 24$, tenemos que $G \cong \mathbb{Z}_{24}$.

Caso 2. Consideremos que $m_1 = 12$, por lo que $m_2 = 2$. Así, tenemos que $G \cong \mathbb{Z}_{12} \times \mathbb{Z}_2$.

Caso 3. Consideremos que $m_1 = 8$, por lo que $m_2 = 3$. Así, tendríamos que $m_2 = 3$, pero esto no puede ser porque $\operatorname{mcd}(8, 3) = 1$ y 3 no divide a 8. Por tanto, $G \cong \mathbb{Z}_{24}$.

Caso 4. Consideremos que $m_1 = 6$. No podemos tomar $m_2 = 4$ porque 4 no divide a 6. Así, nos queda que la única posibilidad es que $m_2 = m_3 = 2$. Así, $G \cong \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Caso 5. Si consideramos $m_1 = 3$, o $m_1 = 2$, volvemos a los casos anteriores.

2. Consideremos $n = 196 = 2^2 \cdot 7^2$.

Caso 1. Consideremos $m_1 = 196$, por lo que $G \cong \mathbb{Z}_{196}$.

Caso 2. Consideremos $m_1 = 98$, por lo que necesariamente $m_2 = 2$ y tenemos que $G \cong \mathbb{Z}_{98} \times \mathbb{Z}_2$.

Caso 3. Consideremos $m_1 = 28$, por lo que necesariamente $m_2 = 7$ y tenemos que $G \cong \mathbb{Z}_{28} \times \mathbb{Z}_7$.

Caso 4. Consideremos $m_1 = 14$, por lo que necesariamente debe ser que $m_2 = 14$ y tenemos que $G \cong \mathbb{Z}_{14} \times \mathbb{Z}_{14}$.

Observación. Para agilizar los cálculos podemos darnos cuenta de que en el m_1 deben estar contenidos todos los factores primos de n.

Observación. Sea G un grupo finito y $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, donde p_i es primo y $\alpha_i \in \mathbb{N}$. Si considero las distintas descomposiciones de α_i, en el sentido de cuántas maneras tengo de expresar α_i como suma de naturales más el cero, es decir,

$$\alpha_i = j_{i_1} + \cdots + j_{i_s}, \; j_{i_t} \in \mathbb{N} \cup \{0\}, \; i_t \in \mathbb{N},$$

entonces el número de grupos abelianos finitos de orden $|G|$ es el producto de las cantidad de descomposiciones de cada α_i.

Teorema 3.2. Sea G un grupo finito abeliano no trivial de orden $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, con p_i primos y $\alpha_i \geq 1$, $\forall i = 1, \ldots, s$. Para cada primo p_i existe un subgrupo G_i de G tal que

$$G \cong G_1 \times \cdots \times G_s,$$

y cada G_i es isomorfo a $\mathbb{Z}_{j_{i,1}} \times \cdots \times \mathbb{Z}_{j_{i,r_i}}$, donde $j_{i,1} \geq \cdots \geq j_{i,r_i}$ y $j_{i,1} + \cdots + j_{i,r_i} = \alpha_i$.

Demostración. Por la proposición anterior, existe subgrupos G_i de orden p^{α_i}. Como consecuencia de la fórmula de Lagrange tenemos que

$$G_i \cap \prod_{j \neq i} G_j = \{e\},$$

para cada i, por lo que se verifica que $G \cong G_1 \times \cdots \times G_s$. Finalmente, por el Teorema de Caracterización tenemos que cada G_i cumple la propiedad deseada. $\square$

Ejemplo. 1. Tomemos $n = 24 = 3 \cdot 2^2$. Entonces, $\alpha_1 = 1 + 0$, solo lo podemos expresar de esta forma; y $\alpha_2 = 3 = 3 + 0 = 2 + 1 = 1 + 1 + 1$, que se puede expresar de estas tres formas. Por tanto, hay $1 \cdot 3$ grupos finitos abelianos de orden 24. Nos salen los siguientes grupos:

$$\mathbb{Z}_3 \times \mathbb{Z}_{2^3} \cong \mathbb{Z}_{24}$$
$$\mathbb{Z}_3 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \cong \mathbb{Z}_{12} \times \mathbb{Z}_2$$
$$\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

2. Tomemos $n = 196 = 2^2 \cdot 7^2$. Tenemos que

$$\alpha_1 = \alpha_2 = 2 = 2 + 0 = 1 + 1.$$

Así, tenemos $2 \cdot 2 = 4$ posibles grupos.

