

# Apuntes de Estructuras Algebraicas

Elias Hernandis

29 de octubre de 2018

Revisión del 29 de octubre de 2018 a las 17:26.

# Índice general

<b>I</b>	<b>Primer parcial - hoja 1</b>	<b>5</b>
<b>1.</b>	<b>Grupos</b>	<b>7</b>
1.1.	Grupos . . . . .	7
1.1.1.	Ejemplos de grupos . . . . .	8
1.2.	Subgrupos . . . . .	10
1.2.1.	El teorema de Lagrange . . . . .	12
1.2.2.	Subgrupos normales y grupo cociente . . . . .	12
<b>2.</b>	<b>Homomorfismos de grupos</b>	<b>15</b>
2.1.	Homomorfismos de grupos . . . . .	15
2.1.1.	Producto libre de grupos . . . . .	16
2.2.	Retículo de subgrupos. Teoremas sobre grupos cíclicos. . . . .	17
2.3.	Teoremas random . . . . .	20
2.3.1.	Centro de un grupo y sus propiedades . . . . .	20
2.4.	Teoremas de la isomorfía (versión de clase) . . . . .	21
2.5.	Teoremas de la isomorfía (versión con pies y cabeza) . . . . .	23
2.6.	Construcción de homomorfismos de grupos y de isomorfismos . . . . .	23
<b>3.</b>	<b>Locuras varias que no sé donde van</b>	<b>27</b>
3.1.	Clasificación de grupos finitos . . . . .	27
3.2.	Otras cosas . . . . .	29
3.3.	Teorema de Cauchy . . . . .	30
3.4.	P-grupos . . . . .	31
<b>II</b>	<b>Parcial 2 - hojas 2 y 3</b>	<b>39</b>



Parte I

Primer parcial - hoja 1



# Capítulo 1

## Grupos

### 1.1. Grupos

**Definición 1** (Grupo). Llamamos grupo al par  $(G, *)$ , donde  $G$  es un conjunto no vacío y  $*$  :  $G \times G \rightarrow G$  es una función que cumple las siguientes propiedades:

1. Clausura.  $\forall a, b \in G, a * b \in G$
2. Asociatividad.  $\forall a, b, c \in G, (a * b) * c = a * (b * c)$
3. Elemento neutro.  $\exists e \in G, \forall a \in G \mid a * e = e * a = a$
4. Elemento inverso.  $\forall a \in G, \exists a^{-1} \in G \mid a * a^{-1} = a^{-1} * a = e$

En general, la clausura es muy difícil de probar, por lo que recurrimos a dar un grupo como subgrupo de otro o dar una biyección entre un grupo existente y lo que queremos probar que es grupo.

#### Notación

- Aunque técnicamente el grupo es el par  $(G, *)$ , es común referirse al grupo como  $G$ .
- Cuando la operación es la suma, se suele llamar al elemento neutro  $e = \mathbf{0}$ . Cuando la operación es el producto, se suele llamar al elemento neutro  $e = \mathbf{1}$ .
- Denotamos por  $a^k$ :
  - si  $k > 0$ ,  $a^k = \underbrace{a * a * \dots * a}_{k \text{ veces}}$
  - si  $k = 0$ ,  $a^0 = e$
  - si  $k < 0$ ,  $a^k = \underbrace{a^{-1} * a^{-1} * \dots * a^{-1}}_{-k \text{ veces}}$
- Se suele omitir la operación. Sobre todo cuando la operación es el producto. Por ejemplo, en  $(G, \cdot)$ ,  $a \cdot b = ab$ .

**Teorema 1** (Propiedad cancelativa). Sea  $G$  un grupo,  $a, b, c \in G$ .

$$a * b = a * c \implies b = c \quad (1.1)$$

$$c * a = b * a \implies a = b \quad (1.2)$$

*Demostración.* Por la existencia del elemento inverso podemos multiplicar por  $a^{-1}$  a la izquierda en la primera expresión y obtenemos  $a^{-1}ab = a^{-1}ac \implies eb = ec \implies b = c$ . Lo mismo ocurre por la derecha en la segunda expresión. ♣

**Proposición 1** (Unicidad del elemento neutro). En un grupo  $G$  hay exactamente un elemento neutro  $e$ .

*Demostración.* Supongamos existen  $e_1, e_2 \in G$  elementos neutros. Por ser  $e_1$  elemento neutro se tiene que  $e_1 * e_2 = e_2$  y por ser elemento neutro  $e_2$  se tiene que  $e_1 * e_2 = e_1$ . Por tanto  $e_1 = e_2$ . ♣

**Proposición 2** (Unicidad del inverso de un elemento). Sea  $G$  un grupo,  $g \in G$ , entonces  $\exists! g^{-1} \mid g * g^{-1} = e$ .

*Demostración.* Supongamos  $a$  tiene inversos  $b_1$  y  $b_2$ . Entonces  $a * b_1 = a * b_2 = e$ . Por la propiedad cancelativa  $b_1 = b_2$ . ♣

**Definición 2** (Orden de un elemento). Sea  $(G, *)$  un grupo. Decimos que  $a \in G$  tiene orden finito si  $\exists k \in \mathbb{N}$  tal que  $a^k = e$ . Si existen tales valores de  $k$ , llamamos orden del elemento  $a$  al mínimo de ellos:

$$o(a) = \min\{k \in \mathbb{N} \mid a^k = e\} \quad (1.3)$$

**Definición 3** (Orden o cardinalidad de un grupo). Sea  $G = \{a_1, a_2, \dots\}$  un grupo junto con alguna operación. Si  $|G| < \infty$  decimos que el orden de  $G$ ,  $|G| = |\{a_1, a_2, \dots, a_n\}| = n$ .

**Definición 4** (Grupo abeliano). Sea  $(G, *)$  un grupo. Diremos que  $G$  es abeliano  $\iff \forall a, b \in G, a * b = b * a$ .

**Teorema 2.** Sea  $G$  un grupo tal que  $\forall g \in G, g * g = e$ . Entonces  $G$  es abeliano.

**Corolario.**  $\forall a \in G, o(a) = 2 \implies G$  es abeliano.

*Demostración.* Sean  $a, b \in G$ . Tenemos que probar que  $a * b = b * a$ . Consideramos el elemento  $(a * b) \in G$  por clausura. Por hipótesis tenemos que  $(a * b) * (a * b) = e \implies (a * b) = (a * b)^{-1} = b^{-1} * a^{-1} = b * a$ . ♣

### 1.1.1. Ejemplos de grupos

**Ejemplo 1** (Ejemplos de grupos infinitos).

- $(\mathbb{R}, +)$  es un grupo
- $(\mathbb{R}, \cdot)$  no es un grupo porque el 0 no tiene inverso
- $(\mathbb{R} \setminus \{0\}, \cdot)$  es un grupo
- $(\mathbb{R} > 0, \cdot)$  es un grupo (subgrupo de  $\mathbb{R}$ )
- $(\mathbb{R} < 0, \cdot)$  no es un subgrupo porque no es cerrado
- $(\mathbb{Z}, +)$  es un grupo
- $n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\}$  con la suma es un grupo
- $GL_2(\mathbb{R}) = \{A \in R^{2 \times 2} \mid \det A \neq 0\}$  las matrices reales  $2 \times 2$  forman un grupo con el producto
- Por lo anterior, las aplicaciones lineales que tienen inversa forman un grupo con la composición (componer aplicaciones es lo mismo que multiplicar matrices y la inversa existe  $\iff \det A \neq 0$ )

**Ejemplo 2** (Grupo de las clases módulo  $n$ ).

$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$  con la suma es un grupo

**Ejemplo 3** (Grupo de cuaterniones). Llamamos  $H$  al subgrupo de  $GL_2(\mathbb{C})$  generado por  $A$  y  $B$ :  $H = \langle A, B \rangle$  donde

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

De probar las multiplicaciones de  $A$  y de  $B$  consigo mismas y entre ellas se obtiene la presentación.

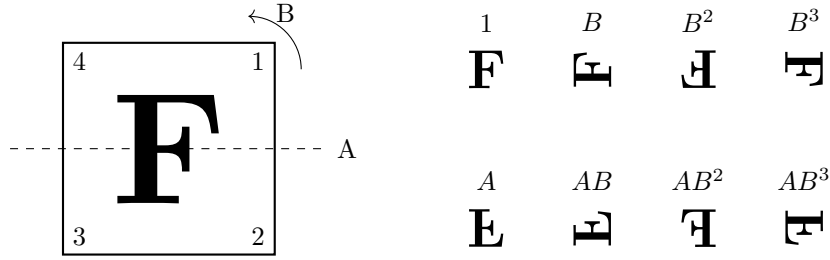
$$o(A) = o(B) = 4 \quad A^2 = B^2 \quad BA = AB^3$$

y queda que  $H = \{1, B, B^2, B^3, A, AB, AB^2, AB^3\}$ . Es posible obtener cualquier operación de  $A$  y  $B$  a partir de la presentación.

elemento	1	$B$	$B^2$	$B^3$	$A$	$AB$	$AB^2$	$AB^3$
orden	1	4	2	4	4	4	4	4

Figura 1.1: Órdenes de los elementos de  $H$



Figura 1.2: Simetría  $A$  y rotación  $B$  que compuestas forman los elementos del grupo  $D_4$ 

**Ejemplo 4** (El famoso grupo  $D_4$ ).  $D_4$  es el grupo formado por las composiciones de rotaciones y simetrías que llevan un cuadrado en un cuadrado ( $f(\square) = \square$ ). También se llama grupo diédrico de orden 4.

Geométricamente,

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}, \quad \alpha = \frac{\pi}{2}$$

pero una vez hemos comprobado que todas las posibles operaciones  $A^i B^j$  y  $B^i A^j$  quedan dentro del grupo (que es cerrado), que existe el neutro (la identidad) y que cada elemento tiene su inverso, podemos obviar el significado geométrico y pasar a describirlo mediante la presentación del grupo.

$$D_4 = \langle A, B \rangle \text{ donde } o(A) = 2, \quad o(B) = 4, \quad BA = AB^3 \quad (1.4)$$

y además queda que  $D_4 = \{1, B, B^2, B^3, A, AB, AB^2, AB^3\}$ .

