

# Resumen Grupos

Mario Calvarro Marines



# Índice general

---

<b>1. Generalidades sobre grupos.</b>	
<b>Fórmula de Lagrange</b>	<b>1</b>
1.1. Grupos cíclicos y diedrales . . . . .	1
1.2. Fórmula de Lagrange . . . . .	2
<b>2. Subgrupos normales y homomorfismos</b>	<b>5</b>
2.1. Subgrupos normales . . . . .	5
2.1.1. Grupo cociente . . . . .	5
2.2. Homomorfismos de grupos . . . . .	6
2.2.1. Teoremas de isomorfía . . . . .	6
<b>3. Grupos de permutaciones</b>	<b>9</b>
3.1. Generalidades . . . . .	9
3.1.1. Grupo simétrico . . . . .	9
3.2. Teorema de Abel . . . . .	10
<b>4. Acción de un grupo sobre un conjunto</b>	<b>13</b>
4.1. Ecuación de clases . . . . .	13
4.1.1. Acciones, órbitas y estabilizadores . . . . .	13
4.1.2. Órbitas y estabilizadores . . . . .	13
4.1.3. Aplicaciones a los $p$ -grupos . . . . .	14
4.2. Teorema de Cauchy . . . . .	14
<b>5. Teoremas de Sylow. Grupos resolubles</b>	<b>15</b>
5.1. Teoremas de Sylow . . . . .	15

<b>6. Grupos abelianos finitos. Función de Euler</b>	<b>17</b>
6.1. Teorema de estructura de los grupos abelianos finitos. . . . .	17

# Generalidades sobre grupos.

## Fórmula de Lagrange

---

### Grupos cíclicos y diedrales

---

#### Definición (Grupo)

Un conjunto  $G$  y la operación  $G \times G \rightarrow G, (a, b) \mapsto ab$  se dicen **grupo** si cumplen:

- Asociatividad.
- Elemento neutro.
- Elementos inversos.

Si además es conmutativo, se dice **abeliano**.

---

#### Proposición

Sea  $G$ , grupo, y  $g \in G \Rightarrow$

$$\{gx : x \in G\} = G = \{xg : x \in G\}$$

---

#### Definición (Subgrupo)

Se dice que  $H \subset G$  es un **subgrupo** de  $G$  si:

- $1_G \in H$
  - $ab^{-1} \in H, \forall a, b \in H$
- 

#### Definición (Subgrupo generado por un subconjunto)

Sea  $G$ , grupo, y  $\emptyset \neq S \subset G$ . Llamamos **subgrupo generado por  $S$**  a:

$$\langle S \rangle = \bigcap_{H \in \mathcal{H}_S} H$$

donde  $\mathcal{H}_S$  es la familia de los subgrupos de  $G$  que contienen a  $S$ .

Otra forma de expresarlo es:

$$\mathcal{W}(S) = \{s_1^{n_1}, \dots, s_k^{n_k} : s_i \in S \text{ \& } n_j \in \mathbb{N}\}$$

y diremos que un grupo es finitamente generado si  $\exists S \subset G : \langle S \rangle = G$ .

---

### Proposición (Identidad de Bézout)

Sean  $m, n \in \mathbb{Z} \setminus \{0\}$  y  $d := \text{mcd}(m, n)$ . Entonces,

$$\exists a, b \in \mathbb{Z} : d = am + bn$$

---

### Definición

Sea  $H \leq G$

- Sea  $a \in G$ . Llamamos **conjugado** de  $H$  vía  $a$ :

$$H^a := a^{-1}Ha := \{a^{-1}ha : h \in H\}$$

Diremos que  $H$  y  $H^a$  son **conjugados**

- Llamamos **centralizador** de  $H$  en  $G$  a:

$$C_G(H) := \{a \in G : ah = ha \ \forall h \in H\}$$

En particular,  $Z(G) := C_G(G)$  se denomina **centro** de  $G$ .

### Proposición

Sea  $G$  un grupo cíclico (generado por un solo elemento), entonces  $H \leq G$  es cíclico.

---

## Fórmula de Lagrange

### Proposición

Sean  $H, K \leq G$ . Entonces,

$$\text{ord}(H) \text{ord}(K) = \text{Card}(HK) \text{ord}(H \cap K)$$

En particular,  $\text{Card}(HK) \leq \text{ord}(H) \text{ord}(K)$

---

### Definición (Clases laterales)

Sean  $H \leq G$ .

