

Estructuras Algebraicas

Victoria Torroja Rubio

8/9/2025

Índice general

| | |
|--|---------------|
| 0. Preliminares | 4 |
| 0.1. Divisibilidad | 4 |
| 0.2. Factorización | 7 |
| 0.3. Aritmética modular | 8 |
| I Grupos | 9 |
| 1. Generalidades de grupos | 10 |
| 1.1. Subgrupos | 12 |
| 1.2. Homomorfismos | 14 |
| 1.3. Grupos cíclicos | 16 |
| 1.4. Grupos finitamente generados | 22 |
| 1.4.1. Grupo diédrico D_n | 23 |
| 1.4.2. Generadores en grupos de congruencias | 25 |
| 2. Cocientes y homomorfismos | 27 |
| 2.1. Subgrupos normales | 30 |
| 2.2. Grupo cociente | 33 |
| 2.3. Teoremas de isomorfía | 34 |
| 3. Grupos finitos abelianos | 36 |
| 4. Grupos de permutaciones | 40 |
| 4.1. Ciclos | 42 |
| 4.2. Conjugación | 45 |
| 4.3. Subgrupo alternado | 46 |
| 5. Acciones de grupos | 49 |
| II Anillos | 53 |
| 6. Generalidades de Anillos | 54 |
| 6.0.1. Enteros de Gauss | 58 |
| 6.0.2. Anillo de polinomios | 58 |
| 6.1. Ideales | 60 |

| | |
|---|----|
| 6.1.1. Construcción del anillo cociente | 60 |
| 6.2. Homomorfismos de anillos | 63 |

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 $\mathbb{N} = \{1, 2, \dots\}$ es el conjunto de los **números naturales** y $\mathbb{Z} = \{\dots, -1, -1, 0, 1, 2, \dots\}$ 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 buen orden, por lo que existe un elemento mínimo r . Así, tenemos que existe $q \in \mathbb{Z}$ tal que

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

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 , $\text{mcd}(n, m)$ 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 $d = \text{mcd}(a, b)$ 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 $d = \text{mcd}(a, b)$. 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 $d|b$. 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 $d = \text{mcd}(a, b)$. □

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 $\text{mcd}(a, b) = \text{mcd}(b, r)$.

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

do, tenemos que $\text{mcd}(b, r) \mid a$, 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 $b \mid a$ 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 $a \mid bc \Rightarrow a \mid b \vee a \mid c$.
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 $a \mid bc$ 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 $p_1, \dots, p_k \in \mathbb{Z}$ y $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ tales que $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

^aSi $n < 0$ 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 $i = 1, \dots, s$ con $s < t, k$, tenemos que

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

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 $k \in \mathbb{Z}$, $a \equiv m \pmod{n}$.

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

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

$$a_1 + a_2 \equiv m_1 + m_2 \pmod{n}.$$

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

$$ba_1 \equiv bm_1 \pmod{n}.$$

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

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

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

Parte I

Grupos

Capítulo 1

Generalidades de grupos

Definición 1.1 (Grupo). Sea la terna (G, \cdot, e) donde G es un conjunto no vacío, $\cdot : G \times G \rightarrow G$ 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. $(\mathbb{R}/\{0\}, \cdot, 1)$ es un grupo abeliano.
3. $(\mathbb{Z}, +, 0)$ es un grupo abeliano.
4. $(\mathbb{N} \cup \{0\}, +, 0)$ 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 sólo 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. $\forall a \in G, (a^{-1})^{-1} = a$.
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 $(a^{-1})^{-1} = a$. Ahora demostramos **2**. Si $a, b \in G$,

$$(ab)(b^{-1}a^{-1}) = aeb^{-1} = aa^{-1} = e.$$

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 $\text{Biy}(X) = \{f : X \rightarrow X : f \text{ biyección}\}$. 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 $ab = a(b^{-1})^{-1} \in H$. 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:

$$\begin{aligned} \cdot : (G_1 \times G_2) \times (G_1 \times G_2) &\rightarrow G_1 \times G_2 \\ (g_1, g_2) \times (g'_1, g'_2) &\rightarrow (g_1 \cdot_{G_1} g'_1, g_2 \cdot_{G_2} g'_2). \end{aligned}$$

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

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

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 $(g_1^{-1}, g_2^{-1}) \in G_1 \times G_2$. En efecto,

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

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 $Z(G) = \bigcap_{x \in G} C_G(x)$. En efecto:

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

(ii) Si $x \in \bigcap_{g \in G} C_G(g)$, $x \in C_G(g)$, $\forall g \in G$. 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, $f : G_1 \rightarrow G_2$ 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 $f_1 : G_1 \rightarrow G_2$ y $f_2 : G_2 \rightarrow G_3$ 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

$$f : \mathbb{R}/\{0\} \rightarrow \text{GL}_n(\mathbb{R})$$

$$t \rightarrow \begin{pmatrix} t & 0 & \cdots & 0 \\ 0 & t & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t \end{pmatrix} = t \cdot I_n.$$

Esta aplicación es un homomorfismo de grupos.

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

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

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

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

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

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

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

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

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

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

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

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 $f(ab^{-1}) \in f(H)$. Así,

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

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

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

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

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 $a \in \text{Ker}(f)$. Entonces, tenemos que $f(a) = f(e_{G_1}) = e_{G_2}$, por lo que $a = e_{G_1}$ y $\text{Ker}(f) = \{e_{G_1}\}$.

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,

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

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 $x \in \text{Ker}(f)$, tenemos que $f(x) = e_{G_2} \in N$, por lo que $x \in f^{-1}(N)$ y consecuentemente $\text{Ker}(f) \leq f^{-1}(N)$. □

Ejemplo. 1. Consideremos $f_m : \mathbb{Z} \rightarrow \mathbb{Z}$ 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 $\text{Ker}(f_m)$ es el subgrupo trivial si $m \neq 0$ y es \mathbb{Z} si $m = 0$.

2. Es homomorfismo la aplicación $\det : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}/\{0\} : M \rightarrow \det(M)$. En concreto, se trata de un homomorfismo sobreyectivo. Además, podemos ver que $\text{Ker}(\det) = \text{SL}_n(\mathbb{R})$.

Definición 1.7 (Isomorfismo y automorfismo). Sea $f : G_1 \rightarrow G_2$ un homomorfismo de grupos. Si f es biyectiva, entonces f es un **isomorfismo** y lo escribimos $G_1 \cong G_2$. Si $f : G_1 \rightarrow G_1$ 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 $f : G_1 \rightarrow G_2$ es un isomorfismo, tenemos que $f^{-1} : G_2 \rightarrow G_1$ 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 $f : G_1 \rightarrow G_2$ es un homomorfismo sobreyectivo, tenemos que $f(G_1) \cong G_2$, es decir, $\text{Im}(f) \cong G_2$.
4. Si $f : G_1 \rightarrow G_2$ es un homomorfismo inyectivo, entonces $G_1 \cong \text{Im}(f)$.
5. La relación de ser isomorfo es una relación de equivalencia.
6. El conjunto de automorfismos de G , $\text{Aut}(G)$, es un subgrupo de $\text{Biy}(G)$.

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 $(a^{-1})^k = a^{-k} = (a^k)^{-1}$.

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

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

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

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

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 $(a^k)^{-1} = (a^{-1})^k$. \square

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

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

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

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

\square

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

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

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

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

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

Dado que $a^l, (a^k)^q \in H$, 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 $x = a^l = (a^k)^q \in H$. 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 $x = (a^k)^n \in H$. Así, tenemos que $\langle a^k \rangle \subset H$.

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

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. \square

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 $k = 0, \dots, n-1$. Es sencillo ver que $(U_n, \cdot, 1) \leq (\mathbb{C}/\{0\}, \cdot, 1)$. 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 $U_n = \langle e^{i\frac{2\pi}{n}} \rangle$.

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

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

Vamos a ver que esta 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

$$x+y = a+\lambda m+b+\mu m = (a+b)+(\lambda+\mu)m \iff x+y \equiv a+b \pmod{m} \iff [x+y]_m = [a+b]_m.$$

Queremos ver ahora que $(\mathbb{Z}_m, +, [0]_m)$ 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 $m = \min \{k \in \mathbb{N} : a^k = e\}$ tenemos que $G = \langle a \rangle = \{e, a, \dots, a^{m-1}\}$. Además, $a^k = e$ si y solo si $m|k$.

Demostración. (i) Sea $a^k \neq e, \forall k \in \mathbb{N}$. Entonces, $a^k \neq e, \forall \mathbb{Z} \setminus \{0\}$, 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 $m = \min \{k \in \mathbb{N} : a^k = e\}$. Vamos a ver que $G = \langle a \rangle = \{e, a, \dots, a^{m-1}\}$. Es trivial que $\{e, a, \dots, a^{m-1}\} \subset G$. Recíprocamente, si $g \in G$, tenemos que existe $l \in \mathbb{Z} \setminus \{0\}$ tal que $g = a^l$. Por el algoritmo de la división, tenemos que existen $q, r \in \mathbb{Z}$ tales que

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

Así, tenemos que

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

Así, como $0 \leq r < m$, debe ser que $g \in \{e, a, \dots, a^{m-1}\}$, por lo que $G \subset \{e, a, \dots, a^{m-1}\}$. Consecuentemente, $G = \{e, a, \dots, a^{m-1}\}$.

Finalmente, como $l = qm + r$, es trivial que $a^l = e \iff r = 0$. □

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

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

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

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

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

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

Ahora vamos a ver que es biyectiva.

Inyectiva. Si $|G| > k \geq t$ y $f(a^k) = f(a^t)$, tenemos que $f(a^{k-t}) = b^{k-t} = e$. 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 $k = 0, \dots, |H| - 1$, tenemos que $f(a^k) = b^k = c$.