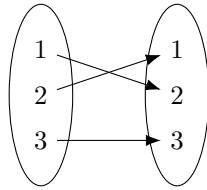
elemento	1	$B$	$B^2$	$B^3$	$A$	$AB$	$AB^2$	$AB^3$
orden	1	4	2	4	2	-	-	-

Figura 1.3: Órdenes de los elementos de  $D_4$ 

**Nota:** lo que hemos hecho con un cuadrado también se puede hacer con un triángulo.

**Ejemplo 5** (Grupo de biyecciones  $S_3$ ). Llamamos  $S_3$  al grupo de las biyecciones  $f : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$ . También podemos pensar en este grupo como el grupo de las permutaciones de 3 elementos. De hecho, utilizamos la siguiente notación para las biyecciones de  $S_3$ :

- (1) indica que  $f(1) = 1$ . Por defecto,  $f(2) = 2$  y  $f(3) = 3$ .
- (12) indica que  $f(1) = 2$  y  $f(2) = 1$ . Por defecto  $f(3) = 3$ .
- (123) indica que  $f(1) = 2$ ,  $f(2) = 3$ ,  $f(3) = 1$ .
- (13) indica que  $f(1) = 3$ ,  $f(3) = 1$  y por defecto  $f(2) = 2$ .

Figura 1.4: Elemento (12) de  $S_3$ 

En este grupo ocurre algo parecido a lo que ocurre en  $D_4$ . Sea  $a = (123)$ ,  $b = (12)$ . Podemos presentar el grupo con

$$S_3 = \langle a, b \rangle \text{ donde } o(a) = 3, \quad o(b) = 2, \quad ba = ab^2 \quad (1.5)$$

y por tanto  $S_3 = \{1, a, a^2, b, ab, a^2b\} = \{(1), (12), (13), (23), (123), (132)\}$ .

Por último, vemos una manera de generar nuevos grupos a partir de grupos existentes.

**Definición 5** (Producto directo de grupos). Sean  $(G_1, *)$ ,  $(G_2, \bullet)$  grupos. Llamamos producto directo de los grupos  $G_1$  y  $G_2$  al grupo  $(G_1 \times G_2, \sim)$ . Donde  $\sim : (G_1 \times G_2) \times (G_1 \times G_2) \rightarrow G_1 \times G_2$ ,  $(g_1, g_2) \sim (g'_1, g'_2) = (g_1 * g'_1, g_2 \bullet g'_2)$ .

## 1.2. Subgrupos

**Definición 6** (Subgrupo). Sea  $(G, *)$  un grupo,  $S \in G, S \neq \emptyset$ . Diremos que  $(S, *)$  es un subgrupo de  $(G, *)$  y lo denotaremos por  $S < G$  si verifica las siguientes condiciones:

1. Clausura.  $\forall a, b, a, b \in S \implies a * b \in S$
2. Elemento neutro.  $e \in S$
3. Elemento inverso.  $\forall s \in S, s^{-1} \in S$

(La propiedad asociativa siempre se hereda.)

**Proposición 3.** Si  $\{S_i\}_{i \in \mathbb{N}}$  es una familia de subgrupos de  $G$ , entonces  $\bigcap S_i$  también es un subgrupo de  $G$ .

**Definición 7** (Subgrupo generado varios elementos). Sea  $(G, *)$  un grupo,  $S \subset G, S \neq \emptyset$ . El subgrupo generado por  $S$  es

$$\langle S \rangle = \{s_1^{\alpha_1} * s_2^{\alpha_2} * \dots * s_n^{\alpha_n} \mid s_1, s_2, \dots, s_n \in S, \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}\} \quad (1.6)$$

<sup>a</sup>Este teorema reemplaza al de grupo generado por dos elementos dado en clase.

**Proposición 4.** El subgrupo generado por  $S, \langle S \rangle$  es el más pequeño que contiene a  $S$ .

El siguiente teorema no lo ha dado drácula<sup>1</sup> pero no me acuerdo pero viene en [?] y simplifica bastante la vida.

**Teorema 3.** Sea  $G$  un grupo y  $H$  un subconjunto de  $G$ . Entonces  $H < G \iff \forall x, y \in H, xy^{-1} \in H$ .

*Demostración.* De [?].

- ( $\implies$ ). Supongamos que  $H < G$ . Entonces  $x, y \in H \implies xy \in H \wedge y \in H \implies y^{-1} \in H$  y por tanto  $xy^{-1} \in H$ .
- ( $\impliedby$ ). Supongamos que  $x, y \in H \implies xy^{-1} \in H$ . Veamos que se cumplen las 3 condiciones para que sea subgrupo:
  - Elemento neutro. Tomamos  $y = x$  y tenemos que  $xx^{-1} = e \in H$ .
  - Elemento inverso. Tomamos ahora  $x = e, y = x$  y tenemos que  $ex^{-1} = x^{-1} \in H$ .
  - Clausura. Tenemos que si  $x, y \in H$  por la propiedad anterior  $y^{-1} \in H$  y por tanto  $xy = x(y^{-1})^{-1} \in H$ .



Normalmente, utilizaremos la definición restringida a un elemento:

**Definición 8** (Subgrupo generado por un elemento). Sea  $G$  un grupo,  $g \in G$ . Llamamos subgrupo generado por  $g$  a

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\} \quad (1.7)$$

**Proposición 5.** El subgrupo generado por  $g \in G$  en efecto es un subgrupo.

*Demostración.*

1. Es cerrado por  $*$  puesto que  $\forall a^k, a^{k'} \in S, a^k * a^{k'} = a^{k+k'} \in S$ .
2.  $a^0 = e \in A$
3.  $\forall a^k, a^{-k} \in A$



**Proposición 6.** Si  $o(g) = n$ , entonces  $\langle g \rangle$  tiene  $n$  elementos (el orden de  $\langle g \rangle$  es  $n$ ).

*Demostración.* Primero comprobamos que no hay más de  $n$  elementos distintos. Consideramos  $k \in \mathbb{Z}, k = cn + r$  para algunos  $c, r \in \mathbb{Z}, 0 \leq r < n$  por el algoritmo de la división. Entonces  $a^k = a^{cn+r} = a^{cn}a^r = a^r$  pues  $o(a) = n$ .

Ahora probaremos que no hay menos de  $n$  elementos distintos, es decir, que  $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$  Supongamos existen  $0 \leq i < j < n$  tales que  $a^i = a^j$ . Entonces por cancelación  $a^{j-i} = e = a^0 \implies j = i$  lo que da una contradicción.



<sup>1</sup>De verdad que quería poner el nombre.

**Teorema 4.** Sea  $G$  un grupo,  $g \in G$ . El menor subgrupo de  $G$  que contiene a  $g$  es  $\langle g \rangle$ .

*Demostración.* Tenemos que probar que para cualquier  $H$  subgrupo de  $G$ ,  $g \in H \implies g^k, \forall k \in \mathbb{Z}$ . ♣

**Definición 9** (Grupo cíclico). Sea  $(G, *)$  un grupo. Diremos que  $G$  es cíclico si  $\exists g \in G \mid \langle g \rangle = G$ .

**Teorema 5.** Si  $G$  es cíclico entonces  $G$  es abeliano.

*Demostración.* Tenemos que probar que  $\forall a, b \in G, ab = ba$ . Sabemos que  $a = g^i, b = g^j$  para algunos  $i, j \in \mathbb{Z} \implies ab = a^i a^j = a^{i+j} = a^{j+1} = a^j a^i = ba$ . ♣

**Teorema 6.** Sea  $g \in G$  tal que  $o(g) = n \in \mathbb{N} \geq 1$  y sea  $r \in \mathbb{N}$ . Si  $r$  y  $n$  son coprimos, entonces  $\langle g \rangle = \langle g^r \rangle$ .

**Corolario.** Si  $r$  y  $n = o(g)$  son coprimos entonces  $o(g) = o(g^r)$ .

*Demostración.* Recordamos que  $p$  y  $q$  son coprimos  $\iff \exists \alpha, \beta \in \mathbb{Z} \mid \alpha p + \beta q = 1$ . Recordamos que  $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$  donde  $n = o(g)$ . Tenemos que probar la doble inclusión. Fijémonos en que  $g^r \in \langle g \rangle \implies \langle g^r \rangle \subset \langle g \rangle$  pues  $\langle g \rangle$  contiene a todos los elementos de la forma  $g^k, k \in \mathbb{Z}$  (ver definición 8). Ahora probaremos que  $\langle g \rangle \subset \langle g^r \rangle$ . Como  $r$  y  $n$  son coprimos,  $g = g^{\alpha r + \beta n} = (g^r)^\alpha (g^n)^\beta = (g^r)^\alpha \in \langle g^r \rangle \implies \langle g \rangle \subset \langle g^r \rangle$ . Concluimos que  $\langle g \rangle = \langle g^r \rangle$ . ♣

**Ejemplo 6.** En  $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$  con la suma tomamos  $g = 1$  y por tanto  $n = o(g) = 4$ , y tomamos  $r = 3$  y por tanto  $\text{mcd}(n, r) = 1$ . Efectivamente se verifica que  $o(1^3) = o(1 + 1 + 1) = o(3) = 4 = o(1)$  o lo que es lo mismo,  $\langle 1 \rangle = \langle 3 \rangle$ .

**Teorema 7.** Sea  $g \in G$  tal que  $o(g) = n$  y sea  $r \in \mathbb{N}$  con  $r \mid n$  ( $r$  divide a  $n$ ). Entonces  $o(g^r) = \frac{n}{r}$ .

*Demostración.* Sea  $n'$  tal que  $n = rn'$ . Probaremos que  $r \mid n \implies o(g^r) = n'$ .

$$\langle g^r \rangle = \{g^r, g^{2r}, g^{3r}, \dots, g^{n'r} = g^n\} \subset \{g, g^2, g^3, \dots, g^n\} = \langle g \rangle$$

$\langle g^r \rangle$  tiene  $n'$  elementos distintos porque para cualquier  $i = 0, \dots, n', o(g^{ir}) \leq o(g) = n$  por lo que no se repite ninguno. Además cualquier  $g^{ir}$  está bien definido porque al dividir  $r$  a  $n$ ,  $ir \in \mathbb{N}$ . ♣

**Teorema 8** (Hoja 1, ejercicio 9). Sea  $o(g) = n \in \mathbb{N}$  y sea  $N \in \mathbb{Z}$ . Entonces  $o(g^N) = \frac{o(g)}{\text{mcd}(N, o(g))}$ .

