

# Grupos finitos

Notas de clase de  
Eugenio Miranda Palacios  
para el curso 2010/2011  
Adaptadas por Manuel Bullejos  
para el curso 2020/2021

## Índice

<b>1. Definición de grupo</b>	<b>2</b>
1.1. Primeros ejemplos . . . . .	3
1.2. Propiedades elementales . . . . .	6
1.3. Grupos simétricos . . . . .	9
1.4. Grupos diédricos . . . . .	18
1.5. Producto directo . . . . .	21
1.6. Grupos de matrices . . . . .	22
1.7. El grupo cuaternio . . . . .	23
<b>2. Homomorfismos y subgrupos</b>	<b>24</b>
2.1. Homomorfismos . . . . .	24
2.2. Subgrupos . . . . .	26
2.2.1. El retículo de subgrupos . . . . .	26
2.2.2. Grupos cíclicos y sus retículos de subgrupos . . . . .	29
2.2.3. El retículo de subgrupos de un producto directo . . . . .	31
2.3. El teorema de Lagrange . . . . .	33

## 2. Homomorfismos y subgrupos

### 2.1. Homomorfismos

**Definición 2.1.** Dados dos grupos  $G$  y  $H$  llamamos *homomorfismo* (o simplemente *morfismo*) de  $G$  a  $H$  a toda aplicación  $f : G \rightarrow H$  que respete la estructura de grupo, esto es:

- Respetar la multiplicación:  $\forall x, y \in G, f(xy) = f(x)f(y)$ .  $\Rightarrow$  Con esto ya lo tenemos todo:  
multiplicas por  $f(1)^{-1}$   $\begin{cases} f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \\ 1 = f(1) \end{cases}$   
y también  $f(x) \cdot f(x^{-1}) = f(x \cdot x^{-1}) = f(1) = 1$
- Respetar elemento neutro:  $f(1) = 1$ .
- Respetar inversos:  $f(x^{-1}) = f(x)^{-1}$ .

El grupo  $G$  se llama *dominio* de  $f$  y el grupo  $H$  se llama *codominio* o *rango* de  $f$ .

**Ejercicio 2.1.** Toda aplicación entre grupos que respete la multiplicación y el neutro respeta inversos.

El conjunto

$$\text{Im}(f) = f_*(G) = \{f(x) \mid x \in G\} \subset H$$

se llama *imagen* de  $f$  y el conjunto

$$\ker(f) = f^*(1) = \{x \in G \mid f(x) = 1\} \subset G$$

se llama *núcleo* de  $f$ .

**Definición 2.2.** El homomorfismo de grupos  $f : G \rightarrow H$  se llama

- *Monomorfismo* si es una aplicación inyectiva.
- *Epimorfismo* si es una aplicación suprayectiva.
- *Isomorfismo* si tiene inverso, i.e.  $\exists f^{-1} : H \rightarrow G$  homomorfismo tal que  $ff^{-1} = Id_H$  y  $f^{-1}f = Id_G$ .

**Teorema 2.3.** Un morfismo  $f : G \rightarrow H$  es isomorfismo si, y solo si, la aplicación  $f$  es biyectiva.

*Demostración.* Está claro que si el homomorfismo  $f$  tiene inverso entonces  $f$  es una aplicación biyectiva. Para probar el recíproco, si  $f$  es biyectiva, entonces existe su inversa  $f^{-1}$ , lo que tendremos que probar es que este es también morfismo. Veamos que respeta la multiplicación y dejemos el resto de la comprobación como ejercicio. Sean  $x, y \in G$  dos elementos y consideremos, por un lado  $f^{-1}(xy)$  y por otro  $f^{-1}(x)f^{-1}(y)$ . Para ver que son iguales, aplicaremos  $f$  a ambos y obtenemos

- $ff^{-1}(xy) = xy$  y
- $ff^{-1}(x)f^{-1}(y) = f^{-1}(x)f^{-1}(y) = xy$ ,

aplicando ahora que  $f$  es inyectiva, tenemos  $ff^{-1}(xy) = f(f^{-1}(x)f^{-1}(y))$  implica  $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$ .  $\square$

Diremos que dos grupos  $G$  y  $H$  son isomorfos si existe un isomorfismo entre ellos y lo representaremos  $G \cong H$ .

Si el dominio y el codominio coinciden,  $G = H$ , diremos que  $f$  es un *endomorfismo*.

Un endomorfismo biyectivo se llama *automorfismo*.

*Ejemplo 2.1.* Sea  $\mathbb{R}^\times$  el grupo de los números reales no nulos con la multiplicación. La aplicación determinante

$$GL(2, \mathbb{R}) \rightarrow \mathbb{R}^\times, \quad A \mapsto \det(A)$$

es un homomorfismo. El núcleo de este homomorfismo es  $SL(2, \mathbb{R})$  y la imagen es todo  $\mathbb{R}^\times$ .

*Ejemplo 2.2.* La aplicación  $\varphi : \mathbb{R}^\times \rightarrow \mathbb{R}^\times$  definida por  $\varphi(x) = |x|$  es un homomorfismo con núcleo  $\{1, -1\}$ .

*Ejemplo 2.3.* La aplicación  $\mathbb{R}[x] \rightarrow \mathbb{R}[x]$  dada por  $f \mapsto f'$  (la derivada de  $f$ ) es un endomorfismo de  $\mathbb{R}[x]$ . La imagen es todo  $\mathbb{R}[x]$  y el núcleo es el conjunto de polinomios constantes.