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

$$o(a) = m = \min \{k \in \mathbb{N} : a^k = e\}.$$

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 $f : G \rightarrow H$ un homomorfismo y sea $x \in G$. Entonces $o(f(x)) | o(x)$. En efecto, tenemos que

$$f(x)^{o(x)} = f(x^{o(x)}) = f(e_G) = e_H \iff o(f(x)) | o(x).$$

Además, si $f : G \rightarrow H$ es isomorfismo, entonces sabemos que existe $f^{-1} : H \rightarrow G$ 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

$$(a, b)^4 = (a^4, b^4) = (e_{C_2}, e_{C_4}) \in C_2 \times C_4.$$

Tenemos que $C_8 = \{e, a, \dots, a^{n-1}\}$ y

$$C_2 \times C_4 = \{(e, e), (e, b), (e, b^2), (e, b^3), (c, e), (c, b), (c, b^2), (c, b^3)\}.$$

2. Tomemos los grupos $(\mathbb{C}, +, 0)$ y $(\mathbb{C}/\{0\}, \cdot, 1)$. Supongamos que existe un homomorfismo de grupos, $f : \mathbb{C}/\{0\} \rightarrow \mathbb{C}$. 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. $o(a) = o(a^{-1})$.
2. $\forall k \in \mathbb{N}$, si $\text{mcd}(o(a), k) = 1$, entonces $o(a^k) = o(a)$. En general,

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

3. Si $b \in G$ con $o(b)$ finito tal que $ab = ba$ y $\text{mcd}(o(a), o(b)) = 1$, entonces $o(ab) = o(a)o(b)$.

Demostración. 1. Como $\langle a \rangle = \langle a^{-1} \rangle$, tenemos que

$$o(a) = |\langle a \rangle| = |\langle a^{-1} \rangle| = o(a^{-1}).$$

2. Fijemos $k \in \mathbb{N}$. Sea $r \geq 1$ con $r \in \mathbb{N}$, entonces tenemos que

$$\begin{aligned} a^{kr} = e &\iff o(a) \mid kr \iff o(a) \mid \text{mcd}(o(a)r, kr) \\ &\iff o(a) \mid r \cdot \text{mcd}(o(a), k) \iff \frac{o(a)}{\text{mcd}(o(a), k)} \mid r. \end{aligned}$$

Así, tenemos que $o(a^k) = \frac{o(a)}{\text{mcd}(o(a), k)}$.

3. Supongamos que $ab = ba$ y que $\text{mcd}(o(a), o(b)) = 1$. Tenemos que

$$(ab)^{o(a)o(b)} = a^{o(a)o(b)}b^{o(a)o(b)} = (a^{o(a)})^{o(b)}(b^{o(b)})^{o(a)} = e \cdot e = e.$$

Tenemos que $o(ab) \mid o(a)o(b)$. 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 $o(a^{o(ab)}) = o(b^{o(ab)})$.

Por (2) tenemos que

$$\frac{o(a)}{\text{mcd}(o(a), o(ab))} = o(a^{o(ab)}) = o(b^{o(ab)}) = \frac{o(b)}{\text{mcd}(o(b), o(ab))}.$$

Sabemos que los órdenes son números naturales y que $\text{mcd}(o(a), o(b)) = 1$, por tanto debe ser que

$$\frac{o(a)}{\text{mcd}(o(a), o(ab))} = \frac{o(b)}{\text{mcd}(o(b), o(ab))} = 1.$$

Así, obtenemos que $o(a) = \text{mcd}(o(a), o(ab))$ y $o(b) = \text{mcd}(o(b), o(ab))$, por lo que $o(a) \mid o(ab)$ y $o(b) \mid o(ab)$. Como $\text{mcd}(o(a), o(b)) = 1$, tenemos que $o(a) o(b) \mid o(ab)$. 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 $d \mid o(a) = n$. Entonces existe un único subgrupo $H \leq G$ de orden d tal que $H = \langle a^{\frac{n}{d}} \rangle$.

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

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

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 $n \mid rd$. En particular, tenemos que $kd \mid rd$, por lo que $k \mid r$. Así, nos queda que $a^r \in \langle a^k \rangle$, por lo que $H \subset \langle a^k \rangle$. Recíprocamente, tenemos que $k = \text{mcd}(k, n)$, por lo que

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

Entonces, tenemos que $(a^k)^d = e$, por lo que $a^k \in H$. Así, tenemos que $\langle a^k \rangle \subset H$. Así, hemos demostrado que $H = \langle a^k \rangle$.

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 $S = \{s_1, \dots, s_k\}$ finito. Llamamos **subgrupo generado por S** al conjunto

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

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

Observación. Se cumple que $\langle S \rangle = \bigcap_{S \subset H \leq G} H$. 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, $\langle S \rangle \subset \bigcap_{S \subset H \leq G} H$.

(ii) Supongamos que $x \in \bigcap_{S \subset H \leq G} H$ 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 $\bigcap_{S \subset H \leq G} H \subset \langle S \rangle$.

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 $S = \{s_1, \dots, s_k\}$. Sea $f : G \rightarrow H$ un homomorfismo de grupos. Entonces $f(\langle S \rangle) = \langle f(S) \rangle$.

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

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

□

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

$$U_n = \{1, u, u^2, \dots, u^{n-1}\}.$$

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

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

Tenemos que $\rho : U_n \rightarrow U_n : z \rightarrow z \cdot u$, 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 $\forall z \in U_n$,

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

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

$$\{1, \tau, \rho, \rho^2, \dots, \rho^{n-1}, \tau\rho, \dots, \tau\rho^{n-1}\} \subset D_n.$$

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:

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

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

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

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

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

Veamos que es una biyección. Tenemos que

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

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

1.4.2. Generadores en grupos de congruencias

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

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

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,

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

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 $\mathcal{U}(\mathbb{Z}_m) = \{[a]_m : \text{mcd}(a, m) = 1\}$.

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

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 $\text{mcd}(a, m) = 1$. 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 $\text{mcd}(\lambda, m) \mid 1$ por lo que $\text{mcd}(\lambda, m) = 1$ y $[\lambda]_m \in \mathcal{U}(\mathbb{Z}_m)$.

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

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 $\text{mcd}(a, m) = 1$, 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 $\text{mcd}(ab, m) > 1$, entonces existe un primo p tal que $p \mid m$ y $p \mid ab$, por lo que $p \mid a$ o $p \mid b$, 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 $\mathcal{U}(\mathbb{Z}_m)$. □

^aEsta 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

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

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 $\varphi(p^k) = (p - 1)p^{k-1}$. En particular, si $k \geq 3$, $\varphi(p^k) = \varphi(p^{k-1})p$.
3. Si $n, m \in \mathbb{N}$ tales que $\text{mcd}(n, m) = 1$, entonces $\varphi(nm) = \varphi(n)\varphi(m)$.

Demostración. 1. Es trivial.

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

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

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

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

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

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

□

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

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

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

Demostración. Demostramos sólomente 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

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

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, \dots, a_k representantes de las k distintas clases de equivalencia. Así,

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

Dado que se trata de uniones disjuntas obtenemos que

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

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 $[a]_{\sim_H} \rightarrow [a^{-1}]_{\sim_H}$ 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, \dots, a_m representantes de las clases de equivalencia de $[G : H]$ y sean b_1, \dots, b_n representantes de las clases de equivalencia $[H : K]$. Así, tenemos que

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

Por tanto, $Ha_i = Kb_1a_i \sqcup \dots \sqcup Kb_na_i$, $\forall i = 1, \dots, m$. 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. \square

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 $H = G$.

\square

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 $G = \langle a \rangle$.

\square

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

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

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

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

^aPara que se cumpla el teorema debe darse que $\text{mcd}(a, p) = 1$.

Demostración. Usando lo anterior, tenemos que

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

□

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 $G \cong C_4$.

2.1. Subgrupos normales

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

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

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**, $H \triangleleft G$, 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. $H \triangleleft G$.
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 $H \triangleleft G$. \square

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

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

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

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

2. Si $K \leq \text{Im}(f)$, entonces $f^{-1}(K) \leq G_1$. Tenemos que ver que $f^{-1}(K) \triangleleft G_1$, 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 $y \in \text{Im}(f)$ y $k' \in K$ tales que $f(x) = y$ y $f(k) = k'$. Así, nos queda que

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

\square

Ejemplo. Consideremos la aplicación $\det : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^*$. Tenemos que $\text{Ker}(\det) = \text{SL}_n(\mathbb{R}) \triangleleft \text{GL}_n(\mathbb{R})$.

Proposición 2.4. Sea G un grupo.

1. Si $H \leq G$ y $[G : H] = 2$, entonces $H \triangleleft G$.
2. Si $K, H \leq G$ y $H \triangleleft G$, entonces $HK \leq G$. Además, si $K \triangleleft G$, $HK \triangleleft G$.
3. Si $K, H \triangleleft G$ 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 $H \triangleleft G$.

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

$$xy^{-1} = (h_1k_1)(h_2k_2)^{-1} = h_1(k_1k_2^{-1})h_2^{-1} \in h_1(k_1k_2^{-1})H = h_1H(k_1k_2^{-1}).$$

Así, tenemos que $h_1H(k_1k_2^{-1}) \subset H(k_1k_2^{-1}) \subset HK$, por lo que $xy^{-1} \in HK$. Si se cumple también que $K \triangleleft G$ entonces dados $g \in G$ y $hk \in HK$,

$$g^{-1}(hk)g = (g^{-1}hg)(g^{-1}kg) \in HK.$$

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

$$h^{-1}k^{-1}hk = h^{-1}k^{-1}hkh^{-1}h = h^{-1}(k^{-1}hkh^{-1})h \in H.$$

$$h^{-1}k^{-1}hk = k^{-1}kh^{-1}k^{-1}hk = k^{-1}(kh^{-1}k^{-1}h)k \in K.$$

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. \square

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

Ejemplo. Tomamos $D_4 = \langle \tau, \rho \rangle = \{e, \tau, \rho, \rho^2, \rho^3, \tau\rho, \tau\rho^2, \tau\rho^3\}$. 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:

$$H_1 = \langle \rho \rangle, H_2 = \langle \tau, \rho^3 \rangle, H_3 = \langle \tau\rho, \rho^2 \rangle.$$

- Calculamos los subgrupos de orden 2:

$$H_4 = \langle \tau \rangle, H_5 = \langle \rho^2 \rangle, H_6 = \langle \tau\rho \rangle, H_7 = \langle \tau\rho^2 \rangle, H_8 = \langle \tau\rho^3 \rangle.$$

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 $K \triangleleft H$ y $H \triangleleft G$ no implica que $K \triangleleft G$. Por ejemplo, en D_4 tenemos que $\langle \tau \rangle \triangleleft \langle \tau, \rho^2 \rangle \triangleleft D_4$ 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 $H \triangleleft G$. 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:

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

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 $H \triangleleft G$. Tenemos que

$$ab(a_1b_1)^{-1} = abb_1^{-1}a_1^{-1} = a(bb_1^{-1})a^{-1}aa_1^{-1} = (a(bb_1^{-1})a^{-1})(aa_1^{-1}) \in H.$$

Nuevamente hemos utilizado que $H \triangleleft G$. 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 $[G : H] = \frac{|G|}{|H|}$.