*Demostración.* Afirmamos que  $n$  y  $N/d$ , con  $d = \text{mcd}(N, n)$  son coprimos. Expresamos  $g^N = (g^{N/d})^d$ . Por el [corolario del] teorema 6 tenemos que  $o(g^{N/d}) = o(g) = n$ . Por el teorema 7 tenemos que  $o((g^{N/d})^d) = \frac{o(g^{N/d})}{d} = \frac{n}{d}$ . ♣

**Teorema 9** (Hoja 1, ejercicio 7). Sea  $(G, *)$  un grupo y  $S \subset G, S \neq \emptyset$  un subconjunto finito de  $G$ . Si  $S$  es cerrado por la operación  $*$  entonces  $S$  es un subgrupo de  $G$ .

*Demostración.* Se verifican las 3 propiedades

1. Clausura. Por hipótesis.
2. Elemento neutro. Sea  $s \in S$ . Si  $s = e$  ya hemos terminado. Si  $s \neq e$ , sabemos que  $\{s^1, s^2, \dots\} \subset S$ . Pero  $S$  es finito  $\implies \exists 0 < i < j$  tales que  $s^i = s^j \implies s^{j-i} = e$ . Como  $j > i \implies j - i > 0$ , hemos obtenido  $e$  de operar  $s$  consigo mismo, luego  $e \in S$ .
3. Elemento inverso. Tomamos  $r = j - i$  de la propiedad anterior. Tenemos  $s^r = e \implies s * s^{r-1} = e \implies s^{r-1} = s^{-1}$ .

### 1.2.1. El teorema de Lagrange

**Definición 10** (Clase lateral). Sea  $(G, *)$  un grupo,  $H < G$ ,  $g \in G$ . Definimos

- $g * H = gH = \{g * h \mid h \in H\}$  es una clase lateral izquierda de  $H$
- $H * g = Hg = \{h * g \mid h \in H\}$  es una clase lateral derecha de  $H$

**Teorema 10.** Si  $H < G$  tiene orden  $n < \infty$  entonces  $|gH| = |Hg| = |H| = n$ .

*Demostración.* Consideramos la aplicación  $f : H \rightarrow gH$ ,  $f(h) \rightarrow g * h$  para un  $g \in G$  dado. Es inyectiva:  $f(h_1) = f(h_2) \implies h_1 = h_2$  puesto que  $gh_1 = gh_2 \implies h_1 = h_2$  por la propiedad cancelativa. Es sobreyectiva porque  $\forall h \in H$ ,  $g * h = f(h)$ . Por tanto  $f$  es biyectiva y los órdenes son iguales. ♣

**Proposición 7.** Sea  $H < G$ ,  $g \in G$ . Las clases laterales  $gH$  y  $Hg$  cumplen las siguientes propiedades (las cumplen las dos pero damos solo las de la izquierda):

1.  $g \in H \iff g * H = H$
2.  $g \in g * H \implies G = \bigcup_{g \in G} g * H$
3.  $g' \in g * H \implies g' * H = g * H$
4.  $g_1 * H \cap g_2 * H \neq \emptyset \implies g_1 * H = g_2 * H$

*Demostración.* (solo de la última propiedad) Sabemos que existe  $\alpha \in g_1 * H \cap g_2 * H$  de la forma  $\alpha = g_1 * h_1 = g_2 * h_2$ ,  $h_1, h_2 \in H$ . Ahora bien,  $g_1 * h_1 = g_2 * h_2 \iff g_2^{-1} * g_1 * h_1 = h_2 \iff g_2^{-1} g_1 \in H \implies g_2(g_2^{-1} g_1)H = g_2(g_2^{-1} g_1 H) = g_2 H$ . ♣

De las propiedades anteriores se obtiene que  $\{g_i * H\}_{g_i \in G}$  es una partición de  $G$ . Además, por el teorema 10, como  $|g * H| = |H|$  la partición divide  $G$  en cajas iguales (ver cuadro 1.5). Pongamos que  $G$  es finito y que hay  $r$  cajas, entonces  $|G| = r|g_i * H| = r|H| \implies |H| \mid |G|$ . A continuación veremos otra forma de dar esta relación de equivalencia.

Para algún  $H < G$ , la partición que hemos dado anteriormente es la definida por la relación de equivalencia  $g_1 R g_2 \iff g_1 * H = g_2 * H$ . Otra manera de definirla es  $g_1 R g_2 \iff g_2^{-1} g_1 \in H$ . Se verifica que esta nueva definición es una relación de equivalencia.

$g_1 * H$	$g_2 * H$	...
...	$H$	...
...	$g_{r-1} * H$	$g_r * H$

Figura 1.5: Partición de  $G$  en  $r$  cajas iguales

**Teorema 11** (de Lagrange). Sea  $G$  un grupo finito y  $H < G$ . Entonces  $|H| \mid |G|$  (el orden de  $H$  divide al orden de  $G$ ).

**Corolario.** Sea  $G$  un grupo y  $g \in G$ . Entonces  $o(g) \mid |G|$  (el orden de un elemento divide al orden del grupo).

**Corolario.** Si  $G$  es un grupo de orden  $p$ , con  $p$  primo, entonces  $G$  es cíclico.

*Demostración.* Sea  $g \in G$ ,  $g \neq e$ . Por el teorema de Lagrange  $|\langle g \rangle| \mid |G| = p$ . Como  $p$  es primo sus únicos divisores son 1 y  $p$  y como  $|\langle g \rangle| > 1$  se ha de tener  $|\langle g \rangle| = p$ . Por tanto  $\langle g \rangle = G$  y  $G$  es cíclico. ♣

### 1.2.2. Subgrupos normales y grupo cociente

**Definición 11** (Subgrupo normal). Sea  $H < G$ . Diremos que  $H$  es un subgrupo normal de  $G$  y lo denotaremos por  $H \triangleleft G \iff \forall g \in G$ ,  $g * H = H * g$ .

**Proposición 8.** Si  $G$  es abeliano entonces todos sus subgrupos son normales.

**Definición 12** (Conjunto cociente en grupos). Sea  $H < G$ . Definimos

$$G/H = \{gH \mid g \in G\} = \{\bar{x} \mid \bar{x} = \{g \in G \mid g^{-1}x \in H\}\} \quad (1.8)$$

**Proposición 9.** Sea  $H \triangleleft G$ .  $(G/H, *)$  con la operación  $* : G/H \rightarrow G/H, (xH)(yH) \mapsto (xy)H$  es un grupo.

*Demostración.* La operación  $*$  está bien definida.  $\forall \bar{x}, \bar{y} \in G/H, \bar{x} * \bar{y} = xHyH = xyHH = xyH = \overline{xy}$ .

El elemento neutro es  $\bar{e}$  pues  $\forall \bar{x} \in G/H, \bar{e} * \bar{x} = eHxH = exH = xH = \bar{x}$ .

El elemento inverso está bien definido:  $\bar{x}^{-1} = \overline{x^{-1}}$  pues  $\forall \bar{x} \in G/H, \bar{x}\bar{x}^{-1} = xHx^{-1}H = xx^{-1}H = eH = \bar{e}$ . ♣

**Definición 13** (Índice). Sea  $H < G$ . Definimos el **índice de  $H$  en  $G$** , y lo representamos mediante  $[G : H]$ , como el cardinal del conjunto cociente  $G/H$ . [?]

**Teorema 12.** De [?]<sup>a</sup> Sea  $H < G$  con  $[G : H] = 2$  (con índice de  $H$  en  $G$  igual a 2). Entonces  $H$  es normal.

<sup>a</sup>No lo hemos dado explícitamente pero se utiliza para algunos ejemplos.



## Capítulo 2

# Homomorfismos de grupos

### 2.1. Homomorfismos de grupos

**Definición 14** (Homomorfismo de grupos). Sean  $(G_1, \cdot), (G_2, *)$  grupos. Decimos que  $f : G_1 \rightarrow G_2$  es un homomorfismo de grupos si  $\forall a, b \in G_1, f(a \cdot b) = f(a) * f(b)$ .

- si  $f$  es inyectiva,  $f$  es un monomorfismo
- si  $f$  es sobreyectiva,  $f$  es un epimorfismo
- si  $f$  es biyectiva,  $f$  es un isomorfismo
- si  $G_2 = G_1$  y  $f$  es un isomorfismo, entonces  $f$  se llama automorfismo

Si existe un isomorfismo entre dos grupos, decimos que son isomorfos y lo denotamos por  $G_1 \simeq G_2$ .

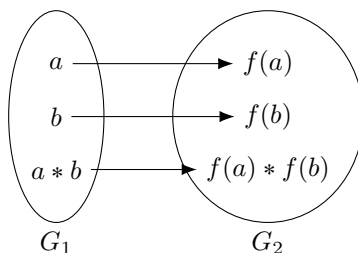


Figura 2.1: Homomorfismo de grupos

**Definición 15** (Núcleo de un homomorfismo). Sea  $f : G_1 \rightarrow G_2$  un homomorfismo. Definimos el núcleo  $\ker f = \{x \in G_1 \mid f(x) = e_2 \in G_2\}$  (los que van a parar al neutro).

**Definición 16** (Imagen de un homomorfismo). Sea  $f : G_1 \rightarrow G_2$  un homomorfismo. Definimos la imagen  $\text{Im} f = \{y \in G_2 \mid \exists x \in G_1, f(x) = y\}$ .

**Proposición 10.** Sea  $f : G_1 \rightarrow G_2$  un homomorfismo.  $\ker f < G_1$ .

*Demostración.* Probamos las 3 propiedades de los subgrupos

1.  $a, b \in \ker f \implies a \cdot b \in \ker f$ .  $f(a \cdot b) = f(a) * f(b) = e_2 * e_2 = e_2$ .
2.  $a \in \ker f \implies a^{-1} \in \ker f$ .  $f(a) = e_2, f(a^{-1}) = e_2 \implies (f(a))^{-1} = e_2$ .
3.  $e_1 \in \ker f$ .



**Teorema 13.** Sea  $f : G_1 \rightarrow G_2$  un homomorfismo.  $\text{Im} f < G_2$ .

*Demostración.* Es análoga a la del  $\ker f$ . ♣

**Teorema 14.** Sea  $f : G_1 \rightarrow G_2$  un homomorfismo.  $\ker f \triangleleft G_1$

*Demostración.* Tenemos que probar que  $\forall a \in G_1, a(\ker f)a^{-1} \subset \ker f$ .

Sea  $h \in \ker f$ .  $f(aha^{-1}) = f(a) \underbrace{f(h)}_{e_2} f(a^{-1}) = f(a)f(a^{-1}) = e_2 \in \ker f$  ♣

**Proposición 11.** Sea  $f : G_1 \rightarrow G_2$  un homomorfismo de grupos.  $f$  es inyectiva si y solo si  $\ker f = \{e\}$ .