*Ejemplo 2.4.* La aplicación  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$  definida por  $\varphi(m) = [m] = [r]$  donde  $r$  es el resto de dividir  $m$  entre  $n$  es un homomorfismo sobre. El núcleo es  $n\mathbb{Z}$ , el conjunto de múltiplos enteros de  $n$ .

*Ejemplo 2.5.* La aplicación  $\varphi : \mathbb{R} \rightarrow \mathbb{R}$  definida por  $\varphi(x) = x^2$  no es un homomorfismo para la adición.

*Ejemplo 2.6.* Toda aplicación lineal entre espacios vectoriales es un homomorfismo de grupos aditivos.

*Ejemplo 2.7.* La aplicación signatura  $sg : S_n \rightarrow \{1, -1\} = \mu_2$  es un epimorfismo de grupos. Al núcleo de esta aplicación lo llamaremos grupo alternado y lo denotaremos  $A_n = \ker(sg) = \{\sigma \in S_n \mid \sigma \text{ es par}\}$ .

*Observación 2.1.*

- Para todo grupo  $G$  la aplicación identidad  $1_G : G \rightarrow G$  es un automorfismo.
- Sean  $f_1 : G \rightarrow H$  y  $f_2 : H \rightarrow K$  dos homomorfismos de grupos. Entonces la aplicación compuesta  $f_2 f_1 : G \rightarrow K$  es un homomorfismo.
- Para un grupo arbitrario  $G$ , el conjunto de todos los automorfismos de  $G$  forman un grupo (con la composición de aplicaciones como operación), que se llama *grupo de los automorfismos de  $G$*  y se representa por  $\text{Aut}(G)$ .
- Si  $f : G \cong H$  es un isomorfismo, entonces  $G$  y  $H$  tienen las mismas propiedades, en particular:
  - $|G| = |H|$ ,

- $\forall x \in G, o(x) = o(f(x))$ .
- Dado un morfismo  $f : G \rightarrow H$ , entonces:
  - $f$  es monomorfismo si, y sólo si,  $\ker(f) = 1$ ,
  - $f$  es epimorfismo si, y sólo si,  $\text{Im}(f) = H$ ,
  - $f$  es isomorfismo si, y sólo si,  $\ker(f) = 1$  e  $\text{Im}(f) = H$ .

## 2.2. Subgrupos

**Definición 2.4.** Un subgrupo de un grupo  $G$  es un subconjunto  $H \subseteq G$  que hereda la estructura de grupo, esto es:

- Hereda el producto: Si  $x, y \in H$  entonces  $xy \in H$ , → Cuidado esto sí que no implica las otras 2. Contraejemplo: El vacío  $\emptyset$
- Hereda el neutro:  $1 \in H$ .
- Hereda los inversos: Si  $x \in H$  entonces  $x^{-1} \in H$ .

*Observación 2.2.* Si  $H$  es un subgrupo de  $G$  escribiremos  $H \leq G$  y  $H$  con la restricción de la multiplicación de  $G$ , el mismo neutro y los mismos inversos es un grupo. Además la inclusión  $H \hookrightarrow G$  es un morfismo de grupos.

*Observación 2.3.* Todo grupo  $G$  no trivial (i.e.  $G \neq \{1\}$ ) tiene al menos dos subgrupos: El *subgrupo trivial* formado sólo por el elemento unidad, que lo denotaremos  $1 \leq G$ , y el mismo  $G$ ,  $G \leq G$ , que es el *subgrupo total*.

Ambos son los *subgrupos impropios*. Cualquier otro subgrupo es un *subgrupo propio*.

**Proposición 2.5.** Si  $G$  es un grupo finito, un subconjunto no vacío  $\emptyset \neq H \subseteq G$  es un subgrupo si, y sólo si, hereda el producto.

*Demostración.* Si  $H \neq \emptyset$ , sea  $x \in H$ , por ser  $G$  finito, el orden de  $x$  ha de ser finito, si  $o(x) = n$ , entonces  $x^n = 1 \in H$ , por ser este cerrado para el producto, y  $x^{-1} = x^{n-1} \in H$  por lo que también hereda los inversos.  $\square$

### 2.2.1. El retículo de subgrupos

Es fácil de comprobar que la intersección de dos subgrupos de un grupo es un subgrupo. En general tenemos la siguiente proposición cuya demostración dejamos como ejercicio.

**Proposición 2.6.** Sea  $\{H_\lambda \mid \lambda \in \Lambda\}$  una familia de subgrupos de un grupo  $G$ . Entonces  $H = \cap_\lambda H_\lambda$  es un subgrupo de  $G$ .

Esta proposición nos permite definir dos conceptos importantes:

**Definición 2.7.** Sea  $S$  un subconjunto de  $G$ . Llamamos *subgrupo generado por  $S$*  a la intersección  $H$  de todos los subgrupos de  $G$  que contienen a  $S$ . Lo representamos por  $H = \langle S \rangle$ .