3. Tomemos $n = 3969 = 7^2 \cdot 3^4$. Calculemos el número de grupos que nos tienen que salir:

$$\alpha_1 = 2 = 2 + 0 = 1 + 1$$
$$\alpha_2 = 4 = 4 + 0 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1.$$

Así, hay $2 \cdot 5 = 10$ grupos abelianos finitos. Tenemos que m_1 es múltiplo de $7 \cdot 3 = 21$.

Caso 1. Supongamos que $m_1 = 21$. Tenemos que $m_2 | m_1$, por lo que debe ser que $m_2 = 7 \cdot 3$. Similarmente, como $m_3 | m_2$, debe ser que $m_3 = m_4 = 3$. Así, $G \cong \mathbb{Z}_{21} \times \mathbb{Z}_{21} \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

Caso 2. Consideremos que $m_1 = 21 \cdot 3$. Tenemos que hay dos opciones para m_2. La primera es considerar $G \cong \mathbb{Z}_{63} \times \mathbb{Z}_{63}$. La otra es coger $G \cong \mathbb{Z}_{63} \times \mathbb{Z}_{21} \times \mathbb{Z}_3$.

Caso 3. Consideremos $m_1 = 147 = 7^2 \cdot 3$. En este caso, solo tenemos la opción $G \cong \mathbb{Z}_{147} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

Caso 4. Consideremos $m_1 = 189 = 7 \cdot 3^3$. Entonces, necesariamente $G \cong \mathbb{Z}_{189} \times \mathbb{Z}_{21}$.

Caso 5. Consideremos $m_1 = 441 = 7^2 \cdot 3^2$. En este caso tenemos las opciones $G \cong \mathbb{Z}_{441} \times \mathbb{Z}_3 \times \mathbb{Z}_3$ y $G \cong \mathbb{Z}_{441} \times \mathbb{Z}_9$.

Caso 6. Consideremos $m_1 = 567 = 7 \cdot 3^4$, entonces tenemos que $G \cong \mathbb{Z}_{567} \times \mathbb{Z}_7$.

Caso 7. Consideremos $m_1 = 1323 = 7^2 \times 3^3$, entonces tenemos que $G \cong \mathbb{Z}_{1323} \times \mathbb{Z}_3$.

Caso 8. Consideremos $m_1 = 3969$, por lo que $G \cong \mathbb{Z}_{3969}$.

Capítulo 4

Grupos de permutaciones

Sea $f : G \to G'$ una biyección. Consideramos la aplicación $\text{Biy}(G) \to \text{Biy}(G') : \sigma \to f^{-1}\sigma f$, que es un isomorfismo de grupos. Vamos a considerar un conjunto finito de elementos al que llamaremos $X_n = \{1, 2, \ldots, n\}$ y $\text{Biy}(X_n)$, para $n \geq 1$.

Definición 4.1 (Grupo de permutaciones). El **grupo de permutaciones** de n elementos, o el **n-ésimo grupo de permutaciones**, es el grupo $\mathcal{S}_n = \text{Biy}(X_n)$ con la composición de funciones, donde $\tau \cdot \sigma = \sigma \circ \tau$.

Observación. El orden de $\mathcal{S}_n$ es $n!$.

Notación. Dado $\mathcal{S}_n$ grupo de permutaciones, si $\sigma \in \mathcal{S}_n$ entonces podemos expresar σ de la forma

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

Ejemplo. Dado $\sigma \in \mathcal{S}_4$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (3, 2).$$

Similarmente, dado $\sigma \in \mathcal{S}_6$

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

Esta última notación es la que utilizaremos con más frecuencia.