- Definimos la clase de equivalencia  $\mathcal{R}_H$  tal que:

$$a\mathcal{R}_H b \Leftrightarrow ab^{-1} \in H$$

y decimos que  $a$  y  $b$  son **congruentes por la derecha**.

$$Ha := \{ha : h \in H\}$$

- Definimos la clase de equivalencia  $\mathcal{R}^H$  tal que:

$$a\mathcal{R}^H b \Leftrightarrow a^{-1}b \in H$$

y decimos que  $a$  y  $b$  son **congruentes por la izquierda**.

$$aH := \{ah : h \in H\}$$

Las clases de equivalencia definidas por estas relaciones tienen el mismo número de elementos que denominamos **índice** de  $H$  en  $G$ ,  $[G : H]$ .

---

### Corolario (Fórmula de Lagrange)

Sea  $G$  un grupo finito.

- $H \leq G$ , entonces:

$$\text{ord}(G) = \text{ord}(H) [G : H]$$

- Si  $K \leq G$  y  $\text{mcd}(\text{ord}(H), \text{ord}(K)) = 1$ , entonces  $H \cap K = \{1_G\}$ .
- Si el orden de  $G$  es un primo, entonces  $G$  es cíclico y está generado por cualquiera de sus elementos distintos de  $1_G$ .

### Corolario (Pequeño teorema de Fermat)

Dados un entero primo  $p$  y  $k \in \mathbb{Z}$  se cumple:

$$k^p \equiv k \pmod{p}$$

### Lema

Sea  $G$  grupo y  $a, b \in G$ , elementos de orden  $n, m$ , entonces:

- $\forall k \in \mathbb{Z}, o(a^k) = \frac{n}{\text{mcd}(n, k)}$ .
- Si  $ab = ba$  y  $\text{mcd}(m, n) = 1 \Rightarrow o(ab) = mn$ .

### Proposición

Sea  $G$  un grupo cíclico finito. Para cada divisor  $d > 0$  de  $\text{ord}(G)$ ,  $\exists! H \leq G : \text{ord}(H) = d$ .

### Proposición (Transitividad del índice)

Sean  $H, K \leq G : H \subset K$  y  $[G : H]$  es finito. Entonces, también lo son  $[G : K]$  y  $[K : H]$  y

$$[G : H] = [G : K] \cdot [K : H]$$





# Subgrupos normales y homomorfismos

---

## Subgrupos normales

---

### Definición

Sean  $H, K \leq G$ , tal que  $H \subset K$ .

- $H$  es **subgrupo normal** de  $K$  si  $Ha = aH, \forall a \in K \Leftrightarrow a^{-1}Ha = H$ . En notación,  $H \triangleleft K$ .
- Denominamos **normalizador** de  $H$  en  $G$ ,  $N_G(H)$ , al subgrupo de  $G$  definido por:

$$N_G(H) := \{a \in G : Ha = aH\} = \{a \in G : a^{-1}Ha = H\}$$

Por tanto,  $C_G(H) \subset N_G(H)$

- Un grupo será **simple** si sus únicos subgrupos normales son los triviales.
- 

### Proposición

- Sean  $H \triangleleft G$  y  $K \leq G$ , entonces  $HK \leq G$  y  $H \triangleleft HK$ .
- Sean  $H, K \triangleleft G$ , entonces:
  1.  $HK \triangleleft G$ .
  2.  $H \cap K \triangleleft G$ . Si, además,  $H \cap K = \{1_G\} \Rightarrow hk = kh, \forall k \in K, h \in H$ .
- Sea  $a \in G$  una involución, entonces  $\langle a \rangle \triangleleft G \Leftrightarrow a \in Z(G)$ .
- Sean  $S$ , generador, y  $H \leq G$  tales que,  $s^{-1}Hs = H, \forall s \in S$ , entonces  $H \triangleleft G$ .
- Sean  $H \leq G$  y  $K \triangleleft G$  finito tal que  $H \subset K$ , entonces  $H \triangleleft G$ .

### Proposición (Índice del normalizador)

Sean  $H \leq G$  finito y  $\Sigma := \{a^{-1}Ha : a \in G\}$ . Entonces,  $\text{Card}(\Sigma) = [G : N_G(H)]$ .