*Demostración.*

- (  $\Leftarrow$  ) Suponemos que  $f$  es inyectiva. Sabemos que en un homomorfismo  $f(e_1) = e_2$  y además  $\ker f = e_1$  por hipótesis.
- (  $\Rightarrow$  ) Tenemos que probar que dados  $a, b \in G_1$ ,  $f(a) = f(b) \Rightarrow a = b$ . Decir que  $f(a) = f(b)$  es lo mismo que decir  $e_2 = f(a)^{-1}f(b) = f(a^{-1})f(b) = f(a^{-1}b) \Rightarrow a^{-1}b \in \ker f = \{e_1\} \Rightarrow a = b$ . ♣

**Proposición 12.** Sean  $G_1, G_2, G_3$  grupos y sean  $f : G_1 \rightarrow G_2$ ,  $g : G_2 \rightarrow G_3$  homomorfismos de grupos. Entonces  $g \circ f$  es a su vez un homomorfismo de grupos.

**Teorema 15.** Sea  $f : G_1 \rightarrow G_2$  un homomorfismo de grupos. Entonces  $o(f(g))$  divide a  $o(g)$ .

**Teorema 16.** Sea  $f : G_1 \rightarrow G_2$  un isomorfismo de grupos. Entonces  $o(g) = o(f(g))$ .

*Demostración.* Consideramos  $f$  y  $f^{-1}$  para los que se verifica el teorema anterior.  $o(g) \mid o(f(g)) \wedge o(f(g)) \mid o(f^{-1}(f(g))) = o(g) \Rightarrow o(g) = o(f(g))$ . ♣

### 2.1.1. Producto libre de grupos

**Definición 17** (Producto libre de grupos). Sean  $S, T$  subconjuntos del grupo  $G$ . Definimos  $ST = \{s * t \mid s \in S \wedge t \in T\}$ .

Observemos que la función  $f : S \times T \rightarrow ST$ ,  $(s, t) \mapsto st$  no es un homomorfismo de grupos. Esto es porque al operar dos elementos de  $S \times T$  no se comporta bien. Sean  $s, s' \in S, t, t' \in T$

$$\begin{aligned} (s, t) &\mapsto st \\ (s', t') &\mapsto s't' \end{aligned}$$

esperamos que

$$f((s, t)(s', t')) = f(st, s't') \mapsto f(s, t)f(s', t') = sts't'$$

pero en realidad ocurre que

$$f((s, t), (s', t')) \mapsto ss'tt' \neq f(s, t)f(s', t')$$

No obstante, aunque la función que lleva  $H_1 \times H_2 \rightarrow H_1H_2$  no sea un homomorfismo, sí podemos saber cuantos elementos tiene  $H_1H_2$ .

**Teorema 17** (Cardinalidad del producto libre). Sean  $H_1, H_2 < G$  con  $G$  finito. Entonces

$$|H_1H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|} \quad (2.1)$$

*Demostración.* Utilizaremos la función  $f : H_1 \times H_2 \rightarrow H_1H_2$  que es sobreyectiva por definición de  $H_1H_2$ . Para una función sobreyectiva  $f : A \rightarrow B$ ,  $|A| = \sum_{b \in B} |f^{-1}(b)|$ .

Sean las fibras los conjuntos  $f^{-1}(h_1h_2)$  de los pares de elementos que van a parar al mismo  $h_1h_2 \in H_1H_2$ . La condición necesaria y suficiente para que  $(h'_1, h'_2)$  esté en la misma fibra que  $(h_1, h_2)$  es que  $h'_1 = h_1\alpha \wedge h'_2 = h_2\alpha$ ,  $\alpha \in H_1 \cap H_2$ . Entonces  $|f^{-1}(h_1, h_2)| = |(h_1\alpha, h_2\alpha)|$ ,  $\alpha \in H_1 \cap H_2 = |H_1 \cap H_2| \Rightarrow |H_1||H_2| = |H_1H_2||H_1 \cap H_2|$  ♣



**Teorema 18.** Sean  $H_1, H_2$  subgrupos de  $G$ , con  $G$  finito. Si  $H_2 \triangleleft G$  entonces  $H_1 H_2 < G$  (si uno de los subgrupos es normal, entonces el producto es subgrupo).

*Demostración.* Observamos que podemos escribir  $H_1 H_2 = \bigcap_{h \in H_1} h * H_2$ . Como  $H_2 \triangleleft G$ ,  $h * H_2 \cdot h' H_2 = hh' H_2 \forall h \in H_1$ . Si nos fijamos  $H_1 H_2$  es cerrado por la operación pues  $hh' H_2 \in H_1 H_2$  y como  $G$  es finito y por tanto  $H_1, H_2$  también,  $H_1 H_2$  es un subgrupo. ♣

**Teorema 19.** Si  $H_1 \triangleleft G \wedge H_2 \triangleleft G \implies H_1 H_2 \triangleleft G$  (si los dos subgrupos son normales, entonces el producto también es normal).

*Demostración.*  $H_1, H_2 < G$  luego  $\forall g \in G$ ,  $g H_1 H_2 g^{-1} = g H_1 g^{-1} g H_2 g^{-1} = H_1 H_2$ . ♣

## 2.2. Retículo de subgrupos. Teoremas sobre grupos cíclicos.

**Definición 18** (Retículo de subgrupos). Dado un grupo  $G$ , el retículo de subgrupos es un grafo con todos los subgrupos de  $G$ . Denotamos la relación de inclusión con un vértice entre dos grupos. Es costumbre poner el mayor grupo arriba y denotar la inclusión por las diferencias en altura.

Lo importante de esta sección:

- Todo subgrupo de un grupo cíclico es cíclico.
- Dado un epimorfismo entre dos grupos existe una correspondencia biyectiva entre los subgrupos del primero y los del segundo.
- En  $\mathbb{Z}/n\mathbb{Z}$  existe un subgrupo por cada divisor de  $n$  y esos son todos los subgrupos que hay.

**Ejemplo 7** (Retículo de subgrupos  $\mathbb{Z}$ ).  $\mathbb{Z}$  tiene infinitos subgrupos, todos los  $k\mathbb{Z}$ . En muchas ocasiones nos va a interesar solo dibujar unos pocos, para relacionarlos con subgrupos de otros grupos distintos de  $\mathbb{Z}$ . A continuación se muestra el retículo de subgrupos de  $\mathbb{Z}$  construido a partir de  $6\mathbb{Z}$ .

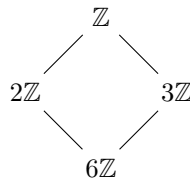


Figura 2.2: Una parte del retículo de subgrupos de  $\mathbb{Z}$ , en concreto la de los  $n\mathbb{Z}$  con  $n \mid 6$ .

Los grupos que contienen a  $6\mathbb{Z}$  son los de la forma  $k\mathbb{Z}$  donde  $k$  divide a 6, ya que entre los múltiplos de los divisores de 6 también se encuentran los múltiplos de 6.

**Proposición 13.** Sea  $n = \min_{r \in \mathbb{N}, r > 0} \{r \in H, H < \mathbb{Z}\}$ . Entonces  $nH = \mathbb{Z}$ .

*Demostración.* Probamos la doble inclusión. Por hipótesis  $n \in H$  y por tanto  $\langle n \rangle = n\mathbb{Z} \subset H$ . Sea  $\alpha \in H$ . Por el algoritmo de la división, podemos expresar  $\alpha = an + s$  con  $0 \leq s < n \implies s = 0 \implies H \subset n\mathbb{Z}$ . Luego  $H = n\mathbb{Z}$ . ♣

El siguiente teorema no lo ha dado Orlando explícitamente pero básicamente lo que dice es lo que dijo en las 3 clases sobre correspondencia entre subgrupos pero un poco más ordenado.

**Teorema 20** (de correspondencia entre subgrupos mediante homomorfismos). Sea  $f : G_1 \rightarrow G_2$  un homomorfismo de grupos. Se tiene [?]:

1. Si  $H_1 < G_1$  entonces  $f(H_1) < G_2$
2. Si  $H_2 < G_2$  entonces  $f^{-1}(H_2) = \{h_1 \in G_1 \mid f(h_1) \in H_2\} < G_1$
3. Si  $H_2 \triangleleft G_2$  entonces  $f^{-1}(H_2) \triangleleft G_1$
4. Si  $H_1 \triangleleft G_1$  y  $f$  es además sobreyectiva (es un epimorfismo) entonces  $f(H_1) \triangleleft G_2$

*Demostración.*

1. Demostramos que se cumplen las 3 propiedades de los grupos. Sabemos que  $e_1 \in H_1 \implies e_2 \in f(H_1) = H_2$ . Además, sabemos que  $\forall x \in H_1, x^{-1} \in H_1$  y por ser  $f$  un homomorfismo tenemos que  $\forall f(x) \in H_2, f(x)^{-1} = f(x^{-1}) \in H_2$ . Por último, tenemos que  $\forall x, y \in H, xy \in H_1 \implies \forall f(x), f(y) \in H_2, f(x)f(y) = f(xy) \in H_2$ .
2. Es análoga a la de la primera afirmación.
3. Tenemos que probar que para un  $g_1 \in G_1, \forall h_1 \in f^{-1}(H_2) = H_1, g_1 h_1 = h_1 g_1$ . Sabemos que  $\forall h_1, \exists h_2 \in H_2 \mid f^{-1}(h_2) = h_1$ . Entonces  $g_1 h_1 = h_1 g_1 \iff f^{-1}(g_2) f^{-1}(h_2) = f^{-1}(h_2) f^{-1}(g_2) \iff f^{-1}(g_2 h_2) = f^{-1}(h_2 g_2)$  que es cierto por hipótesis de que  $H_2$  es normal.
4. Tenemos que probar que para  $g_2 \in G_2$  dado,  $\forall h_2 \in H_2 = f(H_1), g_2 h_2 = h_2 g_2$ . Comenzamos por asegurar que  $\exists g_1 \in G_1 \mid f(g_1) = g_2$  por ser  $f$  sobreyectiva. Por tanto  $g_2 h_2 = h_2 g_2 \iff f(g_1) f(h_1) = f(h_1) f(g_1) \iff f(g_1 h_1) = f(h_1 g_1)$  que es cierto por hipótesis.

♣

Queremos establecer una relación entre los retículos de subgrupos de dos grupos que son el dominio y la imagen de un epimorfismo  $f : G_1 \rightarrow G_2$ . Los subgrupos de  $G_2$  siempre contendrán al elemento neutro  $e_2$  por lo que podemos establecer una relación natural entre los subgrupos de  $G_1$  que contienen a  $\ker f$  con los subgrupos de  $G_2$ .