Ejemplo. Consideremos $\sigma, \tau \in \mathcal{S}_4$ tales que $\sigma = (1, 2, 3)$ y $\tau = (3, 4)(1, 2)$. Tenemos que

$$\sigma \cdot \tau = \tau \circ \sigma = (3, 4)(1, 2)(1, 2, 3) = (2, 4, 3).$$

$$\tau \cdot \sigma = \sigma \circ \tau = (1, 2, 3)(3, 4)(1, 2) = (1, 3, 4).$$

Ejemplo. Calculemos algunos grupos de permutación.

- Tenemos que $\mathcal{S}_2 = \{id, (1, 2)\}$.
- Tenemos que $\mathcal{S}_3 = \{id, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$. Podemos ver que $\mathcal{S}_3 \cong D_3$.

Teorema 4.1 (Teorema de Cayley)**.** Todo grupo finito es isomorfo a un subgrupo de un grupo de permutaciones.

Demostración. Sea G un grupo finito y $g \in G$. Consideremos la aplicación $\tilde{g} : G \to G : x \to x \cdot g$. Es fácil ver que $\tilde{g} \in \text{Biy}\,(G)$. Ahora, consideremos $\phi : G \to \text{Biy}\,(G) : g \to \tilde{g}$. Veamos que ϕ es un homomorfismo de grupos:

$$\phi\,(gh)\,(x) = \widetilde{gh}\,(x) = x \cdot (gh) = \tilde{g}\,(x)\,h = \tilde{h}\,(\tilde{g}\,(x)) = \tilde{g} \cdot \tilde{h}\,(x)\,.$$

Ahora, veamos que es inyectiva. Si $g \in \text{Ker}\,(\phi)$, tenemos que $\tilde{g} = id$, es decir, $\forall x \in G$,

$$g\,(x) = x \cdot g = e.$$

Así, tenemos que $\text{Ker}\,(\phi) = \{e\}$, por lo que ϕ es inyectiva. Así, tenemos que $G \cong \text{Im}\,(\phi) \leq \text{Biy}\,(G) = \mathcal{S}_{|G|}$. □

Definición 4.2 (Soporte)**.** Sea $\sigma \in \mathcal{S}_n$. Llamamos **soporte** de σ al conjunto $\text{sop}\,(\sigma) = \{a \in X_n \ : \ \sigma\,(a) \neq a\}$. Diremos que $\sigma, \tau \in \mathcal{S}_n$ son **disjuntos** si $sop\,(\sigma) \cap \text{sop}\,(\tau) = \emptyset$.

Ejemplo. Consideremos $\sigma, \tau \in \mathcal{S}_6$ tales que

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 5 & 2 & 6 \end{pmatrix} = (2, 3, 4, 5)\,, \quad \tau = (1, 6)\,.$$

Tenemos que $\text{sop}\,(\sigma) = \{2, 3, 4, 5\}$ y $\text{sop}\,(\tau) = \{1, 6\}$, por lo que τ y σ son disjuntos. Podemos ver que la notación de los ciclos nos facilita mucho el cálculo del soporte.

Observación.

1. $\text{sop}\,(\sigma) = \emptyset$ si y solo si $\sigma = id$.
2. $\text{sop}\,(\sigma) = \text{sop}\left(\sigma^{-1}\right)$. En efecto, si $a \in \text{sop}\,(\sigma)$, tenemos que $a \neq \sigma\,(a)$, por lo que $\sigma^{-1}\,(a) \neq a$ y $a \in \text{sop}\left(\sigma^{-1}\right)$. El recíproco es análogo.
3. $m \geq 2$, $\text{sop}\,(\sigma^m) \subset \text{sop}\,(\sigma)$. En efecto, si $a \notin \text{sop}\,(\sigma)$ tenemos que $a = \sigma\,(a)$, por lo que $a = \sigma^m\,(a)$ y $a \notin \text{sop}\,(\sigma^m)$.

Lema 4.1. Sean $\sigma, \tau \in \mathcal{S}_n$ dos permutaciones disjuntas.

1. $\sigma \cdot \tau = \tau \cdot \sigma$.
2. $\forall m \in \mathbb{N}$, se tiene que $(\sigma \cdot \tau)^m = id$ si y solo si $\sigma^m = \tau^m = id$.