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 $H \triangleleft G$ 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 $H = \langle \rho^2 \rangle \triangleleft G$. Tenemos que G/H tiene estructura de grupo y $[G : H] = 4$, por lo que $|D_4/\rho^2| = 4$. 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

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

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

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

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

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

Veamos que $\text{Ker}(\pi) = H$. 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

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

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

(ii) Ya vimos que $\text{Ker}(f) \triangleleft G$. □

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

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

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

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

Demostración. Veamos que la aplicación está bien definida. Si $H \leq G_1$ tenemos que $f(H) \leq \text{Im}(f)$.

Veamos ahora que la aplicación es inyectiva. Supongamos que existen $K_1, K_2 \in \{K \leq G_1 : \text{Ker}(f) \leq K\}$ 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

$$f(k_1) = f(k_2) \iff f(k_1)f(k_2)^{-1} = e \iff f(k_1k_2^{-1}) = e \iff k_1k_2^{-1} \in \text{Ker}(f).$$

Así, tenemos que $k_1k_2^{-1} \in K_1$, 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 $N_1 \in \{N : N \leq \text{Im}(f)\}$. Sabemos que $f^{-1}(N_1) \leq G_1$ y $\text{Ker}(f) \leq f^{-1}(N_1)$, por lo que $f^{-1}(N_1) \in \{K \leq G_1 : \text{Ker}(f) \leq K\}$. Es fácil ver que $f(f^{-1}(N_1)) = N_1$. 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 $H \triangleleft G$).

2.3. Teoremas de isomorfía

Ejemplo. 1. Sea $f_n : (\mathbb{Z}, +) \rightarrow (\mathbb{C}^*, \cdot) : k \rightarrow e^{\frac{2k\pi i}{n}}$. 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 $\text{Im}(f_n) = U_n$, que son las raíces n -ésimas de la unidad. Calculemos el núcleo:

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

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

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

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

$$\bar{f} : G_1 / \text{Ker}(f) \rightarrow \text{Im}(f) : [g] \rightarrow \bar{f}([g]) = f(g),$$

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

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

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

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

$$\bar{f}([g_1][g_2]) = \bar{f}([g_1 g_2]) = f(g_1 g_2) = f(g_1) f(g_2) = \bar{f}([g_1]) \bar{f}([g_2]).$$

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

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

2. Consideremos $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n : (x, y) \rightarrow ([x]_m, [y]_n)$. Tenemos que $\text{Ker}(f) = m\mathbb{Z} \times n\mathbb{Z}$ e $\text{Im}(f) = \mathbb{Z}_m \times \mathbb{Z}_n$. 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 $N \triangleleft G$. Así, $H / H \cap N \cong HN / N$.

Teorema 2.4 (Tercer teorema de isomorfía). Sea G un grupo y $H, N \triangleleft G$ 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 $o(b) \nmid o(a)$, es decir, $b^{o(a)} \neq e$. Así existe un primo p y un $k \geq 1$ tal que $p^k | o(b)$ pero $p^k \nmid o(a)$. Escribimos

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

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 $\exp(G) = o(a)$. \square

- 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 $G = \langle a \rangle \cdot K$

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 $o(x^p) = \frac{o(x)}{p} < o(x)$, por el lema anterior. En particular, por minimalidad de $o(x)$ deducimos que $x^p \in H$ y por tanto, como $o(x^p) \mid \exp(G) = o(a) = |H|$, deducimos que $\langle x^p \rangle$ es el único subgrupo de H de orden $o(x^p)$. Por otro lado, como $o(x) \mid \exp(G) = o(a)$, el lema anterior también implica que $o(a) = o(a^p) \cdot p$, con lo que $o(x^p) \mid o(a^p)$, 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, \dots, m_k tales que m_i divide a m_{i-1} enteros con $k \geq 1$ natural tal que

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

Además, m_1, \dots, m_k son únicos con esta propiedad.

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

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

2. Como $m_i \mid m_{i-1}$, 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 $(5^2 \cdot 2, 5^2 \cdot 2, 5 \cdot 2)$.

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 $m_1, \dots, m_k \in \mathbb{N}$ tales que $G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$. Sabemos que $n = m_1 \cdots m_k$. Como $m \mid n$, entonces existen $n_1, \dots, n_k \in \mathbb{N}$ con $n_i \mid m_i$, $\forall i = 1, \dots, k$ 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 $\text{mcd}(8, 3) = 1$ 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,

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

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 $\alpha_i \geq 1, \forall i = 1, \dots, s$. 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:

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

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:

$$\begin{aligned}\alpha_1 &= 2 = 2 + 0 = 1 + 1 \\ \alpha_2 &= 4 = 4 + 0 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1.\end{aligned}$$

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 $f : G \rightarrow G'$ una biyección. Consideramos la aplicación $\text{Biy}(G) \rightarrow \text{Biy}(G') : \sigma \rightarrow f^{-1}\sigma f$, que es un isomorfismo de grupos. Vamos a considerar un conjunto finito de elementos al que llamaremos $X_n = \{1, 2, \dots, n\}$ 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 $\tilde{g} : G \rightarrow G : x \rightarrow x \cdot g$. Es fácil ver que $\tilde{g} \in \text{Biy}(G)$. Ahora, consideremos $\phi : G \rightarrow \text{Biy}(G) : g \rightarrow \tilde{g}$. 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 $G \cong \text{Im}(\phi) \leq \text{Biy}(G) = \mathcal{S}_{|G|}$. \square

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 $\text{sop}(\sigma) \cap \text{sop}(\tau) = \emptyset$.

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. $\text{sop}(\sigma) = \text{sop}(\sigma^{-1})$. En efecto, si $a \in \text{sop}(\sigma)$, tenemos que $a \neq \sigma(a)$, por lo que $\sigma^{-1}(a) \neq a$ y $a \in \text{sop}(\sigma^{-1})$. 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 $\sigma(x) \in \text{sop}(\sigma)$ y en consecuencia $\sigma(x) \notin \text{sop}(\tau)$. 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

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

Así, por ser σ y τ disjuntos tenemos que $\text{sop}(\sigma^m) = \text{sop}(\tau^m) = \emptyset$, 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 $i_1, \dots, i_k \in X_n$, tenemos que $\sigma(i_j) = i_{j+1}$ (con $\sigma(i_k) = i_1$) y para el resto $i_{k+1}, \dots, i_n \in X_n$ se tiene que $\sigma(i_t) = i_t$. Lo escribimos (i_1, \dots, 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 $2 \leq k \leq n$.

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

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

- Es trivial a partir de la definición.
- Basta con comprobar que su composición es la identidad:

$$(i_1, i_2, \dots, i_k)(i_k, i_{k-1}, \dots, i_1) = (i_1) \cdots (i_k) = id.$$

Comprobar la otra composición es análogo.

3. Si tomamos $\sigma = (i_1, \dots, i_k)$ 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 contruidos.

□

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 consideremos 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 $\{j_1, \dots, j_t\}$ 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 $\sigma_i : X_n \rightarrow X_n$ tal que

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

Así, tenemos que $\sigma_i = (j_i, \sigma(j_i), \dots, \sigma^{s_i-1}(j_i))$ es un s_i -ciclo donde $\text{sop}(\sigma_i) = O_i$. Como $O_i \cap O_j = \emptyset$ si $i \neq j$, tenemos que $\text{sop}(\sigma_i) \cap \text{sop}(\sigma_j) = \emptyset$, $\forall i, j \in \{1, \dots, t\}$ con $i \neq j$. Así, tenemos que

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

□

Observación. La descomposición en ciclos disjuntos es única salvo en el ordenamiento de los factores.

Ejemplo. Tenemos que

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

Corolario 4.1 (Orden de una permutación). Sea $\sigma \in \mathcal{S}_n$ con $\sigma = \sigma_1 \cdots \sigma_k$ ciclos disjuntos. Entonces, $o(\sigma) = \text{mcm}(o(\sigma_1), \dots, o(\sigma_k))$.

Demostración. Por ser $\sigma_1, \dots, \sigma_k$ 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 $\sigma_i^m = id$, $\forall i = 1, \dots, k$. Por tanto, necesitamos que $o(\sigma_i) \mid m$, $\forall i = 1, \dots, k$, por lo que claramente debe ser que

$\text{mcm}(o(\sigma_1), \dots, o(\sigma_k)) \mid m$. Por otro lado, como $\sigma_i^{\text{mcm}(o(\sigma_1), \dots, o(\sigma_k))} = id$, tenemos que $\sigma^{\text{mcm}(o(\sigma_1), \dots, o(\sigma_k))} = id$, por lo que $m \mid \text{mcm}(o(\sigma_1), \dots, o(\sigma_k))$. Así, obtenemos que

$$o(\sigma) = \text{mcm}(o(\sigma_1), \dots, o(\sigma_k)).$$

□

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

Corolario 4.2. Sea $\sigma \in \mathcal{S}_n$. Entonces, podemos escribir σ como producto de trasposiciones.

Demostración. Si $\sigma \in \mathcal{S}_n$, sabemos que $\sigma = \sigma_1 \cdots \sigma_k$ ciclos disjuntos. Basta ver que todo ciclo puede escribirse como producto de trasposiciones. Sea (i_1, \dots, i_k) un k -ciclo arbitrario. Es fácil ver que

$$(i_1, \dots, i_k) = (i_1, i_k)(i_2, i_k) \cdots (i_{k-1}, i_k).$$

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

Observación. 1. Si consideramos el siguiente 3-ciclo:

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

2. En \mathcal{S}_6 nos preguntamos cómo son los elementos de orden 3. Si $\sigma \in \mathcal{S}_6$ con $o(\sigma) = 3$, tenemos que $\sigma = \sigma_1 \cdots \sigma_k$ y tenemos que $3 = o(\sigma) = \text{mcm}(o(\sigma_1), \dots, o(\sigma_k))$, por lo que todos los ciclos que componen a σ deben ser de orden 3. Así, tenemos que σ tiene dos posibles formas:

$$\sigma = (i_1, i_2, i_3).$$

$$\sigma = (i_1, i_2, i_3)(i_4, i_5, i_6).$$

Así, los elementos de orden 3 pueden ser un 3-ciclo o dos 3-ciclos.

3. En \mathcal{S}_5 los elementos de orden tres sólo son los 3-ciclos puesto que sólo tenemos tres elementos. También podemos ver que en \mathcal{S}_5 hay elementos de orden 6, en particular aquellos que son la composición de un 2-ciclo y un 3-ciclo.