**Teorema 21.** <sup>a</sup> Sea  $f : G_1 \rightarrow G_2$  un epimorfismo. Existe una biyección entre el retículo de subgrupos de  $G_2$  y subgrupos de  $G_1$  que contienen al  $\ker f$ . Se cumple que  $H_2 < G_2 \iff f^{-1}(H_2) \supset \ker f$ .

En particular, el número de subgrupos de  $G_2$  es igual al número de subgrupos de  $G_1$  que contienen al núcleo.

$$|\{H_2 \mid H_2 < G_2\}| = |\{H_1 < G_1 \mid \ker f \in H_1\}|$$

<sup>a</sup>Este teorema es un desastre. Las hipótesis no las ha dado y las conclusiones tampoco. Es lo que más o menos he creído que quería decir. Es posible que se corresponda con la proposición 4.4.6 del [?] pero en dicha proposición no se exige que  $f$  sea sobre.

*Demostración.* Sabemos que por ser  $f$  homomorfismo,  $H_1 < G_1 \implies f(H_1) < G_2$ .

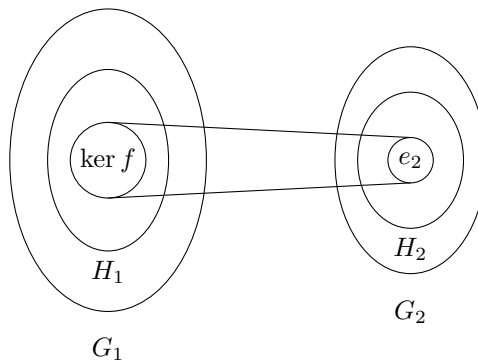
Veamos que la relación entre los subconjuntos de  $G_1$  y de  $G_2$  se mantiene al aplicar el epimorfismo. Sea  $H_2 \subset G_2$ . Como  $f$  es sobre  $f(f^{-1}(H_2)) = H_2$ . Ahora sea  $H'_2 \mid H_2 \subset H'_2 \subset G_2$ . Ocurre lo de antes y además  $f^{-1}(H_2) \subset f^{-1}(H'_2) \subset G_1$ .

Ahora lo extendemos de subconjuntos a subgrupos. Asociamos a cada  $H_2 < G_2$  el subgrupo  $f^{-1}(H_2) < G$ . Es un subgrupo porque al ser  $f$  epimorfismo mantiene la operación. En particular,  $e_2 \in H_2 \implies \ker f = f^{-1}(e_2) \subset f^{-1}(H_2)$ .

Por último afirmamos que si  $\ker f \subset H_1 < G_1$ , entonces  $H_1 = f^{-1}(f(H_1))$ . Para probar esto probamos la doble inclusión.  $H_1 \in f^{-1}(f(H_1))$  es evidente pues  $h \in H_1 \implies f(h) \in f(H_1)$ . Ahora probamos  $\ker f \subset H_1 \implies H \subset f^{-1}(f(H_1))$ .

$$\begin{aligned}
 \alpha \in f^{-1}(f(H_1)) &\iff f(\alpha) \in f^{-1}(f(H_1)) \\
 &\iff \exists h_1 \in f(H_1) \mid f(\alpha) \in f(H_1) \\
 &\iff \exists h_1 \in H \mid f(\alpha)(f(h_1))^{-1} = e_2 \\
 &\iff \exists h_1 \in H_1 \mid f(\alpha h_1^{-1}) = e_2 \\
 &\iff \exists h_1 \in H_1 \mid \alpha h_1^{-1} \in \ker f \\
 &\iff \alpha h_1^{-1} h_1 \implies \alpha \in H_1
 \end{aligned}$$

♣



**Ejemplo 8.** Queremos saber sobre los subgrupos que tiene  $\mathbb{Z}/8\mathbb{Z}$  (ver figura ??). El epimorfismo que utilizamos es  $f : \mathbb{Z} \rightarrow \mathbb{Z}/8\mathbb{Z}, z \mapsto f(z) = \bar{z}$  el habitual.

Para ver los subgrupos de  $\mathbb{Z}/8\mathbb{Z}$  miramos qué subgrupos de  $\mathbb{Z}$  contienen a  $\ker f = \{z \in \mathbb{Z} \mid f(z) = \bar{0}\} = \{z \in \mathbb{Z} \mid z \bmod 8 = 0\} = 8\mathbb{Z}$ . Es decir, tenemos que encontrar los subgrupos de  $\mathbb{Z}$  que contengan a los múltiplos de 8 ( $8\mathbb{Z}$ ):

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z}$$

En general, en  $n\mathbb{Z}$ , los subgrupos que contienen al núcleo son los  $m\mathbb{Z}$  tales que  $m \mid n$  ( $m$  divide a  $n$ ). Luego  $\mathbb{Z}/8\mathbb{Z}$  tendrá 4 subgrupos que serán  $f(8\mathbb{Z}) = \mathbb{Z}/8\mathbb{Z}$ ,  $f(4\mathbb{Z}) = \mathbb{Z}/4\mathbb{Z}$ ,  $f(2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ ,  $f(\mathbb{Z}) = \{e\}$ .

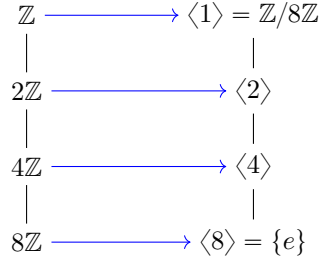


Figura 2.3: Retículo de subgrupos de  $\mathbb{Z}/8\mathbb{Z}$

Lo mismo podríamos hacer para obtener el retículo de  $\mathbb{Z}/6\mathbb{Z}$  (ver figura ??).

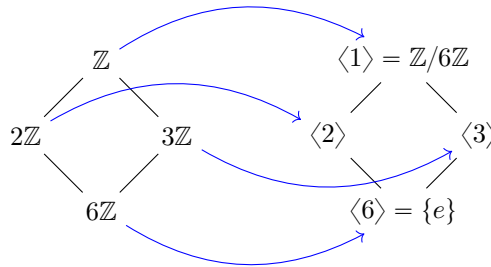


Figura 2.4: Retículo de subgrupos de  $\mathbb{Z}/6\mathbb{Z}$

**Teorema 22.** Todo subgrupo de  $\mathbb{Z}/n\mathbb{Z}$  es cíclico.

*Demostración.* La propiedad de cíclico se hereda de  $\mathbb{Z}$  y se prueba igual utilizando el algoritmo de la división. ♣

**Teorema 23.** Consideramos  $\mathbb{Z}/n\mathbb{Z}$ . Para cada divisor  $d$  de  $n$ , existe un único subgrupo cíclico de orden  $d$ .

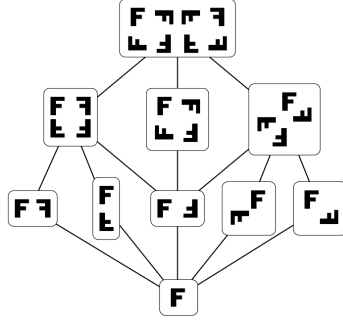
*Demostración.*  $d \mid n \implies n = dn' \implies n'\mathbb{Z} < n\mathbb{Z}$ . Además, por el teorema de prácticas,  $|n'\mathbb{Z}| = d$  y por tanto  $|f(n'\mathbb{Z})| = d$  donde  $f : n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  es la relación de equivalencia habitual. ♣

**Teorema 24.** Sean  $\bar{k}, \bar{k}' \in \mathbb{Z}/n\mathbb{Z}$ . Entonces  $o(\bar{k}) = o(\bar{k}') = d \implies \langle \bar{k} \rangle = \langle \bar{k}' \rangle$

**Ejemplo 9.** Dar el retículo de subgrupos de  $D_4 = \{1, B, B^2, B^3, A, AB, AB^2, AB^3\}$ , donde  $o(A) = 2$ ,  $o(B) = 4$ ,  $BA = AB^3$ . En este caso no tenemos más remedio que ir probando a ver qué combinaciones de elementos dan subgrupos. Como conocemos de dónde viene  $D_4$  nos es más fácil (ver el ejemplo 4).

Nos ayudamos de la imagen.

- Abajo tenemos el subgrupo trivial:  $\{1\}$
- En la primera fila tenemos, de izquierda a derecha:
  - $\{1, AB^2\}$
  - $\{1, A\}$
  - $\{1, B^2\}$
  - $\{1, AB^3\}$
  - $\{1, AB\}$

Figura 2.5: Retículo de subgrupos de  $D_4$  de [?]

- En la segunda fila tenemos los subgrupos de 4 elementos, de izquierda a derecha:
  - $\{1, B^2, A, AB^2\}$
  - $\{1, B, B^2, B^3\}$
  - $\{1, AB, B^2, AB^3\}$
- Y por último el grupo completo:  $D_4 = \{1, B, B^2, B^3, A, AB, AB^2, AB^3\}$ .

### 2.3. Teoremas random

**Teorema 25.** Sean  $n, m \in \mathbb{N}$ . El grupo producto directo  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  es cíclico  $\iff \text{mcd}(n, m) = 1$ .

*Demostración.* Para que  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  sea cíclico debe haber un elemento  $a \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \mid o(a) = m \cdot n$ . Si  $m$  y  $n$  no son coprimos entonces el orden de  $a$  no puede ser  $m \cdot n$ . ♣

**Ejemplo 10.** Sea  $G$  un grupo tal que  $|G| = 4$ . Afirmamos que

- o bien  $G \simeq \mathbb{Z}/4\mathbb{Z}$ ,
- o bien  $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

Ocurre lo siguiente

- si  $\exists a \in G \mid o(a) = 4$  entonces  $G$  es cíclico y por tanto isomorfo a  $\mathbb{Z}/4\mathbb{Z}$ .
- si no, entonces todos los elementos tienen orden menor o igual que 2.

#### 2.3.1. Centro de un grupo y sus propiedades

**Definición 19** (Centro de un grupo). Sea  $G$  un grupo finito. Definimos el centro de  $G$ ,  $Z(G) = \{a \in G \mid \forall g \in G, ag = ga\}$ .

El centro es útil en grupos finitos no abelianos.