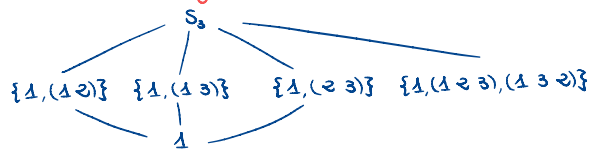
Sin embargo la unión de subgrupos no es subgrupo. Ejemplo:

$S_3 \supseteq \{1, (12)\} \cup \{1, (13)\} \supseteq \{1, (12), (13)\}$

Por ello la definición 2.7

$(12)(13) = (132)$

¿Retículo de subgrupos de  $S_3$ ?



Todos son grupos cíclicos ya que  $G = \langle a \rangle = \{a^i, i \in \mathbb{Z}\}$   
 Son abelianos ya que  $a^i \cdot a^j = a^{i+j} = a^{j+i} = a^j \cdot a^i$

**Definición 2.8.** Sea  $\{H_\lambda \mid \lambda \in \Lambda\}$  una familia arbitraria de subgrupos de  $G$ . Llamamos *compuesto de los  $H_\lambda$*  al subgrupo generado por  $S = \cup_\lambda H_\lambda$ . Lo representamos por  $\vee_\lambda H_\lambda$

En el caso particular en que la familia es finita, sea  $H_1, \dots, H_n$ , su compuesto se representa por  $H_1 \vee \dots \vee H_n$ .

*Observación 2.4.*

1. El subgrupo generado por el vacío es el trivial, i.e.  $\langle \emptyset \rangle = 1$ .
2. Para cualquier  $S \subset G$  no vacío,  $\langle S \rangle$  es el conjunto de todos los elementos de  $G$  que se expresan como producto finito de elementos de  $S$  y de sus inversos.
3. Sea  $G$  un grupo finito. Para cualquier  $S \subset G$  no vacío, el subgrupo  $\langle S \rangle$  es el conjunto de todos los elementos de  $G$  que se expresan como producto finito de elementos de  $S$ .
4. Los elementos de  $H_1 \vee \dots \vee H_n$  son productos finitos de elementos de los  $H_i$ .

El conjunto de subgrupos de un grupo  $G$  está ordenado con la inclusión y junto con las operaciones intersección y compuesto forman un retículo, llamado el *retículo de subgrupos* de  $G$ . El grafo que muestra las relaciones entre sus subgrupos ilumina la estructura del grupo mejor que la tabla de grupo.

En la teoría de grupos se usan diagramas de retículos o parte de ellos para describir grupos específicos y algunas propiedades de grupos generales. Además el retículo de subgrupos de un grupo juega un papel central en la teoría de Galois.

El retículo de subgrupos de un grupo finito dado  $G$  se construye como sigue:

Situamos todos los subgrupos de  $G$  empezando abajo con 1, acabando arriba con  $G$  y, hablando toscamente, con subgrupos de orden mayor colocados más arriba en la página que los de orden más pequeño.

Trazamos líneas entre los subgrupos siguiendo la regla de que hay una línea de  $A$  a  $B$  si  $A$  es un subgrupo de  $B$  y no existen subgrupos propios de  $B$  que contengan propiamente a  $A$ .

Así si  $A < B$  existe un camino (posiblemente varios) desde  $A$  hasta  $B$  que pasa a través de una cadena de subgrupos intermedios.

La posición inicial de los subgrupos sobre la página (que es a priori algo arbitraria) puede elegirse frecuentemente (con un poco de práctica) para producir un dibujo sencillo. Nótese que para cualquier par de subgrupos  $H, K$  de  $G$ , el mínimo subgrupo que contiene a ambos es el *compuesto* de  $H$  y  $K$  (que hemos representado por  $H \vee K$ ) se obtiene rápidamente del retículo como sigue:

Se toman caminos hacia arriba desde  $H$  y  $K$  hasta que se alcanza un subgrupo común  $A$  que contiene a ambos (ya que  $G$  contiene a todos sus subgrupos, un tal  $A$  siempre existe).

Para asegurarnos que  $A = H \vee K$  comprobamos que no existe ningún  $A_1 < A$  que contenga a ambos  $H$  y  $K$ . En otro caso, reemplazamos  $A$  por  $A_1$  y repetimos el proceso para ver si  $A_1 = H \vee K$ .

Por un procedimiento simétrico se puede obtener directamente el mayor subgrupo de  $G$  contenido en  $H$  y  $K$ , es decir su intersección  $H \cap K$ .

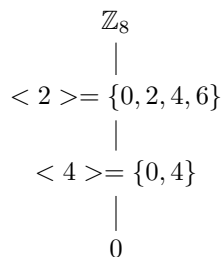
Este proceso tiene algunas limitaciones.

- No puede ejecutarse tal cual para grupos infinitos
- Aún para grupos finitos de orden relativamente pequeño puede ser bastante complicado (algunos grupos con orden 64 ponen el pelo de punta).

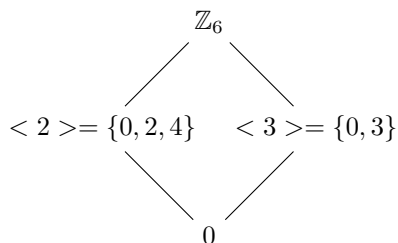
Naturalmente dos grupos isomorfos tienen retículos de subgrupos isomorfos. Pero grupos no isomorfos pueden tener también retículos isomorfos

Esto no es un inconveniente muy serio ya que el retículo es sólo parte de los datos del grupo  $G$  e incluso es útil ver que dos grupos no isomorfos tienen algunas propiedades comunes.