4. En \mathcal{S}_n , $n \geq 2$, con $k \in \mathbb{N}$, nos podemos preguntar cuántos k -ciclos hay en \mathcal{S}_n . Recordamos que los elementos de \mathcal{S}_n son las biyecciones del conjunto $X_n = \{1, \dots, n\}$. En primer lugar, tenemos que calcular el número de soportes posibles, es decir, cuántas formas hay de coger k elementos de X_n . Hay $\binom{n}{k}$ soportes posibles. Por otro lado, dado un soporte $\{i_1, \dots, i_k\}$ hay $k!$ formas de ordenar estos números. Hemos de notar que cada ciclo lo contamos k veces, puesto que

$$(i_1, \dots, i_k) = (i_2, \dots, i_k, i_1) = \cdots = (i_{k-1}, i_k, i_1, \dots, i_{k-2}) = (i_k, \dots, i_{k-1}).$$

Así, en total el número de k -ciclos es:

$$\binom{n}{k} k! \frac{1}{k} = \binom{n}{k} (k-1)!.$$

4.2. Conjugación

Definición 4.5 (Elemento conjugado). Sea G un grupo y $x \in G$. Llamamos **conjugado** de x por $g \in G$ a $g^{-1}xg \in G$.

Proposición 4.3. Sean $\sigma, \tau \in \mathcal{S}_n$ tal que $\sigma = (i_1, \dots, i_k)$. Se cumple que $\tau^{-1}\sigma\tau = (\tau(i_1), \dots, \tau(i_k))$.

Demostración. Sea $j < k$, tenemos que

$$\tau^{-1}\sigma\tau(\tau(i_j)) = \tau(\sigma(\tau^{-1}(\tau(i_j)))) = \tau(\sigma(i_j)) = \tau(i_{j+1}).$$

Si $j = k$ tenemos que

$$\tau^{-1}\sigma\tau(\tau(i_k)) = \tau(\sigma(\tau^{-1}(\tau(i_k)))) = \tau(\sigma(i_k)) = \tau(i_1).$$

Sea $x \notin \tau(\text{sop}(\sigma))$, entonces $\tau^{-1}(x) \notin \text{sop}(\sigma)$, es decir,

$$\sigma(\tau^{-1}(x)) = \tau^{-1}(x) \Rightarrow \tau^{-1}\sigma\tau(x) = \tau(\sigma(\tau^{-1}(x))) = \tau(\tau^{-1}(x)) = x.$$

Así, nos queda que $\tau^{-1}\sigma\tau = (\tau(i_1), \dots, \tau(i_k))$ es un k -ciclo. \square

Proposición 4.4. Sean $\sigma_1, \sigma_2 \in \mathcal{S}_n$, k -ciclos. Entonces existe $\tau \in \mathcal{S}_n$ tal que $\tau^{-1}\sigma_1\tau = \sigma_2$.

Demostración. Sea $\sigma_1 = (i_1, \dots, i_k)$ y $\sigma_2 = (j_1, \dots, j_k)$. Vamos a definir la aplicación siguiente:

$$\tau_{\sigma_1\sigma_2} : \text{sop}(\sigma_1) \rightarrow \text{sop}(\sigma_2) : i_s \rightarrow j_s, \quad 1 \leq s \leq k.$$

Claramente $\tau_{\sigma_1\sigma_2}$ es una biyección. Es fácil ver que $|X_n/\text{sop}(\sigma_1)| = |X_n/\text{sop}(\sigma_2)|$. Podemos extender $\tau_{\sigma_1\sigma_2}$ a una biyección $\tau : X_n \rightarrow X_n$ arbitraria que cumpla $\tau(i_s) = \tau_{\sigma_1\sigma_2}(i_s) = j_s$ para $1 \leq s \leq k$. Por construcción y por la proposición anterior, tenemos que

$$\tau^{-1}\sigma\tau = (\tau(i_1), \dots, \tau(i_k)) = (j_1, \dots, j_k) = \sigma_2.$$

\square

Ejemplo. En \mathcal{S}_5 consideremos $\sigma_1 = (1, 3, 2)$ y $\sigma_2 = (2, 5, 1)$. Calculando τ usando la notación anterior:

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

Hay dos formas posibles de poner los dos valores restantes, 3 y 4, y ambas permutaciones son válidas. Así, las dos permutaciones que funcionarían son:

$$\tau_1 = (1, 2)(3, 5, 4), \quad \tau_2 = (1, 2)(3, 5).$$

Corolario 4.3. Sean $\sigma, \gamma \in \mathcal{S}_n$ permutaciones. Entonces, σ y γ son conjugadas si y solo si tienen una descomposición en ciclos disjuntos parecida; es decir, $\sigma = \sigma_1 \cdots \sigma_k$ y $\gamma = \gamma_1 \cdots \gamma_k$ y tienen la misma longitud en k -ciclos.

Demostración. (i) Si σ y γ son conjugados, existe $\tau \in \mathcal{S}_n$ tal que $\tau^{-1}\sigma\tau = \gamma$. Sabemos que $\sigma = \sigma_1 \cdots \sigma_k$ ciclos disjuntos. Entonces, tenemos que

$$\gamma = \tau^{-1}\sigma\tau = \tau^{-1}(\sigma_1 \cdots \sigma_k)\tau = (\tau^{-1}\sigma_1\tau) \cdots (\tau^{-1}\sigma_k\tau).$$

Tenemos que $\gamma_j = \tau^{-1}\sigma_j\tau$ es un t -ciclo, donde $t = |\text{sop}(\sigma_j)|$. Así, tenemos que $\text{sop}(\tau^{-1}\sigma_j\tau) = \tau(\text{sop}(\sigma_j))$. Por ser τ una biyección, los soportes de γ_j son disjuntos. Así, la descomposición de γ tiene las mismas características que la de σ , que es lo que buscábamos.

(ii) Supongamos que ambas permutaciones tienen esa descomposición. Entonces, siguiendo la demostración de la proposición anterior podemos construir $\tau_{\sigma_i\gamma_i}$ para cada i y luego extendemos la biyección

$$\bigsqcup_{i=1}^r \tau_{\sigma_i\gamma_i} : \bigsqcup_{i=1}^r \text{sop}(\tau_i) \rightarrow \bigsqcup_{i=1}^r \text{sop}(\gamma_i),$$

a una biyección τ de X_n .

□

Ejemplo. En \mathcal{S}_7 sean $\sigma = \sigma_1\sigma_2$, con $\sigma_1 = (2, 1, 5)$ y $\sigma_2 = (3, 4)$, y $\gamma = \gamma_1\gamma_2$, con $\gamma_1 = (7, 4, 2)$ y $\gamma_2 = (1, 3)$. La demostración anterior nos da que

$$\tau_{\sigma_1\gamma_1} = \begin{pmatrix} 1 & 2 & 5 \\ 4 & 7 & 2 \end{pmatrix}, \tau_{\sigma_2\gamma_2} = \begin{pmatrix} 3 & 4 \\ 1 & 3 \end{pmatrix}, \text{ y } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 1 & 3 & 2 & * & * \end{pmatrix}.$$

4.3. Subgrupo alternado

Definición 4.6 (Paridad). Sea $\sigma \in \mathcal{S}_n$.

- Diremos que es **par** si se puede escribir como un producto par de trasposiciones.
- Diremos que es **impar** si no es par.

Observación. A priori podría suceder que una permutación se pueda escribir con un número par e impar de trasposiciones. El siguiente resultado prueba que esto no es posible.

Proposición 4.5. Sea $\sigma \in \mathcal{S}_n$ con $\sigma = \tau_1 \cdots \tau_r = \gamma_1 \cdots \gamma_l$ producto de trasposiciones. Entonces, si r es par l también lo es.

Demostración. Tenemos que $\sigma = \tau_1 \cdots \tau_r = \gamma_1 \cdots \gamma_l$, por lo que

$$\tau_1 \cdots \tau_r \cdot \gamma_l \cdots \gamma_1 = id.$$

Basta ver que la identidad solo se puede escribir como un producto par de trasposiciones. Supongamos que la identidad se puede escribir como un producto impar de trasposiciones. Vamos a coger la de menor longitud s impar, es decir

$$id = (a_1, b_1) \cdots (a_s, b_s), \quad a_1, \dots, a_s, b_1, \dots, b_s \in X_n.$$

Tenemos que $a_i \neq b_i, \forall i = 1, \dots, s$. Ahora, de entre todas las representaciones de longitud s vamos a tomar la que menos cantidad de a_1 tenga. Es claro que $s \neq 1$, puesto que si $s = 1$ entonces $id = (a_1, b_1)$ y tendríamos que $a_1 = b_1$. Podemos suponer que $s \geq 3$. Tenemos que en $(a_2, b_2) \cdots (a_s, b_s)$ aparece a_1 , es decir, está en su soporte. Así, existe $2 \leq j \leq s$ tal que $a_j = a_1$. Escogiendo el mínimo j y operando adecuadamente podemos tomar $j = 2$, por lo que $a_2 = a_1$. Así, podemos distinguir dos casos:

- Si $b_1 = b_2$, tenemos que $(a_1, b_1)(a_2, b_2) = id$, por lo que la identidad es el producto de $s - 2$ trasposiciones, lo cual es imposible porque habíamos dicho que s era la mínima longitud.
- Si $b_1 \neq b_2$, tenemos que $(a_1, b_1)(a_2, b_2) = (a_1, b_2)(b_1, b_2)$. Por tanto, podemos reescribir

$$id = (a_1, b_2)(b_1, b_2) \cdots (a_s, b_s).$$

Como hemos escrito la identidad con un a_1 menos, esto contradice la elección de la representación inicial de id .

□

Definición 4.7 (Subgrupo alternado). En \mathcal{S}_n llamamos **grupo n -ésimo alternado** a $\mathcal{A}_n = \{\sigma \in \mathcal{S}_n : \sigma \text{ par}\}$.

Observación. Consideremos la aplicación $\text{sig} : \mathcal{S}_n \rightarrow \{-1, 1\}$ tal que

$$\sigma \rightarrow \text{sig}(\sigma) = \begin{cases} -1, & \sigma \text{ impar} \\ 1, & \sigma \text{ par} \end{cases}.$$

Es fácil ver que es un homomorfismo. Claramente tenemos que $\text{Ker}(\text{sig}) = \mathcal{A}_n$ e $\text{Im}(f) = \{-1, 1\}$. Por tanto, tenemos que $\mathcal{A}_n \triangleleft \mathcal{S}_n$. Por el primer teorema de isomorfía tenemos que $\mathcal{S}_n/\mathcal{A}_n \cong \{-1, 1\}$, por lo que $[\mathcal{S}_n : \mathcal{A}_n] = 2$ y tenemos que

$$|\mathcal{A}_n| = \frac{n!}{2}.$$

Proposición 4.6. Si $n \geq 3$, \mathcal{A}_n está generado por todos los 3-ciclos de \mathcal{S}_n .