## Grupo cociente

Sea  $H \triangleleft G$  y utilizando la operación:

$$\begin{aligned} G/H \times G/H &\rightarrow G/H \\ (Ha, Hb) &\mapsto Hab \end{aligned}$$

definimos un **grupo cociente**.

### Teorema (de Correspondencia)

Sean  $H \triangleleft G$ ,  $\Sigma_H(G) := \{L \leq G : H \subset L\}$  y  $\Sigma(G/H) := \{L \leq G/H\}$ . Entonces,

$$\begin{aligned}\Sigma_H(G) &\rightarrow \Sigma(G/H) \\ K &\mapsto K/H\end{aligned}$$

es una biyección.

### Lema (Normalizador del cociente)

Sean  $H \leq G$  y  $K \triangleleft G : K \subset H$ . Entonces,

$$N_G(H)/K = N_{G/K}(H/K)$$

En particular,  $H \triangleleft G \Leftrightarrow H/K \triangleleft G/K$ .

## Homomorfismos de grupos

### Definición

Dados  $G_1, G_2$  y una aplicación  $f : G_1 \rightarrow G_2$ , se dice que es **homomorfismo** de grupos si  $f(ab) = f(a)f(b)$ .

### Observación:

- $\forall H_1 \leq G, H_2 := f(H_1) \leq G_2$ . En particular,  $\text{img } f := f(G_1) \leq G_2$  y si  $H_1 \triangleleft G_1 \Rightarrow H_2 \triangleleft \text{img } f$ .
- $\forall H_2 \leq G_2, H_1 := f^{-1}H_2 \leq G_1$ . Además,  $H_2 \triangleleft G_2 \Rightarrow H_1 \leq G_1$ .  
En concreto,  $\ker f \triangleleft G$ .
- $f$  es inyectivo  $\Leftrightarrow \ker f = \{1_G\}$ .
- La composición de homomorfismos es homomorfismo.
- Llamamos **isomorfismo** a  $f$  homomorfismo biyectivo tal que  $f^{-1}$  también es homomorfismo. En tal caso, diremos que  $G_1 \simeq G_2$  son isomorfos.

### Ejemplo:

- Sea  $f : G \rightarrow G$  isomorfismo. Lo llamaremos **automorfismo** y el conjunto  $\text{Aut}(G)$  con la operación  $f \cdot g = g \circ f$  forma un subgrupo de  $\text{Bij}(G)$ .
- Dados  $H \leq G$  y  $a \in N_G(H)$  las aplicaciones:

$$\begin{aligned}f_a : H &\rightarrow H \\ x &\mapsto a^{-1}xa\end{aligned}$$

forman el grupo  $\text{Int}_G(H)$ , **automorfismos internos** de  $H$ , que es un subgrupo de  $\text{Aut}(G)$ .

## Teoremas de isomorfía

### Teorema (Primer teorema de isomorfía)

Dado  $f : G_1 \rightarrow G_2$  homomorfismo, la aplicación:

$$\begin{aligned}\hat{f} : G_1/\ker f &\rightarrow \text{img } f \\ a\ker f &\mapsto f(a)\end{aligned}$$

es un isomorfismo.

### Corolario

- Sea  $f : G_1 \rightarrow G_2$  homomorfismo sobreyectivo y  $H \triangleleft G$ . Entonces,  $G_1/f^{-1}(H) \simeq G_2/H$ .
- Sea  $H \leq G$ , entonces  $N_G(H)/C_G(H) \simeq \text{Int}_G(H)$ . En particular,  $G/Z(G) \simeq \text{Int}(G)$ .



# Grupos de permutaciones

---

## Generalidades

### Grupo simétrico

Siendo  $n \in \mathbb{N}$ , denotamos  $I_n := \{x \in \mathbb{Z} : 1 \leq x \leq n\}$  y  $\mathcal{S}_n$  al conjunto de biyecciones de  $I_n$  en si mismo, que tiene  $\text{Card}(\mathcal{S}_n) = n!$ . Forma el llamado **grupo de permutaciones** con la composición “al revés”.

$$\begin{aligned}\sigma \cdot \tau &:= \sigma\tau : I_n \rightarrow I_n \\ j &\mapsto \tau(\sigma(j))\end{aligned}$$

### Teorema (de Cayley)

Todo grupo  $G$  es isomorfo a un subgrupo de  $\text{Biy}(G)$ . En particular, todo grupo finito es isomorfo a un subgrupo del grupo de permutaciones.