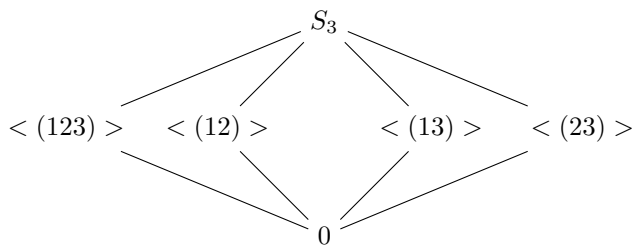
*Ejemplo 2.8.* EL retículo de subgrupos del grupo abeliano  $\mathbb{Z}_8$  sería:



*Ejemplo 2.9.* EL retículo de subgrupos del grupo abeliano  $\mathbb{Z}_6$  sería:



*Ejemplo 2.10.* EL retículo de subgrupos del grupo  $S_3$  sería:



### 2.2.2. Grupos cíclicos y sus retículos de subgrupos

**Definición 2.9.** Un grupo  $G$  se llama *cíclico* si puede ser generado por un elemento, esto es, si existe un  $a \in G$  tal que  $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ .

El elemento  $a$  se llama *generador* de  $G$ .

*Ejemplo 2.11.* El grupo  $(\mathbb{Z}, +)$  es cíclico. De hecho  $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ .

*Ejemplo 2.12.* El grupo  $(\mathbb{Z}_n, +)$  es cíclico. De hecho  $\mathbb{Z}_n = \langle 1 \rangle$  y  $\mathbb{Z}_n = \langle m \rangle$  si y sólo si  $\text{m.c.d.}(n, m) = 1$ . Como consecuencia, en  $\mathbb{Z}_n$  hay  $\varphi(n)$  elementos que lo generan, donde  $\varphi$  es la función (tocien) de Euler.

*Ejemplo 2.13.* El grupo  $U(10) = \{1, 3, 7, 9\}$  es cíclico. De hecho  $U(10) = \langle 3 \rangle = \langle 7 \rangle$ , aunque  $\langle 9 \rangle = \{1, 9\}$ .

*Ejemplo 2.14.* El grupo  $U(8) = \{1, 3, 5, 7\}$  no es cíclico. Porque

$$\begin{aligned}\langle 1 \rangle &= \{1\} \\ \langle 3 \rangle &= \{1, 3\} \\ \langle 5 \rangle &= \{1, 5\} \\ \langle 7 \rangle &= \{1, 7\}\end{aligned}$$

**Proposición 2.10.** Sea  $G$  un grupo y sea  $a \in G$ . Si el orden de  $a$  es infinito, todas las potencias  $\{a^k \mid k \in \mathbb{Z}\}$  son distintas.

Si  $o(a) = n$  es finito entonces  $\langle a \rangle = \{1, a, a^2, \dots, a^{n-1}\}$  y  $a^j = a^k$  si y sólo si  $j \equiv k \pmod{n}$ .

*Demostración.* Observamos primero que si  $a^j = a^k$ , y suponemos  $j < k$ , entonces, multiplicando por  $a^{-j}$ , tenemos que  $a^{k-j} = 1$  y por tanto si el orden de  $a$  es infinito, todas las potencias de  $a$  son distintas.

Por otro lado, si  $o(a) = n$ , para cualquier entero no nulo  $j$ , pongamos  $j = qn + r$  con  $r < n$  el resto de la división, entonces  $a^j = a^{qn+r} = a^r$  y tenemos la segunda parte de la proposición.  $\square$

*Observación 2.5.* Como consecuencia inmediata de la Proposición 2.10 anterior tenemos que:

- Para cualquier  $a \in G$  se verifica que  $o(a) = |\langle a \rangle|$ .
- Si  $o(a) = n$  entonces  $a^k = 1$  si y sólo si  $n$  divide a  $k$ .
- Denotaremos  $C_n$  a un grupo cíclico de orden  $n$ , con notación multiplicativa. Este estará generado por un elemento que podemos llamar  $a$  con la relación  $a^n = 1$ . Escribiremos

$$C_n = \langle a; a^n = 1 \rangle.$$

y diremos que esto es una presentación de  $C_n$ .

**Teorema 2.11.** Sea  $a \in G$  un elemento de orden finito  $n = o(a)$ . Para todo  $k \in \mathbb{Z}$  se tiene que

$$1. \langle a^k \rangle = \langle a^{\text{m.c.d.}(n,k)} \rangle \text{ y}$$

$$2. o(a^k) = \frac{n}{\text{m.c.d.}(n,k)}.$$

*Demostración.* Llamemos  $d = \text{m.c.d.}(n, k)$  y pongamos  $n = dn', k = dk'$  y  $d = un + vk$  (igualdad de Bezout), entonces  $a^k = a^{dk'} = (a^d)^{k'}$  y tenemos  $\langle a^k \rangle \subseteq \langle a^d \rangle$ . Por otro lado  $a^d = a^{un+vk} = (a^n)^u (a^k)^v = (a^k)^v$  de donde  $\langle a^d \rangle \subseteq \langle a^k \rangle$  y deducimos la igualdad.