Demostración. Si tomamos un 3-ciclo (i, j, k) , tenemos que

$$(i, j, k) = (k, i)(j, k) \in \mathcal{A}_n.$$

Por tanto, todos los 3-ciclos están en el grupo alternado. Ahora veamos que las permutaciones pares son productos de 3-ciclos. Consideremos dos trasposiciones, entonces

podemos escribirlas como producto de a lo sumo dos 3-ciclos. En efecto, consideremos las trasposiciones (i, j) y (k, r) . Hay varias opciones:

- Si $\{i, j\} \cap \{k, r\} \neq \emptyset$ y $j = r$, podemos escribir

$$(i, j)(k, r) = (i, j)(k, j) = (j, k, i).$$

- Si $\{i, j\} \cap \{k, r\} \neq \emptyset$ y $\{i, j\} = \{k, r\}$ tenemos que $(i, j)(k, r) = id$.
- Si $\{i, j\} \cap \{k, r\} = \emptyset$, tenemos que

$$(i, j)(k, r) = (r, k, i)(i, j, k).$$

□

Ejemplo. ■ \mathcal{A}_2 tiene un sólo elemento.

- $\mathcal{A}_3 \cong C_3$.
- \mathcal{A}_4 tiene orden 12 y es un grupo en sí mismo, es decir, no es isomorfo a ningún grupo que hayamos visto anteriormente. Además, \mathcal{A}_4 está formado por los 3-ciclos de \mathcal{S}_4 y las permutaciones de dos trasposiciones disjuntas. Es fácil ver que \mathcal{A}_4 no tiene elementos de orden 4 ni de orden 6.
- Si consideramos el conjunto

$$\{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} \leq \mathcal{A}_4,$$

es un subgrupo de orden 4 y lo llamamos **grupo de Klein**, que es isomorfo a $C_2 \times C_2$. En concreto, el grupo de Klein es normal en \mathcal{A}_4 .

Teorema 4.2. Si $n \geq 5$, entonces \mathcal{A}_n es simple.

Capítulo 5

Acciones de grupos

Definición 5.1 (Acción de un grupo). Una **acción** de un grupo G sobre un conjunto $X \neq \emptyset$ es un homomorfismo de grupos

$$G \rightarrow \text{Biy}(X) : g \rightarrow \tilde{g}.$$

Ejemplo. 1. Sea \mathcal{S}_n y $X = X_n$. Tenemos que la identidad es una acción de grupo de \mathcal{S}_n sobre X_n :

$$\mathcal{S}_n \rightarrow \text{Biy}(X_n) : \sigma \rightarrow \sigma.$$

2. Consideremos $G = \langle \sigma \rangle$, con $\sigma \in \mathcal{S}_n$ y $X = X_n$. La inclusión, definida de la forma

$$\in : H \subset G \rightarrow G : x \rightarrow x,$$

es una acción de grupo de $\langle \sigma \rangle$ en X_n .

3. Si G actúa sobre X y $H \leq G$, entonces H actúa sobre X . Basta con tomar la restricción de la acción a H .

4. Sea $H \leq G$. Definimos una acción

$$\alpha : H \rightarrow \text{Biy}(G) : h \rightarrow \tilde{h},$$

tal que $\tilde{h} : G \rightarrow G : g \rightarrow gh$. Veamos que α es un homomorfismo. Sean $x, y \in H$ y $g \in G$,

$$\alpha(xy)(g) = \tilde{xy}(g) = gxy = \tilde{y}(gx) = \tilde{y}(\tilde{x}(g)) = \tilde{y} \circ \tilde{x}(g) = \tilde{x} \cdot \tilde{y}(g).$$

A esto se lo llama **acción por traslación a la derecha**. La acción por la izquierda no funciona de la forma anterior, solo funciona si es de la forma

$$\tilde{h} : G \rightarrow G : g \rightarrow h^{-1}g.$$

5. Sea $H \leq G$. Definimos la **acción por conjugación** $\alpha : H \rightarrow \text{Biy}(G)$ tal que $\tilde{h}(g) = h^{-1}gh$. Ya sabemos que $\tilde{h} \in \text{Biy}(G)$. Veamos que es homomorfismo.

$$\tilde{xy}(g) = (xy)^{-1}g(xy) = y^{-1}x^{-1}gxy = y^{-1}\tilde{x}(g)y = \tilde{y}(\tilde{x}(g)) = \tilde{x} \cdot \tilde{y}(g).$$

Definición 5.2 (Órbita). Sea G un grupo que actúa sobre X . Tomamos $x \in X$, definimos la **órbita** de x como

$$O_x = \{\tilde{g}(x) \in X : g \in G\}.$$

Observación. Consideremos la relación

$$x \sim y \iff \exists \tilde{g} \in \text{Biy}(X), \tilde{g}(x) = y \iff \exists g \in G, \tilde{g}(x) = y.$$

Es fácil comprobar que se trata de una relación de equivalencia, por lo que podemos considerar el cociente X/\sim . Si consideramos las clases de equivalencia de este cociente, corresponden con las órbitas, es decir, $[x]_\sim = O_x$. Así, dados $x, y \in X$, tenemos que $O_x \cap O_y = \emptyset$ o $O_x = O_y$, por tratarse de clases de equivalencia.

Definición 5.3 (Estabilizador de un elemento). Sea G un grupo que actúa sobre X . Llamamos **estabilizador** de $x \in X$ a

$$G_x = \{g \in G : \tilde{g}(x) = x\}.$$

Observación. Es fácil ver que $G_x \leq G$. En efecto, está claro que $e \in G_x$ puesto que $id(x) = x, \forall x \in G$. Por otro lado, supongamos que $a, b \in G_x$, entonces tenemos que

$$\tilde{a} \cdot \widetilde{b^{-1}}(x) = \tilde{a} \cdot \tilde{b}^{-1}(x) = \tilde{b}^{-1}(\tilde{a}(x)) = \tilde{b}^{-1}(x) = x.$$

Así, tenemos que $ab^{-1} \in G_x$, por lo que $G_x \leq G$.

Ejemplo. Consideremos la permutación $\sigma = (1, 4, 5)(2, 6) \in \mathcal{S}_7$ y $G = \langle \sigma \rangle$. Sabemos que G actúa sobre X_7 . Consideremos $x = 4 \in X_7$ y calculemos su órbita y su estabilizador:

$$O_4 = \{1, 4, 5\}, G_4 = \{id, \sigma^3\}.$$

Ahora si $x = 7$ tenemos que $O_7 = \{7\}$ y $G_7 = G$. Podemos observar que $|O_4| = [G : G_4]$ y $|O_7| = [G : G_7]$.

Teorema 5.1 (Teorema de la órbita-estabilizador). Sea G un grupo que actúa sobre un conjunto no vacío X y $x \in X$. La órbita O_x está en biyección con G/\sim_{G_x} . En particular, si la órbita O_x es finita, entonces $|O_x| = [G : G_x]$.

Demostración. Recordemos que \sim_{G_x} es la relación de equivalencia que viene dada por

$$g_1 \sim_{G_x} g_2 \iff g_1 g_2^{-1} \in G_x.$$

También tenemos que $[G : G_x] = |G/\sim_{G_x}|$. Definimos la función

$$O_x \rightarrow G/\sim_{G_x} : \tilde{g}(x) \rightarrow G_x g.$$

Veamos que es una biyección. Claramente es sobreyectiva. Veamos que es inyectiva y que está bien definida.

$$\tilde{g}_1(x) = \tilde{g}_2(x) \iff \tilde{g}_2^{-1}(\tilde{g}_1(x)) = x \iff \tilde{g}_1 \tilde{g}_2^{-1}(x) = x \iff \tilde{g}_1 \tilde{g}_2^{-1} \in G_x.$$

Con esto hemos visto que es inyectiva y que está bien definida. \square

Corolario 5.1 (Fórmula de las órbitas). Sea G un grupo que actúa sobre un conjunto finito X y sea \mathcal{C} el conjunto de los representantes de las órbitas. Entonces,

$$|X| = \sum_{x \in \mathcal{C}} |O_x| = \sum_{x \in \mathcal{C}} [G : G_x].$$

Demostración. Tenemos que

$$X = \bigsqcup_{x \in \mathcal{C}} O_x.$$

De aquí la deducción es trivial. \square

Definición 5.4 (Punto fijo). Dicemos que $x \in X$ es un **punto fijo** si $O_x = \{x\}$, es decir, si la órbita es trivial. Llamaremos $\text{Fix}(X)$ al conjunto de los puntos fijos de X por una acción.

Observación. 1. Sea $x \in X$, entonces $O_x = \{x\} \iff G = G_x$.

2. Es fácil ver que

$$|X| = \sum_{x \in \mathcal{C}} |O_x| = |\text{Fix}(X)| + \sum_{x_i \in X} |O_{x_i}|,$$

donde x_i son elementos cuyas órbitas son no triviales.

Proposición 5.1 (Ecuación de clases). Sea G un grupo finito. Entonces,

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

donde x_i son los elementos cuyas órbitas no son triviales mediante la acción de conjugación.

Demostración. Sea G un grupo finito y consideramos la acción por conjugación, $\tilde{g}(x) = g^{-1}xg$ para $x \in X = G$. Tenemos que

$$x \in Z(G) \iff O_x = \{x\}.$$

Por otro lado, si $x \notin Z(G)$, tendremos que $G_x = C_G(x)$. Así, basta con aplicar la observación anterior para obtener el resultado deseado. \square

Teorema 5.2 (Teorema de Cauchy). Si G es un grupo finito y p un primo que divide a $|G|$, entonces existe $g \in G$ tal que $o(g) = p$.

Demostración. \square

Corolario 5.2. Sea G un grupo de orden $2p$ con $p \geq 3$ primo. Entonces, $G \cong D_p$ o $G \cong C_2 \times C_p$.

Demostración.

□

Parte II

Anillos

Capítulo 6

Generalidades de Anillos

Definición 6.1 (Anillo). Sea $(A, +, \cdot)$, donde A es un conjunto no vacío y $+: A \times A \rightarrow A$ y $\cdot: A \times A \rightarrow A$ son dos operaciones internas. Diremos que A es un **anillo** si:

1. $(A, +)$ es un grupo abeliano.
2. El producto es asociativo, es decir, $\forall x, y, z \in A$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
3. El producto es distributivo por la derecha y por la izquierda, es decir, $\forall x, y, z \in A$,

$$(x + y) \cdot z = x \cdot z + y \cdot z \quad y \quad z \cdot (x + y) = z \cdot x + z \cdot y.$$

Definición 6.2. Sea $(A, +, \cdot)$ un anillo.