---

### Definición (Soporte)

Llamamos **soporte** de una permutación  $\sigma \in \mathcal{S}_n$  al conjunto:

$$\text{sop}(\sigma) := \{j \in I_n : \sigma(j) \neq j\}$$

y decimos que dos permutaciones son **disjuntas** si lo son sus soportes.

---

### Proposición

- Sea  $j \in \text{sop}(j)$ , entonces  $\sigma(j) \in \text{sop}(j)$ .
- Dos permutaciones disjuntas conmutan.

---

### Definición (Ciclos)

Una permutación  $\sigma \in \mathcal{S}_n$  se denomina **ciclo de longitud  $k$**  si  $\exists i_1, \dots, i_k \in I_n$  tales que  $\text{sop}(\sigma) = \{i_1, \dots, i_k\}$  y

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k \text{ \& } \sigma(i_k) = i_1$$

Si es de longitud 2 lo denominaremos como **transposición**.

---

### Proposición

- Toda permutación es composición de ciclos disjuntos y esta factorización es única salvo el orden de los factores.

- Si  $\sigma_1, \dots, \sigma_r$  son ciclos disjuntos y  $\text{long}(\sigma_i) \leq \text{long}(\sigma_{r+1}), \forall 1 \leq i \leq r-1$ , se llama **estructura cíclica** de  $\sigma := \sigma_1 \cdots \sigma_r$  a la  $r$ -tupla  $(\text{long}(\sigma_1), \dots, \text{long}(\sigma_r))$ .

### Lema

Siendo  $\sigma, \tau \in \mathcal{S}_n$  disjuntas tal que  $o(\sigma) = \ell$  y  $o(\tau) = m$ , entonces  $o(\sigma\tau) = \text{mcm}(\ell, m)$

### Corolario

Sea  $\sigma := \sigma_1 \cdots \sigma_k$  una factorización en ciclos de la permutación. Entonces,

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

### Definición (Índice)

- $\forall \sigma \in \mathcal{S}_n$  consideramos el endomorfismo,  $f_\sigma : \mathbb{R}^n \rightarrow \mathbb{R}^n$  que cumple que  $f_\sigma(e_j) = e_{\sigma^{-1}(j)}$ . Entonces,

$$\begin{aligned} \psi : \mathcal{S}_n &\rightarrow \text{Aut}(\mathbb{R}^n) \\ \sigma &\mapsto f_\sigma \end{aligned}$$

es homomorfismo de grupos.

La matriz de  $f_\sigma$  proviene de desordenar las columnas de la identidad, por tanto,  $\det(f_\sigma) \in \{1, -1\}$ . Definimos, pues, el homomorfismo **índice**:

$$\varepsilon := \det \circ \psi : \mathcal{S}_n \rightarrow \mathcal{U}_2$$

- Al kernel de  $\varepsilon$  se le denota  $\mathcal{A}_n$ , **n-ésimo grupo alternado**. Si  $\sigma \in \mathcal{A}_n$  se dice **par** y en caso contrario **impar**.

### Lema

Las transposiciones constituyen un sistema generador de  $\mathcal{S}_n$ .

### Proposición

El ciclo  $\sigma := (a_1, \dots, a_k) \in \mathcal{S}_n \in \mathcal{A}_n \Leftrightarrow k$  impar.

### Proposición (Sistemas generadores de $\mathcal{S}_n$ y $\mathcal{A}_n$ )

- $\mathcal{S}_n$  es generado por  $\{\alpha_i := (1, i) : 2 \leq i \leq n\}$ .
- $\mathcal{S}_n$  es generado por  $\{\tau_i := (i, i+1) : 1 \leq i \leq n-1\}$ .
- $\mathcal{S}_n$  es generado por  $(1, 2)$  y  $(1, \dots, n)$ .
- $\mathcal{A}_n$  es generado por  $\{\sigma_i := (1, 2, i) : 3 \leq i \leq n\}$ .