Ahora  $o(a^k) = |\langle a^k \rangle| = |\langle a^d \rangle| = o(a^d)$  y para demostrar la segunda parte basta con ver que  $o(a^d) = \frac{n}{d} = n'$ . Claramente  $(a^d)^{n'} = a^{dn'} = a^n = 1$ , y si  $(a^d)^m = a^{dm} = 1$  entonces  $dm$  es un múltiplo de  $n = dn'$  y por tanto  $m$  es un múltiplo de  $n'$ .

El orden de  $\langle a^d \rangle$  es divisor de  $\frac{(a^d)^k}{n} = \frac{1}{n} = \frac{k}{d \cdot n'}$   $k < n'$   $dk < dn' = n$  Contradicción

Como consecuencia inmediata tenemos:

### Corolario 2.12.

1. Sea  $a \in G$  un elemento de orden finito  $o(a) = n$ . Entonces  $\langle a^j \rangle = \langle a^k \rangle$  si y sólo si  $\text{m.c.d.}(j, n) = \text{m.c.d.}(k, n)$ .
2. Sea  $G = \langle a \rangle$  un grupo cíclico de orden  $|G| = n$ . Entonces  $G = \langle a^k \rangle$  si y sólo si  $\text{m.c.d.}(k, n) = 1$  y por tanto en un grupo cíclico de orden  $n$  hay exactamente  $\varphi(n)$  elementos que lo generan.
3. Una clase  $[k] \in \mathbb{Z}_n$  es un generador de  $\mathbb{Z}_n$  si y sólo si  $\text{m.c.d.}(k, n) = 1$ .

**Teorema 2.13** (Teorema fundamental de los grupos cíclicos).

1. Todo subgrupo de un grupo cíclico es cíclico.
2. Si  $|\langle a \rangle| = n$ , el orden de cualquier subgrupo de  $\langle a \rangle$  es un divisor de  $n$ .
3. Para cada  $m$  divisor positivo de  $n$ , el grupo  $|\langle a \rangle|$  tiene exactamente un subgrupo de orden  $m$ , a saber  $\langle a^{n/m} \rangle$ .

*Demostración.* 1. Sea  $G = \langle a \rangle$  y  $H \leq G$  un subgrupo. Sea  $m$  el mínimo entero positivo tal que  $a^m \in H$ , claramente  $\langle a^m \rangle \subseteq H$ . Veamos que se da la igualdad, supongamos que  $a^p \in H$ , dividimos  $p$  por  $m$  y ponemos  $p = mq + r$  con  $r = 0$  o  $0 < r < m$ . Entonces  $a^p = a^{mq+r} = (a^m)^q a^r$  y despejando tenemos  $a^r = a^p (a^m)^{-q} \in H$ , por ser producto de dos elementos de  $H$ . Por ser  $m$  el menor entero positivo con esta condición, ha de ser  $r = 0$ , de donde  $a^p = (a^m)^q \in \langle a^m \rangle$  y se tiene el otro contenido.

2. Es consecuencia inmediata del apartado anterior y del apartado 2 del Teorema 2.11.
3. Si  $m$  es un divisor de  $n$  y ponemos  $n = nq$  entonces  $o(a^{\frac{n}{m}}) = o(a^q) = \frac{n}{\text{m.c.d.}(n,q)} = \frac{n}{q} = m$  y  $H = \langle a^q \rangle$  es un subgrupo de orden  $m$ . Si  $H' = \langle a^k \rangle$  es otro subgrupo de orden  $m$ , entonces  $m = o(a^k) = \frac{n}{\text{m.c.d.}(n,k)}$  de donde  $q = \text{m.c.d.}(n, k)$  y, por el apartado 1 de 2.11,  $H' = \langle a^k \rangle = \langle a^{\text{m.c.d.}(n,k)} \rangle = \langle a^q \rangle = H$ .

□



Si aplicamos el Teorema 2.13 al caso de grupos cíclicos en notación aditiva, tendremos

**Corolario 2.14.** Para cada  $d$  divisor positivo de  $n$  el grupo  $\langle [\frac{n}{d}] \rangle$  es el único subgrupo de  $\mathbb{Z}_n$  de orden  $d$ . Estos son los únicos subgrupos de  $\mathbb{Z}_n$ .

Podemos contar ahora el número de elementos de cada orden en un grupo cíclico.

Recordemos primero que la función  $\varphi$  de Euler (o tocién de Euler) está definida en cada entero positivo  $n$  como el número de enteros positivos menores que  $n$  y primos relativos con  $n$ ,

$$\varphi(n) = |\{k \in \mathbb{Z} \mid k > 0, \text{ m. c. d.}(k, n) = 1\}| = |U(n)|.$$

**Corolario 2.15.** Sea  $d$  un entero positivo divisor de  $n$ . El número de elementos de orden  $d$  en un grupo cíclico de orden  $n$  es  $\phi(d)$ .

*Demostración.* Si  $d$  divide a  $n$ , cada elemento de orden  $d$  en un grupo cíclico  $G = \langle a \rangle$  de orden  $n$  genera un subgrupo de orden  $d$  y como sólo hay uno  $H = \langle a^{\frac{n}{d}} \rangle$ , cada elemento de orden  $d$  es un generador de  $H$  y por tanto el número de elementos de orden  $d$  de  $G$  coincide con el número de generadores de  $H$  que a su vez coincide con  $\varphi(|H|) = \varphi(d)$ . → Por el corolario 2.13 3)  $\square$

Nótese que para un grupo cíclico de orden  $n$ , el número de elementos de orden  $d$  depende sólo de  $d$ . Así que  $\mathbb{Z}_8$ ,  $\mathbb{Z}_{640}$  y  $\mathbb{Z}_{80000}$  tienen cada uno  $\phi(8) = 4$  elementos de orden 8.