1. Diremos que es **unitario** si existe $1_A \in A$ tal que $a \cdot 1_A = 1_A \cdot a$, $\forall a \in A$.
2. Diremos que es un **anillo conmutativo** si $\forall a, b \in A$, $a \cdot b = b \cdot a$.

Observación. Si el anillo es unitario el elemento neutro para el producto es único. En efecto, si 1_A y $1'_A$ son elementos neutros para el producto tenemos que

$$1_A = 1_A \cdot 1'_A = 1'_A.$$

Ejemplo. 1. Tenemos que $(\mathbb{Z}, +, \cdot)$ es un anillo unitario conmutativo. De manera similar, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$ también son anillos unitarios conmutativos.

2. El conjunto $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$ es un anillo unitario (es no conmutativo si $n \geq 2$).
3. $(\mathbb{Z}_n, +, \cdot)$ con $n \geq 2$ es un anillo unitario conmutativo.
4. $(2\mathbb{Z}, +, \cdot)$ es un anillo conmutativo no unitario (esto es cierto en general para $d\mathbb{Z}$ con $d \in \mathbb{Z}/\{-1, 0, 1\}$).

Notación. Dado un anillo $(A, +, \cdot)$, $a \in A$ y $n \in \mathbb{N}$, denotamos

$$na := \underbrace{a + \cdots + a}_{n \text{ veces}}, \quad -na = \underbrace{(-a) + \cdots + (-a)}_{n \text{ veces}}, \quad a^n = \underbrace{a \cdots a}_{n \text{ veces}}.$$

Además, si A es unitario definimos que $a^0 = 1$. Decimos que 0 es el elemento neutro para la suma y 1 es el elemento neutro para el producto, si es unitario.

Proposición 6.1. Sea $(A, +, \cdot)$ un anillo.

1. $\forall a \in A, a \cdot 0 = 0 \cdot a = 0$.
2. $\forall a, b \in A, -(ab) = (-a)b = a(-b)$.
3. Si $(B, \oplus, *)$ es un anillo, entonces $A \times B$ también es un anillo con las operaciones coordenada a coordenada. Además, si A y B son unitarios, $A \times B$ es unitario.

Demostración. 1. Sea $a \in A$,

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \iff a \cdot 0 = 0.$$

Por la izquierda se hace igual.

2. Si $a, b \in A$ tenemos que

$$ab + (-a)b = (a + (-a))b = 0 \cdot b = 0.$$

Los otros casos son análogos.

3. Tenemos que $A \times B$ es un grupo abeliano con la suma por serlo A y B . Es fácil ver que el producto es una operación interna, veamos que es asociativo. Si $(a, b), (c, d), (e, f) \in A \times B$,

$$\begin{aligned} ((a, b) \cdot (c, d)) \cdot (e, f) &= (a \cdot c, b \cdot d) \cdot (e, f) = ((a \cdot c) \cdot e, (b \cdot d) \cdot f) \\ &= (a \cdot (c \cdot e), b \cdot (d \cdot f)) = (a, b) \cdot (c \cdot e, d \cdot f) \\ &= (a, b) \cdot ((c, d) \cdot (e, f)). \end{aligned}$$

Veamos que el se cumple la propiedad distributiva:

$$\begin{aligned} [(a, b) + (c, d)] \cdot (e, f) &= (a + c, b \oplus d) \cdot (e, f) = ((a + c) \cdot e, (b \oplus d) \cdot f) \\ &= (a \cdot e + c \cdot e, b \cdot f \oplus d \cdot f) = (a \cdot e, b \cdot f) + (c \cdot e, d \cdot f) \\ &= (a, b) \cdot (e, f) + (c, d) \cdot (e, f). \end{aligned}$$

Por otro lado, si son los dos unitarios está claro que $A \times B$ también lo será puesto que $(1_A, 1_B) \in A \times B$ y $\forall (a, b) \in A \times B$ se tiene que

$$(1_A, 1_B) \cdot (a, b) = (a, b) \cdot (1_A, 1_B) = (a, b).$$

□

Definición 6.3 (Subanillo). Sea $(A, +, \cdot)$ un anillo y $\emptyset \neq B \subset A$. Diremos que $(B, +, \cdot)$ es **subanillo** de A si $(B, +)$ es subgrupo de $(A, +)$ y B es cerrado para el producto, es decir, $\forall b_1, b_2 \in B, b_1 \cdot b_2 \in B$.

Observación. Sea $(A, +, \cdot)$ un anillo unitario y $(B, +, \cdot)$ un subanillo.

1. B puede no ser unitario. En efecto, en el ejemplo anterior vimos que $(2\mathbb{Z}, +, \cdot)$ es subanillo no unitario de $(\mathbb{Z}, +, \cdot)$, que es unitario.
2. Puede ser que B sea unitario pero $1_A \notin B$. En efecto, tenemos que $A \times B$ es unitario y $\{0\} \times B$ es un subanillo unitario, pero las unidades son distintas puesto que en el primer caso la unidad es $(1_A, 1_B)$ y en el segundo es $(0, 1_B)$.

Definición 6.4 (Subanillo unitario). Dado un anillo $(A, +, \cdot)$, llamamos **subanillo unitario** de A a un subanillo tal que $1_A \in B$ (por tanto $1_B = 1_A$).

Definición 6.5 (Unidad). Sea A un anillo conmutativo unitario y $a \in A$. Diremos que a es **unidad** si existe $b \in A$ tal que $a \cdot b = 1_A$.

Observación. 1. Está claro que 1_A es siempre unidad y 0_A nunca es unidad.

2. Si $a \in A$ es unidad, podemos hablar de su inverso multiplicativo como a^{-1} , puesto que de haberlo es único. En efecto, supongamos que existe $b, b' \in A$ tales que $a \cdot b = a \cdot b' = 1$, entonces,

$$b = b \cdot 1 = b \cdot (ab') = b'.$$

Definición 6.6 (Conjunto de unidades). Sea A un anillo conmutativo unitario. Definimos el **conjunto de todas las unidades** de A como

$$\mathcal{U}(A) = \{a \in A : a \text{ unidad}\}.$$

Observación. Es fácil ver que el conjunto de las unidades es un grupo abeliano con el producto. En efecto:

- Si $a, b \in \mathcal{U}(A)$, tenemos que

$$ab(b^{-1}a^{-1}) = 1_A.$$

Por tanto, $ab \in \mathcal{U}(A)$, por lo que la operación es interna.

- La asociatividad de la operación se deduce por ser A un anillo, al igual que la existencia de los inversos se deduce de la definición de unidad.
- El elemento neutro claramente es 1_A .

Por tanto, los inversos con el producto son únicos y si $a \cdot b = 1_A$, podemos escribir $b = a^{-1}$.

Ejemplo. 1. $\mathcal{U}(\mathbb{Q}) = \mathbb{Q}^*$. Lo mismo sucede en \mathbb{R} y \mathbb{C} .

$$2. \mathcal{U}(\mathbb{Z}) = \{1, -1\}.$$

$$3. \mathcal{U}(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n : \text{mcd}(a, n) = 1\}.$$

Proposición 6.2. Si $A \times B$ es un anillo unitario conmutativo, entonces $\mathcal{U}(A \times B) = \mathcal{U}(A) \times \mathcal{U}(B)$.

Demostración. Sea $(a, b) \in \mathcal{U}(A \times B)$, por lo que existe $(c, d) \in A \times B$ tal que

$$(a, b) \cdot (c, d) = (a \cdot c, b \cdot d) = (1_A, 1_B).$$

Por tanto, $a \in \mathcal{U}(A)$ y $b \in \mathcal{U}(B)$ y $(a, b) \in \mathcal{U}(A) \times \mathcal{U}(B)$. El recíproco es análogo. \square

Definición 6.7 (Divisor de cero y dominio de integridad). Sea A un anillo y $a \in A/\{0\}$. Diremos que a es **divisor de cero** si existe $b \in A/\{0\}$ tal que $a \cdot b = 0$. Decimos que A es **dominio de integridad** si no tiene divisores de cero.

Ejemplo. 1. Podemos ver que \mathbb{Z}_6 no es dominio de integridad, puesto que $[2] \cdot [3] = [0]$ y $[2], [3] \neq 0$, por lo que $[2]$ y $[3]$ son divisores de cero.
2. En general, \mathbb{Z}_p con p primo es dominio de integridad.

Proposición 6.3. Una unidad no es divisor de cero.

Demostración. Supongamos que $a \in \mathcal{U}(A)$ es divisor de cero. Por tanto, $\exists b \in A/\{0\}$ tal que $ab = 0_A$. Como a es unidad, existe a^{-1} , por tanto

$$ab = 0_A \Rightarrow a^{-1}(ab) = a^{-1}0_A \Rightarrow b = 0_A.$$

Esto contradice nuestra hipótesis, por lo que debe ser que a no es divisor de cero. \square

Definición 6.8 (Cuerpo). Sea $(A, +, \cdot)$ un anillo conmutativo unitario. Diremos que A es un **cuerpo** si $\mathcal{U}(A) = A/\{0\}$, es decir, todo elemento salvo el 0 tiene inverso multiplicativo.

Ejemplo. 1. Antes hemos visto que \mathbb{Q}, \mathbb{R} y \mathbb{C} son cuerpos.
2. Si $p \geq 2$ es primo, $(\mathbb{Z}_p, +, \cdot)$ también es cuerpo y lo llamaremos \mathbb{F}_p .
3. Como $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$ está claro que \mathbb{Z} no es un cuerpo. De manera similar, \mathbb{Z}_m con m no primo tampoco es un cuerpo.
4. $(\mathbb{Q}[t], +, \cdot)$ no es un cuerpo.

Observación. 1. Ser dominio de integridad no se conserva bajo productos directos. En efecto, sabemos que \mathbb{R} es un dominio de integridad, pero $(\mathbb{R}^2, +, \cdot)$ no es un dominio de integridad, puesto que $(0, 1) \cdot (1, 0) = (0, 0)$.
2. Un cuerpo es un dominio de integridad, puesto que las unidades del cuerpo son todas menos el cero y una unidad no puede ser divisor de cero.

Definición 6.9 (Característica de un anillo). Sea A un anillo unitario. Definimos la **característica** de A , $\text{char}(A)$, al mínimo $k \in \mathbb{N}$ tal que $k \cdot 1_A = 1_A + \cdots + 1_A = 0_A$. Si no existe $k \in \mathbb{N}$ con $k \cdot 1_A = 0_A$ decimos que A tiene **característica cero**.

Ejemplo. Es fácil ver que \mathbb{Q} , \mathbb{R} y \mathbb{C} tienen característica cero. Por otro lado, \mathbb{F}_p tiene característica p .