**Proposición 14.** Sean  $a, b \in Z(G)$ . Entonces  $ab \in Z(G)$ .

*Demostración.* Tenemos que  $ag = ga$  y que  $bg = gb$ . Ahora tenemos que probar que  $g(ab) = (ab)g$ . Es trivial manipulando  $(ab)g = agb = gab$ . ♣

**Proposición 15.** Sea  $G$  un grupo.  $Z(G)$  es un subgrupo y además es un subgrupo normal.

*Demostración.*  $\forall g \in G, Z(G)g = \{ag \mid a \in G \wedge \forall b \in G, ab = ba\} = \{ga \mid a \in G \wedge \forall b \in G, ab = ba\} = gZ(G)$ . ♣

**Proposición 16.** Si  $H < Z(G)$  entonces  $H$  es abeliano y normal.

**Proposición 17.** Sea  $g \in G$ ,  $\phi_g : G \rightarrow G$  el isomorfismo definido por  $\phi_g(x) = gxg^{-1}$ . Entonces

$$\begin{aligned} x \in Z(G) &\iff \forall g \in G, gx = xg \iff gxg^{-1} = x \\ x \in Z(G) &\iff \forall g \in G, \phi_g(x) = x \end{aligned}$$

**Proposición 18.**  $G$  es abeliano  $\iff G = Z(G)$

Sea  $a \in G \wedge o(a) = n$ . Si  $a$  es el único elemento de orden  $n$  entonces  $n = 2 \wedge a \in Z(G)$ . Probamos primero que  $n = 2$ . Si  $a$  es el único elemento de orden  $n$  entonces tiene que ocurrir que  $a$  y  $a^{n-1}$  tienen el mismo orden por lo que  $1 = n - 1 \implies n = 2$ .

**Proposición 19.** Si  $G/Z(G)$  es cíclico de orden  $n$  entonces  $n = 1$ . Otra manera de formularlo: Si  $G/Z(G)$  es cíclico, entonces  $G = Z(G)$ . Otra manera más de formularlo: si  $G/Z(G)$  es cíclico entonces  $G$  es abeliano.

*Demostración.* Supongamos que  $G/Z(G) \simeq \mathbb{Z}/n\mathbb{Z}$ . Vamos a probar que  $n$  tiene que ser 1. Supongmos que  $G/Z(G) = \{\bar{\alpha}_i, i = 1, \dots, n\}$  donde  $\bar{\alpha}_i = \alpha^i Z(G)$ . Fijamos  $g \in G$  con  $g = \alpha^j h$ ,  $h \in Z(G)$ ,  $0 \leq j < n$  y fijamos  $f' \in G$  con  $g' = \alpha^{j'} h'$ ,  $h' \in Z(G)$ ,  $0 \leq j' < n$ . Entonces  $gg' = \alpha^j h \alpha^{j'} h' = \alpha^{j+j'} h h' = \alpha^{j'} h' \alpha^j h = g'g$  (podemos conmutar las  $h$  con cualquier elemento porque  $h \in Z(G)$ , por el contrario, los  $\alpha$  no necesitamos conmutarlos, solo agruparlos cuando están juntos). Es decir, que  $\forall g, g' \in G$  tenemos que  $gg' = g'g$  por lo que  $G$  es abeliano. ♣

**Ejemplo 11** (Hoja 1, ej 33). Sea  $G$  un grupo. Suponed que existe un único  $a \in G$  de orden 2. Demostrad que  $a \in Z(G)$ .

*Demostración.* Recordamos que  $a \in Z(G) \iff ga = ag, \forall g \in G$ . Definimos el isomorfismo de conjugación  $\phi_g(x) = gxg^{-1}$  para algún  $g$ . Como  $\phi_g$  es isomorfismo lleva elementos de orden  $n$  en elementos de orden  $n$ . Entonces  $\phi_g(a) = a$  ya que  $a$  es el único elemento de orden 2. Por tanto  $gag^{-1} = a \implies ga = ag \implies a \in Z(G)$ . ♣

## 2.4. Teoremas de la isomorfía (versión de clase)

**Teorema 26** (O ejemplo). Sea  $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ .  $f$  es un isomorfismo  $\iff f(\bar{1}) = \bar{a} \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$

**Ejemplo 12.** Sea  $g \in G$  fijado. Definimos  $\phi_g : G \rightarrow G$

$$\begin{array}{ccc} G & \xrightarrow{\phi_g} G & \xrightarrow{\phi_g^{-1}} G \\ x & \mapsto gxg^{-1} & \\ z & \mapsto & g^{-1}x(g^{-1})^{-1} \end{array}$$

Y  $\phi_g \cdot \phi_g^{-1} = Id$ .

*Demostración.* Para que  $f$  sea isomorfismo tiene que ser sobre luego  $o(\bar{a}) = n \implies \bar{a} \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ . ♣

**Teorema 27.** Sea  $f : G_1 \rightarrow G_2$  un homomorfismo de grupos,  $H \triangleleft G_1$  con  $H \subset \ker f$ . Sea  $\pi : G_1 \rightarrow G_1/H$  el homomorfismo que genera las clases de equivalencia (ver figura 2.9). Entonces se cumple lo siguiente

1. existe un homomorfismo de grupos  $\bar{f} : G_1/H \rightarrow G_2$  tal que  $\bar{f} \circ \pi = f$
2.  $\ker \bar{f} = \ker f/H$

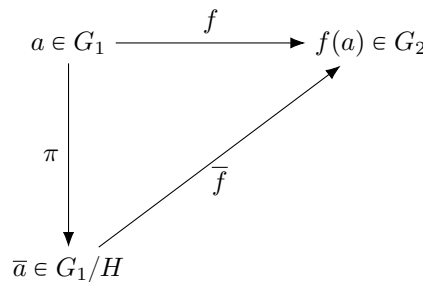


Figura 2.6: Homomorfismos que intervienen en el teorema 27

*Demostración.*

1. Probaremos que si construimos  $\bar{f}$  con  $\bar{f}(\bar{a}) = f(a)$  entonces  $\bar{f}$  está bien definida. Tenemos que ver que  $\bar{a} = \bar{a'} \implies f(a) = f(a')$ . Partimos de  $\bar{a} = \bar{a'} \implies a(a')^{-1} \in H \implies f(a(a')^{-1}) = e_2 \implies f(a)f(a')^{-1} = e_2 \implies f(a) = f(a')$ .
2. Observemos que  $\bar{f}(\bar{a}\bar{b}) = \bar{f}(\overline{ab}) = f(ab) = f(a)f(b) = \bar{f}(\bar{a})\bar{f}(\bar{b})$ . Ahora probamos las dos inclusiones a la vez  $\bar{a} \in \ker \bar{f} \iff \bar{f}(\bar{a}) = e_2 \iff f(a) = e_2 \iff a \in \ker f$ .

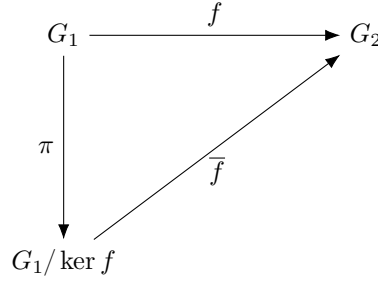


Figura 2.7: Primer teorema de la isomorfía.

**Teorema 28** (Primer de la isomorfía). Sea  $f : G_1 \rightarrow G_2$  un epimorfismo. Existe un isomorfismo  $\bar{f} : G_1/\ker f \rightarrow G_2$ .

*Demostración.*  $f = \pi \circ \bar{f}$  y  $f$  es sobre, luego  $\bar{f}$  también es sobreyectiva. ♣

**Teorema 29** (Segundo teorema de la isomorfía). Sean  $H \triangleleft G$ ,  $K \triangleleft G$  y  $H \subset K$  Entonces

$$(G/H)/(K/H) = G/K \quad (2.2)$$

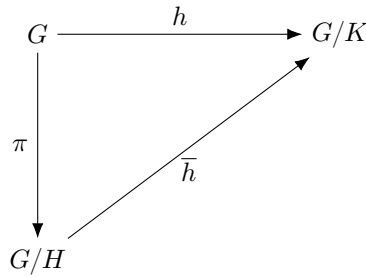


Figura 2.8: Segundo teorema de la isomorfía.

*Demostración.*  $\bar{h}$  es sobreyectiva y  $\ker \bar{h} = K/H$  ♣

**Teorema 30.** Sea  $f : G_1 \rightarrow G_2$  un epimorfismo. Si  $N \triangleleft G_1$ , entonces  $f(N) \triangleleft G_2$ . Como  $f$  es epimorfismo cualquier  $g \in G_2$ ,  $g_2 = f(g_1)$  para algún  $g_1 \in G_1$ . Como  $N \triangleleft G_1$ , tenemos que  $gNg^{-1} \in N$ . Que  $f(N) \triangleleft G_2$  quiere decir que  $\forall f(g) \in G_2, f(g)f(N)f(g^{-1}) \subset f(N)$ . Ahora bien  $f(g)f(N)f(g^{-1}) \subset f(N)$ . Y esto sigue pero lo ha dicho y no lo ha escrito y no me ha dado tiempo.

**Lema.** Sea  $h : G_1 \rightarrow G_2$  homomorfismo de grupos. Sean  $N \triangleleft G_1$  y  $N \subset \ker h$ .

1. Entonces existe un homomorfismo de grupos  $\bar{f} : G_1/N \rightarrow G_2$  que cumple  $\bar{f} \circ \pi = f$
2.  $\ker \bar{f} = \ker f/N$ .

**Corolario.** Si  $N = \ker f$  entonces  $\ker \bar{f} = \{0\}$  y  $\bar{f}$  es un monomorfismo.

**Corolario.** Si  $f$  es además un epimorfismo, entonces  $\bar{f}$  es una biyección.

*Demostración.* Consideramos  $f : H \rightarrow HK$  que es un homomorfismo porque  $H < HK$  (porque  $h = he_k$ ,  $\forall h \in H$  y satisface la definición de producto). Y ahora consideramos un epimorfismo  $h : HK \rightarrow HK/K$  que existe porque  $K \triangleleft HK$ . Sea  $\pi = f \circ g$ . Afirmamos que  $\ker \pi = H \cap K$ . Faltan cosas.

$$H/(H \cap K) \simeq HK/K$$

**Corolario.** Si  $H, K < G$  con  $K \triangleleft G$  entonces existe un epimorfismo  $\pi : H \rightarrow HK/K$  y  $\ker \pi = H \cap K$ . ♣

**Teorema 31.** <sup>a</sup> Sea  $f : G_1 \rightarrow G_2$  un homomorfismo de grupos. Entonces  $\text{Im } f \simeq G_1 / \ker f$ .

<sup>a</sup>Esta vez sí que dijo teorema.