*Observación 2.6.* Es interesante calcular la intersección y el compuesto de dos subgrupos de un grupo cíclico. Dejamos como ejercicio probar que si  $C_n = \langle a \rangle$  es un grupo cíclico de orden  $n$ , para enteros  $i, j < n$  se tiene:

$$\blacksquare \langle a^i \rangle \vee \langle a^j \rangle = \langle a^i, a^j \rangle = \langle a^{\text{m.c.d.}(i,j)} \rangle \text{ y}$$

$$\blacksquare \langle a^i \rangle \cap \langle a^j \rangle = \langle a^{\text{m.c.m.}(i,j)} \rangle.$$

### 2.2.3. El retículo de subgrupos de un producto directo

Es inmediato comprobar que si tenemos dos subgrupos  $H' \leq H$  y  $K' \leq K$ , entonces el producto  $H' \times K'$  es un subgrupo del producto,  $H' \times K' \leq H \times K$ . Sin embargo, no todos los subgrupos de un producto son productos de subgrupos. Por ejemplo la diagonal

$$\Delta = \{(x, x); x \in H\} \leq H \times H$$


es un subgrupo que no es producto de subgrupos.

Recordemos ahora que en la Sección 1.5 vimos que el grupo  $\mathbb{Z}_2 \times \mathbb{Z}_2$  no tenía elementos de orden 4 y por tanto no es cíclico. Pero el grupo  $\mathbb{Z}_2 \times \mathbb{Z}_3$  sí que tiene elementos de orden 6 y por tanto sí que es cíclico. Para terminar esta sección nos preguntamos ¿cuando el producto de grupos cíclicos es cíclico? La siguiente Proposición nos responde a esta pregunta:

**Proposición 2.16.** El producto de dos grupos cíclicos  $C_n \times C_m$  es cíclico si, y sólo si,  $m.c.d(n, m) = 1$ .

*Demostración.* Para que  $C_n \times C_m$  sea cíclico, necesitamos encontrar un elemento de orden  $n \cdot m$ , pero el orden de un elemento  $(x, y)$  del producto es el m.c.m de los órdenes sus componentes,

$$o(x, y) = m.c.m(o(x), o(y))$$


 Por el Teorema 2.11 2)

y los ordenes de estos son divisores de  $n$  y  $m$  respectivamente y por tanto son menores o iguales a  $n$  y  $m$  respectivamente. Por tanto

$$o(x, y) = m.c.m(o(x), o(y)) \leq m.c.m(n, m) \leq n \cdot m$$

y se dará la igualdad si, y sólo si,  $n$  y  $m$  son primos relativos ( $m.c.d.(n, m) = 1$ ). Por tanto  $C_n \times C_m$  tiene un elemento de orden  $n \cdot m$  si, y sólo si,  $n$  y  $m$  son primos relativos. □

Y por lo tanto  $o(x)$  y  $o(y)$  también son primos relativos, pues de no serlo,  $n$  y  $m$  tampoco lo serían

## 2.3. El teorema de Lagrange

### Clases laterales

Sea  $G$  un grupo y  $H$  un subgrupo suyo. Definimos dos relaciones binarias en  $G$  de la siguiente forma:

$$x {}_H \sim y \text{ si y sólo si } y^{-1}x \in H$$

$$x \sim_H y \text{ si y sólo si } xy^{-1} \in H$$

*Observación 2.7.* Dejamos como ejercicio probar que las relaciones recién definidas son relaciones de equivalencia.

Además si  $x \in G$  es un elemento cualquiera, entonces

1. La clase de equivalencia de  $x$  bajo la relación  ${}_H \sim$  es

$$xH = \{xh \mid h \in H\}$$

y se llama *clase lateral por la izquierda de  $H$  en  $G$  definida por  $x$* . El conjunto de todas las clases por la izquierda de  $H$  en  $G$  forman una partición de  $G$  que representamos por  $G/{}_H \sim$ ,

$$G/{}_H \sim = \{xH; x \in G\}.$$

2. La clase de equivalencia de  $x$  bajo la relación  $\sim_H$  es

$$Hx = \{hx \mid h \in H\}$$

y se llama *clase lateral por la derecha de  $H$  en  $G$  definida por  $x$* . El conjunto de todas las clases por la derecha de  $H$  en  $G$  forman una partición de  $G$  que representamos por  $G/\sim_H$ ,

$$G/\sim_H = \{Hx; x \in G\}.$$

La siguiente proposición es fácil de demostrar y dejamos su demostración como ejercicio.

**Proposición 2.17.** Dado un grupo  $G$  y un subgrupo suyo  $H \leq G$ , entonces:

1. Para todo  $x \in G$ ,  $x \in xH$ ,  $x \in Hx$ .  $\longrightarrow$  Porque por ser subgrupo, en  $H$  está la unidad.

2. Para todo  $x \in G$  las aplicaciones  $H \rightarrow xH; h \mapsto xh$  y  $H \rightarrow Hx; h \mapsto hx$  son biyecciones.