Observación. Si A es un anillo con característica finita y es dominio de integridad, entonces la característica es un número primo. Si suponemos que $\text{char}(A) = p \cdot m$ con p divisor primo, entonces tenemos que

$$(p1_A)(m1_A) = pm1_A = 0.$$

Como se trata de un dominio de integridad no puede haber divisores de cero, debe ser que $m = 1$.

6.0.1. Enteros de Gauss

Consideremos el anillo $(\mathbb{C}, +, \cdot)$ (sabemos que es un cuerpo) e $i \in \mathbb{C}$. Definimos el conjunto

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Como $\{1, i\}$ es una base de \mathbb{C} , sabemos que todos los elementos de $\mathbb{Z}[i]$ se pueden expresar de forma única como combinación lineal de esos dos elementos. Es fácil ver que $\mathbb{Z}[i]$ es un subanillo unitario de \mathbb{C} . En particular, tenemos que $\mathbb{Z}[i]$ tiene estructura de anillo unitario conmutativo. Como \mathbb{C} es dominio de integridad y $\mathbb{Z}[i]$ es subanillo, $\mathbb{Z}[i]$ es también dominio de integridad. Veamos que

$$\mathcal{U}(\mathbb{Z}[i]) = \{\pm 1, \pm i\}.$$

Es trivial ver que $\{\pm 1, \pm i\} \subset \mathcal{U}(\mathbb{Z}[i])$. Recíprocamente, si $a + bi \in \mathcal{U}(\mathbb{Z}[i])$ existe $c + di \in \mathcal{U}(\mathbb{Z}[i])$ tal que

$$(a + bi)(c + di) = 1 \iff (a - bi)(c - di) = 1.$$

Así, nos queda que

$$1 = (a + bi)(c + di)(a - bi)(c - di) = (a^2 + b^2)(c^2 + d^2).$$

Necesariamente debe ser que $a^2 + b^2 = 1$ y $c^2 + d^2 = 1$. Así, podemos considerar cuatro casos:

- Si $a = 0$ y $b = 1$, tenemos que $a + bi = i$.
- Si $a = 1$ y $b = 0$, tenemos que $a + bi = 1$.
- Si $a = -1$ y $b = 0$, tenemos que $a + bi = -1$.
- Si $a = 0$ y $b = -1$, tenemos que $a + bi = -i$.

Observación. Un entero de Gauss $z \in \mathbb{Z}[i]$ es una unidad si y solo si $z \cdot \bar{z} = 1$.

6.0.2. Anillo de polinomios

Sea A un anillo conmutativo unitario. Llamemos **anillo de polinomios** en la variable x a $A[x]$ donde sus elementos son

$$a_n x^n + \cdots + a_1 x + a_0, \quad a_i \in A, \quad n \in \mathbb{N}.$$

Además, decimos que $a_n x^n + \cdots + a_1 x + a_0$ es el polinomio 0 si y solo si $a_0 = \cdots = a_n = 0$. Dotamos a $A[x]$ de una operación de suma y producto que conocemos. Sean $p, q \in A[x]$ con

$$p = a_n x^n + \cdots + a_1 x + a_0, \quad a_i \in A, \quad n \in \mathbb{N}.$$

$$q = b_m x^m + \cdots + b_1 x + b_0, \quad b_j \in A, \quad m \in \mathbb{N}.$$

La suma la definimos de la forma:

$$p + q := \sum_{k=0}^{\max\{n,m\}} (a_k + b_k) x^k.$$

El producto lo definimos de la forma:

$$p \cdot q := \sum_{k=0}^{n+m} c_k x^k, \quad c_k = \sum_{i+j=k} a_i b_j.$$

Es fácil ver que $A[x]$ es un anillo conmutativo unitario y tiene como subanillo a $A \subset A[x]$.

Definición 6.10. Sea $A[x]$ un anillo de polinomios y sea $p \in A[x]$, con $p = a_n x^n + \cdots + a_1 x + a_0$.

1. Llamamos **grado** de p , $\text{grad}(p) = n$.^a
2. Diremos que a_n, \dots, a_1, a_0 son los **coeficientes** de p .
3. Al coeficiente a_0 lo llamamos **coeficiente independiente** y al coeficiente a_n lo llamamos **coeficiente director**, y escribimos $l(p) = a_n$.

^aPor convención decimos que $\text{grad}(0) = -\infty$, así tenemos que los elementos de A son los polinomios de grado menor o igual a 0.

Lema 6.1. Sean $p, q \in A[x]$ no nulos.

1. $\text{grad}(p + q) \leq \max\{\text{grad}(p), \text{grad}(q)\}$ y se da la igualdad si $l(p) + l(q) \neq 0$.
2. $\text{grad}(p \cdot q) \leq \text{grad}(p) + \text{grad}(q)$ y se da la igualdad si $l(p)l(q) \neq 0$ y tendremos que $l(p \cdot q) = l(p) \cdot l(q)$.

Ejemplo. Consideremos $\mathbb{Z}_6[x]$ y $3x + 1, 4x + 2 \in \mathbb{Z}_6[x]$. Tenemos que

$$(3x + 1) + (4x + 2) = 7x + 3 = x + 3.$$

$$(3x + 1) \cdot (4x + 2) = 12x^2 + 10x + 2 = 4x + 2.$$

Proposición 6.4. Sea A un anillo conmutativo unitario.

1. Si A es dominio de integridad, entonces $\mathcal{U}(A) = \mathcal{U}(A[x])$.
2. A es dominio de integridad si y solo si $A[x]$ es dominio de integridad.

Demostración. 1. Está claro que $\mathcal{U}(A) \subset \mathcal{U}(A[x])$ por ser $A \subset A[x]$. Sea $p \in \mathcal{U}(A[x])$, entonces existe $q \in \mathcal{U}(A[x])$ tal que $pq = 1$. Como $p, q \neq 0$, tenemos que $l(p), l(q) \neq 0$, por lo que $l(p)l(q) \neq 0$. Así, tenemos que

$$0 = \text{grad}(1) = \text{grad}(pq) = \text{grad}(p) + \text{grad}(q).$$

Por tanto, necesariamente debe ser que $\text{grad}(p) = \text{grad}(q) = 0$. Por tanto, $p = a_0, q = b_0 \in A$, por lo que $a_0b_0 = 1$. Así, $p \in \mathcal{U}(A)$.

2. Supongamos que A es dominio de integridad y sean $p, q \in A[x]$. Como $p, q \neq 0$ tenemos que $l(p), l(q) \neq 0$, por lo que $l(p)l(q) \neq 0$. Así,

$$l(pq) = l(p)l(q) \neq 0 \Rightarrow pq \neq 0.$$

Recíprocamente, como $A \subset A[x]$ es subanillo tenemos que si $A[x]$ es dominio de integridad, A también lo es. □

Observación. 1. Es fácil ver que $\text{char}(A) = \text{char}(A[x])$.

2. El anillo $A[x]$ no es un cuerpo, puesto que x no es unidad.

6.1. Ideales

Definición 6.11 (Ideal). Sea A un anillo unitario conmutativo y $\mathfrak{a} \subset A$ no vacío. Diremos que \mathfrak{a} es un **ideal** si:

(a) $(\mathfrak{a}, +)$ es subgrupo de $(A, +, 0_A)$.

(b) $\forall b \in \mathfrak{a}$ y $\forall x \in A$ se tiene que $bx \in \mathfrak{a}$, es decir, $\mathfrak{a}A \subset \mathfrak{a}$.

Ejemplo. 1. Algunos ideales triviales son $\{0\}$ y A .

2. Si $\mathfrak{a} \subsetneq A$ es un ideal, decimos que es un **ideal propio**.

3. Si $A = \mathbb{Z}$ y $\mathfrak{a} = 3\mathbb{Z}$, tenemos que \mathfrak{a} es un ideal. En general, $n\mathbb{Z}$ para $n \in \mathbb{N}$ es un ideal de \mathbb{Z} .

Observación. 1. Si $\mathfrak{a} \subset A$ es un ideal y $u \in \mathfrak{a}$ es unidad, tenemos que $\mathfrak{a} = A$. En efecto, si $x \in A$, tenemos que $(xu^{-1})u \in \mathfrak{a}A \subset \mathfrak{a}$. Así, los ideales propios no tienen unidades.

2. Sea $b \in A$. Decimos que $(b) := bA = \{bx : x \in A\}$ es el **ideal principal generado por b** .

6.1.1. Construcción del anillo cociente

Sea $(A, +, \cdot)$ un anillo conmutativo unitario y $\mathfrak{a} \subsetneq A$ un ideal. Entonces, sabemos que \mathfrak{a} es subgrupo normal de A , por ser A abeliano. Por tanto, podemos considerar el grupo A/\mathfrak{a} . Recordamos que

$$[a] = [b] \iff a - b \in \mathfrak{a}.$$

Definamos la suma de la forma:

$$+ : A/\mathfrak{a} \times A/\mathfrak{a} \rightarrow A/\mathfrak{a} : ([a_1], [a_2]) \rightarrow [a_1] + [a_2] = [a_1 + a_2].$$

De forma análoga podemos definir el producto,

$$\cdot : A/\mathfrak{a} \times A/\mathfrak{a} \rightarrow A/\mathfrak{a} : ([a_1], [a_2]) \rightarrow [a_1] \cdot [a_2] := [a_1 \cdot a_2].$$

Veamos que la aplicación está bien definida. Supongamos que $[a_1] = [a_2]$ y $[b_1] = [b_2]$. Tenemos que

$$a_1 b_1 - a_2 b_2 = a_1 b_1 - a_2 b_1 - a_2 b_2 + a_2 b_1 = b_1 \underbrace{(a_1 - a_2)}_{\in \mathfrak{a}} + a_2 \underbrace{(b_1 - b_2)}_{\in \mathfrak{a}} \in \mathfrak{a}.$$

Así tenemos que $[a_1 b_1] = [a_2 b_2]$ y la operación está bien definida. Así, diremos que $(A/\mathfrak{a}, +, \cdot)$ es el **anillo cociente** que es conmutativo y unitario.

Ejemplo. 1. Consideremos $A = \mathbb{Z}$ y $\mathfrak{a} = n\mathbb{Z}$, que es un ideal por un ejemplo anterior. Sabemos que $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. Tenemos que \mathbb{Z} es dominio de integridad y $n\mathbb{Z}$ también lo es por ser subanillo, sin embargo \mathbb{Z}_n sólo es dominio de integridad si n es primo. Por tanto, ser dominio de integridad no se conserva por cocientes.