## Teorema de Abel

### Teorema (De Abel)

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

### Corolario

Si  $n \geq 5$ , entonces  $\mathcal{A}_n$  es el único subgrupo normal propio de  $\mathcal{S}_n$ .

---

### Definición

$H \leq \mathcal{S}_n$  será **transitivo** si  $\forall (i, j)$  tal que  $1 \leq i, j \leq n$ ,  $\exists \sigma \in H$  tal que  $\sigma(i) = j$ .

---

### Proposición

Si  $p \in \mathbb{Z}$  es primo y  $H \leq \mathcal{S}_p$  transitivo que contiene una transposición, entonces  $H = \mathcal{S}_p$ .





# Acción de un grupo sobre un conjunto

---

## Ecuación de clases

### Acciones, órbitas y estabilizadores

---

#### Definición

Denominamos **acción de un grupo**  $G$  sobre un conjunto  $X \neq \emptyset$  a cualquier homomorfismo:

$$\begin{aligned} G &\rightarrow \text{Bij}(X) \\ g &\mapsto \tilde{g} \end{aligned}$$

Esto define una relación de equivalencia tal que  $x \sim y \Leftrightarrow \exists g \in G : y = \tilde{g}(x)$ .

La clase de equivalencia definida así se denomina **G-órbita** de  $x$  bajo la acción de  $G$ ,  $O_{G,x} := \{\tilde{g}(x) : g \in G\}$ .

---

Observación:

$\{O_x : x \in X\}$  particiona  $X$  y, siendo  $R \subset X$  un conjunto de representantes de las clases, se cumple  $X = \bigsqcup_{x \in R} O_x$ . Por tanto,  $\text{Card}(X) = \sum_{x \in R} \text{Card}(O_x)$ .

---

#### Definición

Llamamos **estabilizador** de  $x \in X$  bajo la acción de  $G$  al subgrupo:

$$\text{Stab}_G(x) := \{g \in G : \tilde{g}(x) = x\}$$

---

### Órbitas y estabilizadores

#### Proposición (Cardinal de una órbita)

Si  $G$  actúa sobre  $X$  y  $x \in X$ , se cumple  $\text{Card}(O_x) = [G : \text{Stab}_G(x)]$ .

#### Corolario (Fórmula de las órbitas)

Sea  $R$  conjunto de representantes de las órbitas de  $X$ , finito, bajo la acción de  $G$ . Entonces,

$$\text{Card}(X) = \sum_{x \in R} [G : \text{Stab}_G(x)]$$

## Aplicaciones a los $p$ -grupos

---

### Definición

Llamamos  **$p$ -grupo** a aquellos cuyo orden es potencia de un número primo  $p$ .

---

### Lema (Centro de un $p$ -grupo)

Sea  $H \neq \{1_G\} \leq G$ ,  $p$ -grupo. Entonces,  $H \cap \mathcal{Z}(G) \neq \{1_G\}$ . En particular,  $\mathcal{Z}(G) \neq \{1_G\}$ , por lo que  $G$  no es simple salvo si  $\text{ord}(G) = p$ .

### Lema (Criterio de abelianidad)

- Sean  $p$ ,  $n^\circ$  primo,  $n \in \mathbb{N}$  y  $G : \text{ord}(G) = p^n$ . Entonces,  $\text{ord}(\mathcal{Z}(G)) \neq p^{n-1}$ . En particular, si  $\text{ord}(G) = p^3$ , no abeliano, entonces  $\text{ord}(\mathcal{Z}(G)) = p$ .
- Todo  $G$  de orden  $p^2$ , es abeliano.

### Lema

Sean  $p$ ,  $n^\circ$  primo,  $G$  finito y  $H \leq G$  que es  $p$ -grupo. Entonces  $[G : H] \equiv [N_G(H) : H] \pmod{p}$ .

## Teorema de Cauchy

### Teorema (de Cauchy)

Sea  $p$ ,  $n^\circ$  primo, y  $G$  grupo de orden múltiplo de  $p$ . Entonces, el  $n^\circ$  de subgrupos de  $G$  de orden  $p$  es congruente con 1 mód  $p$ . En particular,  $\exists a \in G$  de orden  $p$ .