3. Existe una biyección  $G/{}_H \sim \cong G/\sim_H$  dada por  $xH \leftrightarrow Hx^{-1}$ .

**Definición 2.18.** Después de 3 en la Proposición 2.17 tenemos que los cardinales de los conjuntos  $G/{}_H \sim$  y  $G/\sim_H$  coinciden. Llamaremos *índice de  $H$  en  $G$*  al cardinal de cualquiera de ellos y se representa por

$$[G : H] = |G/{}_H \sim| = |G/\sim_H|.$$

Notemos ahora que si  $G$  es un grupo finito, ya que  $G/H \sim$  es una partición de  $G$ , el orden de  $G$  es igual a la suma de los cardinales de las clases por la izquierda, pero como todas las clases tienen el mismo cardinal, el orden de  $G$  será el número de clases por la izquierda por el cardinal de una de ellas, por ejemplo  $1H = H$ . Análogamente, si sustituimos clases por la izquierda por clases por la derecha, tenemos que el orden de  $G$  es el número de clases por la derecha por el cardinal de cualquiera de ellas, por ejemplo  $H1 = H$ . En definitiva, si  $G$  es finito entonces

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

Tenemos así:

**Teorema 2.19** (Teorema de Lagrange). *Sea  $G$  un grupo finito y  $H$  un subgrupo suyo, entonces*

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

*En particular, el orden de un subgrupo de un grupo finito es un divisor del orden del grupo,  $|H|$  divide a  $|G|$ .*

Como consecuencias inmediatas del Teorema de Lagrange 2.19 tenemos

**Corolario 2.20.**

1. Sea  $G$  un grupo finito. Todo  $x \in G$  verifica  $o(x) \mid |G|$ .
2. Si  $|G| = p$  primo, entonces todo elemento de  $G$  no trivial tiene orden  $p$  y por tanto  $G$  es cíclico,  $G \cong C_p$ .
3. Sea una torre de subgrupos de un grupo finito  $K \leq H \leq G$ . Entonces

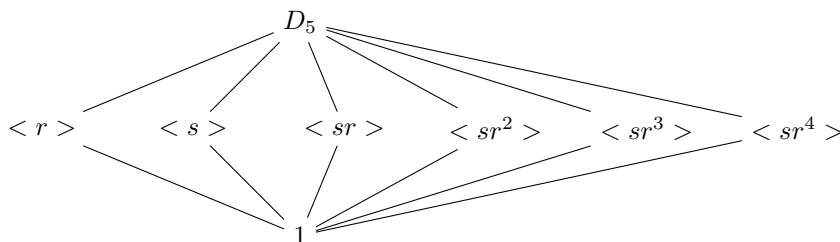
$$[G : K] = [G : H][H : K]$$

El Corolario 2.20 nos facilita la obtención del retículo de subgrupos de un grupo, como vemos en el siguiente ejemplo.

*Ejemplo 2.15.* Claculemos el retículo de subgrupos de  $D_5$ , puesto que  $|D_5| = 10 = 2 \cdot 5$ , los subgrupos de  $D_5$  no triviales sólo pueden tener ordenes 2 o 5, ambos primos y por tanto todos los subgrupos de  $D_5$  serán cíclicos de ordenes 2 o 5. Si ponemos

$$D_5 = \{1, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\},$$

tenemos  $o(r) = o(r^2) = o(r^3) = o(r^4) = 5$  (todos generan el mismo subgrupo) y  $o(s) = o(sr) = o(sr^2) = o(sr^3) = o(sr^4) = 2$  y el retículo quedaría:



*Ejemplo 2.16.* Veamos como podemos utilizar el Corolario 2.20 para clasificar los grupos de orden 4.

Si  $G$  es un grupo de orden 4, sus elementos no triviales tiene orden 2 o 4, si  $G$  tiene un elemento de orden 4 entonces  $G$  es cíclico  $G \cong C_4$ . Si no tiene elementos de orden 4 todos sus elementos no triviales son de orden 2, veamos como sería  $G$ . Tomamos un elemento  $a \in G, a \neq 1$ , entonces  $a^2 = 1$  y ha de haber otro elemento no trivial en  $G$  llamemosle  $b \in G, b \neq 1, b \neq a$ . Entonces

$$G = \{1, a, b, ab\}$$

y  $ab \neq 1, ab \neq a, ab \neq b$  y tiene orden 2, por lo que  $(ab)^2 = abab = 1 \Rightarrow ab = b^{-1}a^{-1} = ba$ .

Entonces  $G$  es un grupo de 4 elementos, generado por dos elementos de orden 2 que conmutan, y ha de ser isomorfo a  $C_2 \times C_2$ .

Como hemos dicho, el objetivo de este curso será el clasificar grupos de orden pequeño, al final del curso escribiremos una tabla con todos los posibles grupos hasta orden 15, ya podemos comenzar añadiendo datos a dicha tabla:

orden	abelianos	no abelianos
1	1	ninguno
2	$C_2$	ninguno
3	$C_3$	ninguno
4	$C_4$ $C_2 \times C_2$	ninguno ninguno
5	$C_5$	ninguno
6	??	?? $S_3 \cong D_3$
7	$C_7$	ninguno
8	??	??
9	??	??
10	??	??
11	$C_{11}$	ninguno
12	??	??
13	$C_{13}$	ninguno
14	??	??
15	??	??