2. Sea $A = \mathbb{R}[x]$ y $\mathfrak{a} = (x^2 + 1)$. Estudiemos el conjunto cociente $\mathbb{R}[x]/\mathfrak{a}$. Tenemos que $[x^2 + 1] = [0]$, por lo que $[x^2] = [-1]$. Así, si $k \in \mathbb{N}$, tenemos que

$$[x^{2k}] = [x^2]^k = [-1]^k.$$

$$[x^{2k+1}] = [x^2]^k \cdot [x] = [(-1)^k] [x].$$

Así, si tomamos el polinomio $a_n x^n + \dots + a_1 x + a_0$, tenemos que

$$[a_n x^n + \dots + a_1 x + a_0] = [b][x] + [c].$$

Así, si $p \in \mathbb{R}[x]/\mathfrak{a}$, tenemos que $p = bx + c$. Análogamente, si $q \in \mathbb{R}[x]/\mathfrak{a}$ con $q = dx + e$, tenemos que

$$p + q = (b + d)x + (c + e).$$

$$p \cdot q = (bx + c)(dx + e) = bdx^2 + (be + cd)x + ce = (be + cd)x + (ce - bd).$$

Así, para cada elemento $p \in \mathbb{R}[x]/\mathfrak{a}$ podemos encontrar un elemento inverso respecto a la multiplicación. Así, tenemos que $\mathbb{R}[x]/\mathfrak{a}$ es un cuerpo. En efecto, se trata de \mathbb{C} .

Definición 6.12. Sea A un anillo conmutativo unitario y $\mathfrak{a}, \mathfrak{b} \subset A$ ideales.

1. Definimos el **ideal suma** como $\mathfrak{a} + \mathfrak{b} := \{a + b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$.
2. Definimos el **ideal intersección** como $\mathfrak{a} \cap \mathfrak{b} := \{x \in A : x \in \mathfrak{a}, x \in \mathfrak{b}\}$.
3. Definimos el **ideal producto** como $\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{k=1}^n x_k y_k : x_k \in \mathfrak{a}, y_k \in \mathfrak{b}, n \in \mathbb{N} \right\}$.

Definición 6.13 (Ideal generado por un conjunto). Sea A un anillo conmutativo unitario y $\emptyset \neq S \subset A$. Llamamos **ideal generado por S** a

$$(S) := \{a_1 s_1 + \cdots + a_k s_k : s_i \in S, a_i \in A, k \in \mathbb{N}\}.$$

Además, (S) es el menor ideal que contiene a S y si $S = \{s_1, \dots, s_n\}$, tenemos que $(S) = (s_1, \dots, s_n) = (s_1) + \cdots + (s_n)$.

Ejemplo. En \mathbb{Z} tenemos que $(4, 6) = (2)$. Sin embargo, en \mathbb{R} , $(4, 6) = \mathbb{R}$.

Definición 6.14 (Ideal primo). Sea A un anillo conmutativo unitario. Sea $\mathfrak{p} \subsetneq A$ un ideal. Diremos que \mathfrak{p} es un **ideal primo** si $xy \in \mathfrak{p}$ implica que $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$, $\forall x, y \in A$.

Ejemplo. En \mathbb{Z} sabemos que $n\mathbb{Z}$ son los ideales, con $n \in \mathbb{N}$. En efecto, si $\mathfrak{a} \subset \mathbb{Z}$ es un ideal, tenemos que es subgrupo aditivo, por lo que $\mathfrak{a} = n\mathbb{Z}$ para algún $n \in \mathbb{N}$. Entonces, tenemos que $n\mathbb{Z}$ es ideal primo si y solo si n es primo.

Proposición 6.5. Sea A un anillo conmutativo unitario y $\mathfrak{p} \subset A$ un ideal. Tenemos que \mathfrak{p} es primo si y solo si A/\mathfrak{p} es dominio de integridad.

Demostración. Sabemos que $\mathfrak{p} \neq A$ y que A/\mathfrak{p} es un anillo también conmutativo unitario. Además, si $a, b \in A$, tenemos que

$$[ab] = [a][b] = [0] \iff ab \in \mathfrak{p}.$$

- (i) Supongamos que \mathfrak{p} es primo y sean $[a], [b] \in A/\mathfrak{p}$ con $[a] \cdot [b] = [0]$. Por lo visto anteriormente, tenemos que $ab \in \mathfrak{p}$, por lo que debe ser que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, y en consecuencia debe ser que $[a] = [0]$ o $[b] = [0]$. Por tanto, A/\mathfrak{p} es dominio de integridad.
- (ii) Supongamos que A/\mathfrak{p} es dominio de integridad y $ab \in \mathfrak{p}$. Así, tenemos que $[ab] = [a][b] = [0]$. Como A/\mathfrak{p} es dominio de integridad debe ser que $[a] = 0$ o $[b] = 0$, es decir, $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. Por tanto, \mathfrak{p} es primo.

□

Definición 6.15 (Ideal maximal). Sea A un anillo y $\mathfrak{m} \subsetneq A$ un ideal. Diremos que es un **ideal maximal** si no existe un ideal $\mathfrak{a} \subset A$ tal que $\mathfrak{m} \subsetneq \mathfrak{a}$.

Proposición 6.6. Sea A un anillo conmutativo unitario y $\mathfrak{m} \subset A$ un ideal. Tenemos que \mathfrak{m} es maximal si y solo si A/\mathfrak{m} es cuerpo.

Demostración. (i) Supongamos que $\mathfrak{m} \subset A$ es un ideal maximal. Tenemos que ver que $A/\mathfrak{m} - \{[0]\} \subset \mathcal{U}(A/\mathfrak{m})$. Sea $[a] \in A/\mathfrak{m}$ con $[a] \neq [0]$, es decir, $a \in A - \mathfrak{m}$. Como $a \notin \mathfrak{m}$, podemos considerar el ideal $(\mathfrak{m} \cup \{a\}) \supsetneq \mathfrak{m}$. Como \mathfrak{m} es maximal, necesariamente debe ser que $A = (\mathfrak{m} \cup \{a\})$. Así, $1 \in A = (\mathfrak{m} \cup \{a\})$, por lo que

existe $b \in \mathfrak{m}$ y $c \in A$ tal que $1 = b + ac$. Por tanto,

$$[1] = [ac] = [a][c] \Rightarrow [a] \in \mathcal{U}(A/\mathfrak{m}).$$

(ii) Supongamos que A/\mathfrak{m} es un cuerpo y existe un ideal \mathfrak{m}' tal que $\mathfrak{m} \subsetneq \mathfrak{m}'$. Queremos ver que $\mathfrak{m}' = A$, para ello basta con ver que $1 \in \mathfrak{m}'$. Sea $a \in \mathfrak{m}' - \mathfrak{m}$. Como A/\mathfrak{m} es un cuerpo, existe $b \in A/\mathfrak{m}$ tal que $[1] = [a][b] = [ab]$. Así, tenemos que

$$[1 - ab] = [0] \Rightarrow 1 - ab \in \mathfrak{m} \Rightarrow 1 \in \mathfrak{m} + (a).$$

Por tanto, debe ser que $1 \in \mathfrak{m}'$. □

Ejemplo. En $\mathbb{R}[x]$, el ideal $(x^2 + 1)$ es maximal puesto que $\mathbb{R}[x]/(x^2 + 1)$ es un cuerpo.

Corolario 6.1. Todo ideal maximal es primo.

Demostración. Si $\mathfrak{m} \subset A$ es un ideal maximal tenemos que A/\mathfrak{m} es un cuerpo, por lo que A/\mathfrak{m} es dominio de integridad, por lo que \mathfrak{m} es primo. □

Ejemplo. En \mathbb{Z} , los ideales maximales son los $p\mathbb{Z}$ donde p es primo. Es decir, en \mathbb{Z} los ideales primos son los maximales.

6.2. Homomorfismos de anillos

Definición 6.16 (Homomorfismo de anillos). Sean A y B anillos y $f : A \rightarrow B$. Diremos que f es un **homomorfismo de anillos** si:

1. $f(a + b) = f(a) + f(b), \forall a, b \in A$.
2. $f(a \cdot b) = f(a) \cdot f(b), \forall a, b \in A$.

Diremos que es un **homomorfismo de anillos unitarios** si A y B son unitarios y $f(1) = 1$.

Definición 6.17. Dado un homomorfismo de anillos $f : A \rightarrow B$:

1. Si f es biyectiva la llamamos **isomorfismo**.
2. Si f es inyectiva la llamamos **monomorfismo**.
3. Si f es sobreyectiva la llamamos **epimorfismo**.
4. Si $A = B$, a f la llamamos **endomorfismo**.

Proposición 6.7. Sea $f : A \rightarrow B$ un homomorfismo de anillos unitarios.

1. $f(0) = 0$.
2. $\forall n \in \mathbb{Z}, \forall a \in A, f(na) = nf(a)$.
3. Si $n \in \mathbb{N}, \forall a \in A, f(a^n) = f(a)^n$.
4. Si $a \in \mathcal{U}(A)$, entonces $f(a) \in \mathcal{U}(B)$. En particular, $f|_{\mathcal{U}(A)} : \mathcal{U}(A) \rightarrow \mathcal{U}(B)$ es un homomorfismo de grupos y $f(a^n) = f(a)^n, \forall n \in \mathbb{Z}$.

Demostración. 1. Como f es homomorfismo de grupos es trivial.

2. Sea $n \in \mathbb{N}$ y $a \in A$,

$$f(na) = f(a + \cdots + a) = f(a) + \cdots + f(a) = nf(a).$$

3. Sea $n \in \mathbb{N}$ y $a \in A$,

$$f(a^n) = f(a \cdots a) = f(a) \cdots f(a) = f(a)^n.$$

4. Sea $a \in \mathcal{U}(A)$, por lo que existe $x \in A$ tal que $ax = 1$. Así, tenemos que

$$f(a)f(x) = f(ax) = f(1) = 1 \Rightarrow f(a) \in \mathcal{U}(B).$$

□

Ejemplo. 1. Sea A un anillo, entonces la identidad es un homomorfismo de anillos unitario.

2. Si $B \subset A$ es un subanillo unitario, la función inclusión $i : B \rightarrow A$ es homomorfismo de anillos unitarios.
3. La aplicación $f : \mathbb{Z} \rightarrow \mathbb{R} : n \rightarrow 2n$ no es un homomorfismo de anillos unitario puesto que $f(1) = 2 \neq 1$.
4. La aplicación $f : A \rightarrow A \times A : a \rightarrow (a, 0)$ es un homomorfismo de anillos no unitario, puesto que $f(1) = (1, 0) \neq (1, 1)$.