# Teoremas de Sylow. Grupos resolubles

---

## Teoremas de Sylow

### Teorema (Primer teorema de Sylow)

Sean  $p$ ,  $n^o$  primo, y  $G$ , finito, cuyo orden es  $\text{ord}(G) := p^n m$ ;  $m, n \in \mathbb{N}$  y  $p \nmid m$ . Sean  $H, K \leq G$  de orden  $p^n$ . Entonces,  $H$  y  $K$  son conjugados.

---

### Definición

Llamamos **p-subgrupo de Sylow** a los subgrupos de  $G$  de orden  $p^n$ .

---

### Corolario

Sea  $p$ ,  $n^o$  primo, y  $G$ , finito, cuyo orden es  $\text{ord}(G) = p^n m$ ;  $n, m \in \mathbb{N}$  y  $p \nmid m$ . Sea  $H$  un  $p$ -subgrupo de Sylow de  $G$ .

- $H \triangleleft G \Leftrightarrow$  es el único  $p$ -subgrupo.
- Se cumple  $N_G(N_G(H)) = N_G(H)$

### Teorema (Segundo teorema de Sylow)

- Sea  $G$ , finito, tal que  $\text{ord}(G) := p^n m$ ;  $p$ ,  $n^o$  primo, y  $n, m \in \mathbb{N}$  tales que  $p \nmid m$ . Entonces, si  $i \in \mathbb{Z} : 0 \leq i \leq n-1$  y  $H_i \leq G$  de orden  $p^i$ ,  $\exists H_{i+1} \leq G$  de orden  $p^{i+1}$  tal que  $H_i \triangleleft H_{i+1}$ .
- En particular,  $\exists H_1, \dots, H_n \leq G$  de ordenes  $p, p^2, \dots, p^n$ , tales que  $H_i \triangleleft H_{i+1}$ .
- $\forall H \leq G$  de orden potencia de  $p$  está contenido en alguno de los  $p$ -subgrupos de Sylow.

### Corolario

Sean  $p$ ,  $n^o$  primo,  $n \in \mathbb{N}$  y  $G$  de orden  $p^n$ . Entonces,  $\forall k = 0, \dots, n$ ,  $\exists H_k \triangleleft G$  de orden  $p^k$ .

### Teorema (Tercer teorema de Sylow)

Sea  $p$ ,  $n^o$  primo, y  $G$ , finito, tal que  $\text{ord}(G) = p^n m$ ;  $n, m \in \mathbb{N}$  y  $p \nmid m$ . Entonces,  $n_p := n^o$  de  $p$ -subgrupos de Sylow cumple:

- $n_p = [G : N_G(H)]$ ,  $\forall H$   $p$ -subgrupo de  $G$ .
- $n_p$  divide a  $m$  y  $n_p - 1$  es múltiplo de  $p$ .

**Corolario (Teorema de Wilson)**

$\forall p > 0$ , primo, se cumple que  $(p - 1)! + 1 \in p\mathbb{Z}$ .

# Grupos abelianos finitos. Función de Euler

---

## Teorema de estructura de los grupos abelianos finitos.

---

### Definición (Exponente)

El **exponente** de un grupo finito  $G$ , denotado  $e(G)$ , es el menor entero  $k > 0$  tal que  $g^k = 1_G$ ,  $\forall g \in G$ .

---

### Proposición

- $e(G)$  es el mínimo común múltiplo de los órdenes de los elementos de  $G$ . En particular,  $e(G) \mid \text{ord}(G)$ .
- Si  $G$  es abeliano  $e(G)$  es el máximo de los órdenes de los elementos de  $G$ .

### Teorema (Teorema de estructura)

Sea  $G$ , grupo abeliano finito. Entonces,  $\exists m_1, \dots, m_r \in \mathbb{Z}$  tales que  $m_i \mid m_{i-1}$ ,  $\forall 2 \leq i \leq r$  y  $G \simeq \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_r}$ . Además,  $r, m_1, \dots, m_r$  son únicos con estas condiciones.

---

### Definición

Los anteriores  $m_1, \dots, m_r$  se denominan **coeficientes de torsión** de  $G$ .

---

### Proposición (Grupos abelianos de orden dado)

Sean  $n, m > 1$  enteros tal que  $\text{mcd}(n, m) = 1$ . Entonces, todo grupo abeliano  $G$  de orden  $mn$  es isomorfo a  $H \times K$ , donde  $H$  y  $K$  son grupos abelianos de órdenes  $m$  y  $n$ .