Demostración. Supongamos que $\text{sop}\,(\sigma) \cap \text{sop}\,(\tau) = \emptyset$.

1. Si $x \notin \text{sop}\,(\sigma) \cup \text{sop}\,(\tau)$ tenemos que $\sigma\,(x) = x$ y $\tau\,(x) = x$, por lo que

   $$\sigma\,(\tau x) = \sigma\,(x) = \tau\,(x) = \tau\,(\sigma\,(x))\,.$$

   Ahora, supongamos sin pérdida de generalidad que $x \in \text{sop}\,(\sigma)$. Como σ y τ son disjuntos, debe ser que $x \notin \text{sop}\,(\tau)$, es decir, $\tau\,(x) = x$. Por otro lado, tenemos que $\sigma(x) \in \operatorname{sop}(\sigma)$ y en consecuencia $\sigma(x) \notin \operatorname{sop}(\tau)$. Así, podemos concluir que

$$\sigma(\tau(x)) = \sigma(x) = \tau(\sigma(x)).$$

2. La segunda implicación es trivial. Supongamos que $(\sigma \cdot \tau)^m = id$, es decir, $\sigma^m = (\tau^m)^{-1}$. Así, nos queda que

$$\operatorname{sop}(\sigma) \supset \operatorname{sop}(\sigma^m) = \operatorname{sop}(\tau^m) \subset \operatorname{sop}(\tau).$$

Así, por ser σ y τ disjuntos tenemos que $\operatorname{sop}(\sigma^m) = \operatorname{sop}(\tau^m) = \emptyset$, por lo que $\sigma^m = \tau^m = id$.

□

Observación. Tenemos que $\mathcal{S}_2 \cong C_2$. Para $n \geq 3$, tenemos que $Z(\mathcal{S}_n) = \{id\}$.

4.1. Ciclos

Definición 4.3 (Ciclo). Sea $\sigma \in \mathcal{S}_n$. Diremos que σ es un k**-ciclo** o **ciclo de orden** k si dados $i_1, \ldots, i_k \in X_n$, tenemos que $\sigma(i_j) = i_{j+1}$ (con $\sigma(i_k) = i_1$) y para el resto $i_{k+1}, \ldots, i_n \in X_n$ se tiene que $\sigma(i_t) = i_t$. Lo escribimos $(i_1, \ldots, i_k)$.

Ejemplo.

1. En $\mathcal{S}_4$ podemos considerar el 3-ciclo $(1,2,3)$ y el 4-ciclo $(1,4,2,3)$.
2. En $\mathcal{S}_3$ podemos considerar $\sigma = (1,3,2)$. Tenemos que $\sigma^{-1} = (2,3,1)$. En efecto, tenemos que
$$\sigma \circ \sigma^{-1} = (1,3,2)(2,3,1) = (1)(2)(3).$$
3. Considerando nuevamente en $\mathcal{S}_4$ el ciclo $(1,2,3)$, tenemos que
$$(1,2,3) = (2,3,1) = (3,1,2).$$

Proposición 4.1. Sea $2 \leq k \leq n$.

1. Si $l \leq k$, tenemos que $(i_1, \ldots, i_k) = (i_l, i_{l+1}, \ldots, i_k, i_1, \ldots, i_{l-1})$.
2. El inverso de $(i_1, i_2, \ldots, i_k)$ es $(i_k, i_{k-1}, \ldots, i_2, i_1)$.
3. Todo k-ciclo tiene orden k.
4. Si $\sigma \in \mathcal{S}_n$ es un k-ciclo, entonces $\sigma = \left(i, \sigma(i), \ldots, \sigma^{k-1}(i)\right)$, $\forall i \in \operatorname{sop}(\sigma)$. Además $k = |\operatorname{sop}(\sigma)|$.

Demostración. Consideremos $2 \leq k \leq n$.

1. Es trivial a partir de la definición.
2. Basta con comprobar que su composición es la identidad:
$$(i_1, i_2, \ldots, i_k)(i_k, i_{k-1}, \ldots, i_1) = (i_1) \cdots (i_k) = id.$$

Comprobar la otra composición es análogo.