Este teorema viene a decir que dado un homomorfismo  $f : G_1 \rightarrow G_2$ , si lo restringimos a  $f : G_1 \rightarrow \text{Im } f$  obtenemos un epimorfismo.

**Proposición 20.** Sea  $G$  un grupo con orden  $n$ . Sea  $H < G$  con índice de  $H = p \mid \text{mcd}(p, n) = 1$ . Entonces  $H$  es un subgrupo normal.

## 2.5. Teoremas de la isomorfía (versión con pies y cabeza)

**Teorema 32.** (Primer teorema de la isomorfía) Sea  $f : G_1 \rightarrow G_2$  un epimorfismo y sea  $\pi : G_1 \rightarrow G_1 / \ker f$ . Entonces existe un isomorfismo  $\bar{f} : G_1 / \ker f \rightarrow G_2$  tal que  $f = \pi \circ \bar{f}$ .

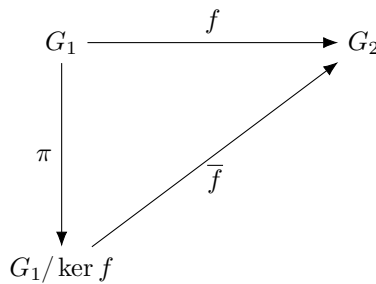


Figura 2.9: Primer teorema de la isomorfía.

**Teorema 33.** (Segundo teorema de la isomorfía) Sea  $G$  un grupo,  $H \triangleleft G$ ,  $K \triangleleft G$  y  $H < K$ . Entonces  $K/H$  es un subgrupo normal de  $G/H$  y

$$G/H / K/H \simeq G/K \quad (2.3)$$

**Teorema 34** (Tercer teorema de la isomorfía). Sea  $G$  un grupo,  $H < G$ ,  $K \triangleleft G$ . Entonces  $HK < G$ ,  $K \triangleleft HK$  y  $H \cap K \triangleleft H$ . Además,

$$HK/K \simeq H/(H \cap K) \quad (2.4)$$

## 2.6. Construcción de homomorfismos de grupos y de isomorfismos

Sea  $G$  abeliano con  $|G| = n = rs$ , sea  $H < G$ ,  $K < G$  con  $|H| = r$ ,  $|K| = s$  y  $H \cap K = \{e\}$ .

- Notemos que como  $G$  es abeliano,  $H$  y  $K$  son subgrupos normales.
- Al aplicar el teorema 17 tenemos que el denominador es  $|H \cap K| = 1$  por lo que  $|HK| = |H||K| = rs = n$ .
- Como  $G$  es abeliano:
  1.  $G = HK$  (porque  $HK$  es un subgrupo con el mismo número de elementos que  $G$  por el teorema 17)
  2. La función  $f : H \times K \rightarrow G$ ,  $(h, k) \mapsto hk$  es un homomorfismo de grupos (nótese que esto no ocurriría si  $G$  no fuese abeliano).

Es más, si se cumple todo lo anterior,  $f$  es además un isomorfismo  $\implies H \times K \simeq G$ .

**Ejemplo 13** (Homomorfismo trivial). Siempre nos queda el homomorfismo trivial  $f : G_1 \rightarrow G_2$ ,  $f(g_1) = e_2, \forall g_1 \in G_1$ .

**Ejemplo 14.** Consideramos  $S_3$ , que tiene  $|S_3| = 6$  y no es abeliano y los subgrupos  $H = \langle (12) \rangle$  y  $K = \langle (123) \rangle$  con  $|H| = 2$  y  $|K| = 3$ . Podemos construir la función  $f : H \times K \rightarrow S_3$  pero no es un homomorfismo de grupos. De hecho, al ser  $K \triangleleft S_3$ , el producto  $HK$  es un subgrupo y la función  $f$  es una biyección, pero aún así no es compatible con la estructura de grupo.

**Ejemplo 15.** Consideramos  $D_4$  y un grupo  $G$  con  $a, b \in G$  donde hemos establecido un homomorfismo que definimos con  $f(A) = a$  y  $f(B) = b$ . Ocurre lo siguiente

- El homomorfismo queda totalmente definido ya que todos los elementos de  $D_4$  son palabras en  $A$  y  $B$  y por la estructura de homomorfismo podemos operar tras aplicar la operación a cada letra. Por ejemplo  $f(ABA) = aba$ .
- Es necesario que  $o(a) = 2$  y  $o(b) = 4$ , de lo contrario no se cumpliría la estructura de homomorfismo entre  $D_4$  y  $G$ .

**Ejemplo 16.** Consideramos  $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}$  La presentación de este grupo es  $o(1) = n$ . Queremos construir un homomorfismo  $f : \mathbb{Z}/n\mathbb{Z} \rightarrow G'$ . Para que  $f$  sea un homomorfismo necesitamos que  $f(0) = e$ . Ahora supongamos que establecemos  $f(1) = a$ . Naturalmente sigue (para que  $f$  sea un homomorfismo) que  $f(2) = a * a = a^2$ . Observamos que la condición necesaria y suficiente para que el homomorfismo definido por  $f(1) = a$  es que  $a^n = e$ , o lo que es lo mismo que  $o(a)$  divida a  $n$ .

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\rightarrow G' \\ 0 &\mapsto e \\ 1 &\mapsto a \\ 2 &\mapsto a^2 \\ &\dots \\ n = 0 &\mapsto a^n = e \end{aligned}$$

**Ejemplo 17.** En  $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  podemos construir  $n$  homomorfismo ya que

- cualquier  $a \in \mathbb{Z}/n\mathbb{Z}$  cumple la condición necesaria para que  $f(1) = a$  induzca un homomorfismo
- todo homomorfismo queda determinado por  $f(1) = a$  para algún  $a \in \mathbb{Z}/n\mathbb{Z}$ .

Es decir que  $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}$ .

**Ejemplo 18.** Si ahora nos preguntamos por los isomorfismos  $\text{Isom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \subset \text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$  nos damos cuenta de que los únicos  $a \in \mathbb{Z}/n\mathbb{Z}$  que nos dan isomorfismos son aquellos que tienen  $o(a) = n$ .

Es decir que  $\text{Isom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ .

**Ejemplo 19** (Isomorfismo conjugación). Fijamos  $g \in G$  y definimos  $\phi_g : G \rightarrow G$ ,  $x \mapsto gxg^{-1}$ . Es un homomorfismo de grupos pues  $y \mapsto gyg^{-1}$  y  $xy \mapsto gxyg^{-1} = gxg^{-1}gyg^{-1}$ .

Ahora consideramos  $g^{-1}$  y  $\phi_{g^{-1}} : G \rightarrow G$ ,  $x \mapsto g^{-1}xg$  y como antes se verifica que es homomorfismo.

Además,  $\phi_g \circ \phi_{g^{-1}} = \text{id}$  luego  $\phi_g$  es un isomorfismo de grupos.

**Ejemplo 20.** Consideramos ahora  $N \triangleleft G$  y por tanto para cualquier  $g \in G$ ,  $gN = Ng$ . La función  $\phi_g(N) \subset N$  es un isomorfismo que además lleva los elementos de  $N$  en  $N$ , por tanto podemos restringirla a  $\phi_g : N \rightarrow N$  e inducir un isomorfismo.

Es decir, los subgrupos que no se mueven por ninguna función  $\phi_g$  son los subgrupos normales.

**Ejemplo 21.** Consideramos el grupo  $(\mathbb{Z}, +)$  que es cíclico y un grupo  $G$  con  $a \in G$ . Utilizando notación multiplicativa en la que el  $1$  representa el elemento neutro (en este caso  $1 = 0$ )

$$\begin{aligned} \mathbb{Z} &\rightarrow G \\ 1 &\mapsto a \\ k &\mapsto a^k \\ k + k' &\mapsto a^{k+k'} \end{aligned}$$

Es decir, que al seleccionar  $1 \mapsto a$  queda determinada la imagen de todos los demás  $k \in \mathbb{Z}$  y además la función que obtenemos es un homomorfismo. Por tanto el conjunto de los homomorfismos de  $\mathbb{Z}$  en  $G$  es TODO  $G$ :  $\text{Hom}(\mathbb{Z}, G) = G$ .

**Ejemplo 22** (del primer teorema de la isomorfía). Consideramos el grupo  $G = \{1, i, -1, -i\}$  con el producto y establecemos la función  $f : \mathbb{Z} \rightarrow G$  que lleva  $1 \mapsto i$ . Además  $f$  es sobreyectiva y  $\ker f = 4\mathbb{Z}$ . El primer teorema de la isomorfía nos dice que existe un isomorfismo  $\bar{f} : \mathbb{Z}/\ker f \rightarrow G$  y este es  $\bar{f}$ ,  $\bar{f}([a]) \mapsto i^a$  (en  $\ker f$  no se repiten los elementos por lo que convertimos el epimorfismo  $f$  en un homomorfismo  $\bar{f}$ ).

En general todos los grupos cíclicos de orden  $n$  son isomorfos entre sí, porque todos son isomorfos a  $\mathbb{Z}/n\mathbb{Z}$  y los isomorfismos son reversibles y la composición sigue siendo isomorfismo.

Hemos visto que  $\text{Hom}(\mathbb{Z}, G) = G$  porque al determinar  $f(1) = a$  determinamos el homomorfismo y por tanto tenemos un homomorfismo para cada elemento  $a \in G$ .

¿Pero qué pasa si tomamos los homomorfismos  $f : \mathbb{Z}/n\mathbb{Z} \rightarrow G$  con  $a \in G$  definidos por  $f(\bar{1}) = a$ ? Pasa que para que sean homomorfismos necesitamos que  $o(a) = o(1) = n$  para que así  $\bar{0} = \bar{n} \mapsto a^n = e$ .



**Ejemplo 23.** Veamos un ejemplo (notamos que  $(12)^4 = id$ )

$$\begin{aligned} f : \mathbb{Z}/4\mathbb{Z} &\rightarrow S_3 \\ \bar{1} &\mapsto (12) \\ \bar{2} &\mapsto id = (1) \\ \bar{3} &\mapsto (12) \\ \bar{4} = \bar{0} &\mapsto id \end{aligned}$$

Observamos que  $\text{Hom}(\mathbb{Z}/4\mathbb{Z}, S_3) \subset \text{Hom}(\mathbb{Z}, S_3)$  puesto que al tomar  $\mathbb{Z}/4\mathbb{Z}$  no podemos tomar cualquier  $a$  sino que tenemos que asegurarnos de que  $o(a) = o(1)$  (en este caso  $o(a) = 2$  pero sigue funcionando porque lo que importa es que  $a^{o(1)} = id$ ).