*Ejemplo 2.17.* El teorema de Lagrange y el conocer los grupos hasta orden 5, nos facilita el cálculo de algunos retículos de subgrupos, como por ejemplo el retículo de subgrupos de  $A_4$  que es un grupo de orden 12. Primero observamos que las permutaciones en  $A_4$  sólo pueden ser de los tipos:

- 1 como la identidad,
- 3 como (123) o
- 2, 2 como (12)(34.)

Por tanto los órdenes de los elementos de  $A_4$  pueden ser: 1, 3 ó 2.  $A_4$  no tiene elementos de orden 4 ni 6 ni de orden 12.

En la siguiente tabla indicamos cuantos elementos hay de cada tipo:

tipo	nº elementos	orden
1	1	1
3	8	3
2,2	3	2
Total	12	

Notar que para contar cuantos elementos hay del tipo 2,2, esto es, de la forma  $(12)(34)$ , observamos que fijada la primera transposición, la segunda está totalmente determinada pero también se tiene que  $(12)(34) = (34)(12)$ . Por tanto el número de permutaciones del tipo 2,2 será el numero de transposiciones de  $S_4$  dividido por 2.

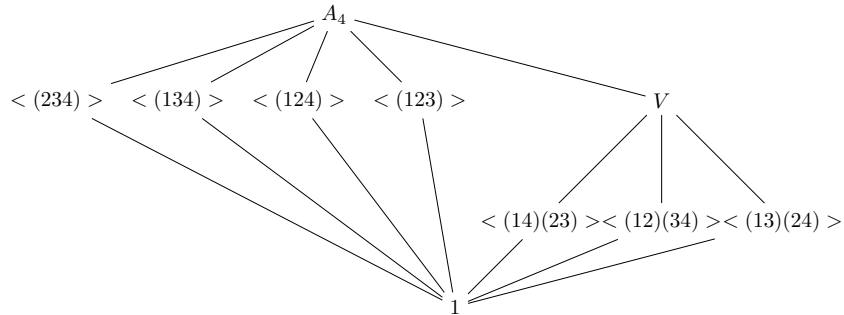
Los subgrupos de orden 2 estarán generados por elementos de orden 2 y habrá tres:  $\langle (12)(34) \rangle$ ,  $\langle (13)(24) \rangle$  y  $\langle (14)(23) \rangle$ .

Los tres elementos de orden 2 junto con la identidad forma el único subgrupo de orden 4:

$$V = \{1, (12)(34), (13)(24), (14)(23)\}.$$

Los subgrupos de orden 3 estarán generados por un ciclo de longitud 3 y en cada uno de estos subgrupos habrá (aparte de la identidad) dos ciclos de orden tres. Por tanto hay  $8/2 = 4$  subgrupos de orden tres:  $\langle (123) \rangle$ ,  $\langle (124) \rangle$ ,  $\langle (134) \rangle$  y  $\langle (234) \rangle$ .

Por último, si  $A_4$  tuviese un subgrupo de orden 6, tendría que tener un ciclo de orden 3 y un producto de dos transposiciones, es mecánico comprobar que si esto sucede el subgrupo sería todo  $A_4$  y por tanto  $A_4$  no tiene subgrupos de orden 6. El retículo quedaría:



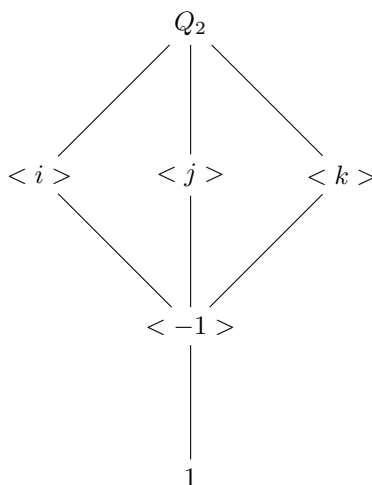
*Ejemplo 2.18.* Vamos a calcular ahora el retículo de subgrupos de

$$Q_2 = \{1, -1, i, -i, j, -j, k, -k\} = \langle i, j; i^4 = 1, i^2 = j^2, ji = i^{-1}j \rangle.$$

Los órdenes de los elementos en  $Q_2$  son

$$o(-1) = 2, o(i) = o(-i) = o(j) = o(-j) = o(k) = o(-k) = 4.$$

Por tanto  $Q_2$  tiene un único subgrupo de orden 2 que está contenido en todos los subgrupos de orden 4 que son 3. El retículo de subgrupos sería:



$$|G| = 6$$

$$C_2 \times C_3 \cong C_6$$

$$D_3 \cong S_3$$

$$\text{Si } \exists a \in G : |a| = 6, G^{\wedge} = C_6$$

$$|a| = 2, 3, 6$$

$$\forall x \in G, |x| = 2 \Rightarrow G \text{ abeliano}$$

$$\text{Si } |a| = 3, G = \{1, a, a^2, b, a^2b, ab\}$$

$A_n$  es el subgrupo de las permutaciones pares de  $S_n$   
 las permutaciones impares no forman subgrupo

$$\text{Como conjuntos, } |A_n| = |\text{Impares}|$$

$$|A_n| = \frac{n!}{2}$$

Calcular retículo de subgrupos de  $Q_8$  y  $D_4$

ambos son de orden 8

En un producto cartesiano  $G \times H$ , ¿orden de  $(a, b)$ ?

$$\text{u.c.m.}(|a|, |b|)$$