3. Si tomamos $\sigma = (i_1, \ldots, i_k)$ y $l \leq k$, tenemos que $\sigma^l(i_1) = i_{l+1}$. Como buscamos la identidad, necesitamos que $i_{l+1} = i_1$, que solo ocurre cuando $l = k$. No hay un menor elemento que lo cumpla.

4. Se deduce de **(1)** y **(3)** por como están construidos.

$\square$

Proposición 4.2 (Descomposición en ciclos disjuntos)**.** Todo $\sigma \in \mathcal{S}_n$ se puede descomponer como producto de ciclos disjuntos dos a dos tal que $\sigma = \sigma_1 \cdots \sigma_k$.

Demostración. Sea $\sigma \in \mathcal{S}_n$ y vamos a considerar la siguiente relación de equivalencia:

$$x \sim y \iff \exists s \in \mathbb{N},\ \sigma^s(x) = y \iff \exists \tau \in \langle \sigma \rangle, \tau(x) = y.$$

Esta relación de equivalencia genera una partición de X_n. Consideremos $\{j_1, \ldots, j_t\}$ representantes de las clases de equivalencia con más de un elemento y llamamos O_i a la clase de equivalencia de j_i. Para cada $1 \leq i \leq t$, definimos $\sigma_i : X_i \to X_i$ tal que

$$\sigma_i(x) = \begin{cases} \sigma(x), \ x \in O_i \\ x, \ x \notin O_i \end{cases}.$$

Así, tenemos que $\sigma_i = \left(j_i, \sigma(j_i), \ldots, \sigma^{s-1}(j_i)\right)$ es un s-ciclo donde $\operatorname{sop}(\sigma_i) = O_i$. Como $O_i \cap O_j = \emptyset$ si $i \neq j$, tenemos que $\operatorname{sop}(\sigma_i) \cap \operatorname{sop}(\sigma_2) = \emptyset$, $\forall i, j \in \{1, \ldots, t\}$ con $i \neq j$. Así, tenemos que

$$\operatorname{sop}(\sigma) = \bigsqcup_{i=1}^{t} \operatorname{sop}(\sigma_i) \Rightarrow \sigma = \sigma_1 \cdots \sigma_t.$$

$\square$

Ejemplo. Tenemos que

$$(1,4,2,3) = (1,2,3,4)(1,3,4).$$

Proposición 4.3. Sea $\sigma \in \mathcal{S}_n$ con $\sigma = \sigma_1 \cdots \sigma_k$ ciclos disjuntos. Entonces, $o(\sigma) = \operatorname{mcm}(o(\sigma_1), \ldots, o(\sigma_k))$.

Demostración. Por ser $\sigma_1, \ldots, \sigma_k$ disjuntos tenemos que para cualquier $m \in \mathbb{Z}$,

$$\sigma^m = \sigma_1^m \cdots \sigma_k^m.$$

Además, hemos visto que $\sigma^m = id$ si y solo si $\sigma_i^m = id$, $\forall i = 1, \ldots, k$. Por tanto, necesitamos que $o(\sigma_1) | m$, $\forall i = 1, \ldots, k$, por lo que claramente debe ser que $\operatorname{mcm}(o(\sigma_1), \ldots, o(\sigma_k)) | m$, por lo que

$$o(\sigma) = \operatorname{mcm}(o(\sigma_1), \ldots, o(\sigma_k)).$$

□

Definición 4.4 (Trasposiciones)**.** A los 2-ciclos los llamamos **trasposiciones**.

Corolario 4.1. Sea $\sigma \in \mathcal{S}_n$. Entonces, podemos escribir σ como producto de 2-ciclos.

Demostración. Si $\sigma \in \mathcal{S}_n$, sabemos que $\sigma = \sigma_1 \cdots \sigma_k$ ciclos disjuntos. Está claro que cualquier n-ciclo lo podemos expresar como

$$(i_1, \ldots, i_n) = (i_1, i_n)\,(i_n, i_2) \cdots (i_{n-1}, i_n)\,.$$

Así, cada n-ciclo es producto de trasposiciones y σ lo es. □