Queremos analizar los homomorfismos  $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ . Ahora no importa el  $\bar{a}$  que elijamos para que  $f$  sea homomorfismo porque  $\text{Im} f = \langle \bar{a} \rangle$ .

Para que  $f$  sea epimorfismo, necesitamos que  $\text{Im} f = \langle \bar{a} \rangle = \mathbb{Z}/n\mathbb{Z}$  es decir que  $o(a)$  sea coprimo con  $n$ .

Concluimos que  $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \subset \text{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ .



## Capítulo 3

# Locuras varias que no sé donde van

Lo que hemos dado en octubre básicamente.

**Teorema 35.** Si  $G$  es abeliano y  $|G| < \infty$  entonces  $G$  es un producto de grupos cíclicos finitos.

*Demostración.* Dice que no lo vamos a probar, pero veremos algunos resultados. ♣

Vamos a aplicar el teorema 35 a grupos abelianos.

**Teorema 36.** Sea  $G$  abeliano con  $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ . Entonces

$$G \simeq \mathbb{Z}/p_1^{\beta_{11}}\mathbb{Z} \times \mathbb{Z}/p_1^{\beta_{1s_1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_n^{\beta_{ns_1}}\mathbb{Z} \times \mathbb{Z}/p_n^{\beta_{ns_n}}\mathbb{Z} \text{ donde } \alpha_i = \sum_{j=1 \dots s_i} \beta_{ij} \quad (3.1)$$

En particular, se cumple que para grupos cíclicos  $G$  de orden  $n$ , donde  $G \simeq \mathbb{Z}/n\mathbb{Z}$ .

**Teorema 37.** Sea un número y su factorización en primos:  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ . Entonces

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \times \dots \times \mathbb{Z}/p_n^{\alpha_n}\mathbb{Z} \quad (3.2)$$

*Demostración.* Sea  $d$  tal que  $d \mid n$  y  $n = dn'$ . Por tanto  $n' = p_2^{\alpha_2} \dots p_n^{\alpha_n}$  y  $d = p_1^{\alpha_1}$ . Como  $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n', \dots, n-1\}$  tenemos que  $o(n') = p_1^{\alpha_1}$ . Luego  $H = \langle n' \rangle$  es el único subgrupo de orden  $p_1^{\alpha_1}$  y  $N = \langle p_1^{\alpha_1} \rangle$  es el único subgrupo de orden  $n'$ . Ahora bien, por cómo hemos elegido  $n'$  y  $d$ ,  $\text{mcd}(n', d) = 1$  por lo que  $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$ . Podemos repetir este procedimiento hasta que descompongamos  $n$  en potencias de primos y tendremos que  $\text{mcd}(p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_n^{\alpha_n}) = 1$  y por tanto  $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \times \dots \times \mathbb{Z}/p_n^{\alpha_n}\mathbb{Z}$  ♣

**Teorema 38.** Sea  $G$  abeliano donde  $|G| = r \cdot s$  con  $\text{mcd}(r, s) = 1$  y ean  $K < G \wedge N < G$  donde  $|K| = r \wedge |N| = s$ . Entonces  $G \simeq K \times N$ .

*Demostración.* Sabemos que  $f : K \times N \rightarrow G$ ,  $(k, h) \mapsto kh$  es un homomorfismo y por tanto  $\text{Im} f < G$ . Para probar que  $f$  es un isomorfismo probaremos que  $\text{Im} f = G$ . Como  $|K| = r \wedge |N| = s$  y  $r$  y  $s$  son coprimos entonces  $K \cap N = \{e\}$ . Por tanto  $|K \cap N| = 1$  y utilizando el teorema 17 tenemos que  $|KN| = \frac{|K||N|}{|K \cap N|} = |K||N| = rs$  por lo que  $f$  es sobreyectiva, y, por tanto, biyectiva, es decir, que  $f$  es un isomorfismo. ♣

**Ejemplo 24.** Podemos afirmar que si  $|G| = 6$  y  $G$  es abeliano entonces  $G \simeq \mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ .

Observemos que la hipótesis de abeliano es fundamental (ver ejemplo 14).

Sea  $|G| = p^2q$  con  $p, q$  primos distintos. Entonces o bien  $G \simeq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$  o bien  $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ .

### 3.1. Clasificación de grupos finitos

Grupos notables de distintos órdenes finitos

- $|G| = 3, 5, 7, 11, \dots, p$  donde  $p$  es primo:
  - Abelianos cíclicos: son isomorfos con  $\mathbb{Z}/p\mathbb{Z}$ .

- Abelianos no cíclicos: no hay, por el corolario del teorema de Lagrange 11.
- $|G| = 4$ :
  - Abelianos cíclicos: son isomorfos con  $\mathbb{Z}/4\mathbb{Z}$
  - Abelianos no cíclicos: son isomorfos con  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .
  - No abelianos: no hay.
- $|G| = 6$ :
  - Abelianos cíclicos: son isomorfos con  $\mathbb{Z}/6\mathbb{Z}$ .
  - Abelianos no cíclicos: no hay porque todo grupo abeliano cuyo orden se puede descomponer en dos primos es cíclico (ver Hoja 1 ejercicio 19).
  - No abelianos: todos son isomorfos con  $D_3 \simeq S_3$  (ver ejemplo 25).
- $|G| = 8$ :
  - Abelianos cíclicos: son isomorfos con  $\mathbb{Z}/8\mathbb{Z}$ .
  - Abelianos no cíclicos: son isomorfos o bien con  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  o bien con  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  (depende de los órdenes de los elementos de  $G$ ).
  - No abelianos: son isomorfos o bien con el famoso grupo  $D_4$  (ver ejemplo 4) o bien con el grupo de cuaterniones  $H$  (ver ejemplo 3). Ver ejemplo 26

**Ejemplo 25.** Sea  $G$  no abeliano con  $|G| = 6$ . Entonces  $G \simeq D_3$ .

*Demostración.* 1.  $G$  no abeliano  $\implies G$  no cíclico  $\implies \exists g \in G \mid o(g) \neq 6$

2.  $G$  no abeliano  $\implies \exists b \in G \mid o(b) \neq 2 \implies o(b) = 3$  ya que si  $b \in G$  entonces  $o(b) \mid |G|$  (corolario teorema de Lagrange (11)).

3. Sabemos pues que  $\langle b \rangle = \{1, b, b^2\} < G$  y  $|\langle b \rangle| = 3 \implies [G : \langle b \rangle] = \frac{|G|}{|\langle b \rangle|} = 2$ . Es decir, que hay otra caja disjunta en la partición a la que llamamos  $K$

4. Por el teorema del cardinal del producto libre (teorema 17) tenemos que  $6 \geq |HK| = \frac{|H||K|}{|\langle b \rangle \cap K|}$ . Como  $\langle b \rangle \cap K = \{e\}$  por ser las cajas disjuntas tenemos que  $|K| = 2$  ya que si fuera  $|K| = 3$  tendríamos que  $|HK| = 9 \not\leq 6$ .

5. Definimos  $\phi_a(x) : G \rightarrow G, x \mapsto axa^{-1}$  (el isomorfismo de conjugación).  $\phi_a$  es un isomorfismo, incluso cuando lo restringimos a un subgrupo normal. El subgrupo  $\langle b \rangle$  es normal porque tiene índice 2 (ver teorema 12).

6. Por ello tenemos que si  $\phi_a(x) = y$  entonces tiene que ser  $o(x) = y$ . Por tanto, aplicando  $\phi_a$  a  $b$  tenemos lo siguiente:

$$\begin{aligned}\phi_a(b) &= aba^{-1} = b \implies ab = ba \implies G \text{ abeliano} \\ \phi_a(b) &= aba^{-1} = b^{-1} \implies ab = b^2a \implies ba = ab^2\end{aligned}$$

7. La primera no puede ser por hipótesis. La segunda nos da el final de la presentación de  $D_3$ :

$$D_3 = \langle a, b \rangle \text{ donde } o(a) = 2, o(b) = 3, ba = ab^2$$



**Ejemplo 26** (de aplicación de muchos teoremas). Probar que si  $G$  es un grupo no abeliano entonces o bien  $G \simeq D_4$  o bien  $G \simeq H$  donde  $H$  es el grupo de cuaterniones (ver ejemplo 3).

*Demostración.*

1. Tenemos que  $G$  no es abeliano. Por el contrarrecíproco del teorema 5 tenemos que no puede ser cíclico por lo que  $\nexists g \in G \mid o(g) = 8$ .
2. Por el teorema 2 sabemos que  $\exists b \in G \mid o(b) \neq 2 \implies o(b) = 4$ .
3. Por el teorema de Lagrange 11 sabemos que dicho  $b$  tiene que tener  $o(b) = 4$  ya que  $\forall b \in G, o(b) \mid |G|$ . Por tanto  $\langle b \rangle = \{1, b, b^2, b^3\}$ .
4. Como  $\langle b \rangle$  tiene orden 4, el índice es  $[G : \langle b \rangle] = 2$  por lo que hay otro subgrupo en  $G$  disjunto a  $\langle b \rangle$ . Sea  $a$  un elemento de dicho subgrupo.

5. Fijado  $a$ , definimos el isomorfismo de conjugación  $\phi_a : G \rightarrow G$ ,  $\phi_a(x) = axa^{-1}$ . Este isomorfismo sigue siendo un isomorfismo cuando lo restringimos a un subgrupo normal como es el caso de  $\langle b \rangle$  (ver teorema 12).
6. Para  $b \in G$  pueden ocurrir las siguientes, porque  $\phi_a$  debe mantener los órdenes por ser isomorfismo:
- $\phi_a(b) = aba^{-1} = b \implies ab = ba \implies G$  abeliano. Descartamos esta opción por hipótesis.
  - $\phi_a(b) = aba^{-1} = b^{-1} \implies ba = ab^{-1} = ab^3$
7. Ahora consideramos los posibles órdenes de  $a$  que pueden ser 2 o 4 por el teorema de Lagrange:
- Si  $o(a) = 2$  entonces  $G \simeq D_4$  ♣
  - Si  $o(a) = 4$  entonces  $\langle a \rangle = \{1, a, a^2, a^3\}$ .
    - a) Miramos  $\langle a \rangle \cap \langle b \rangle = \{1, a, a^2, a^3\} \cap \{1, b, b^2, b^3\} = \{1\} \implies |\langle a \rangle \cap \langle b \rangle| = 1$
    - b) Por el teorema del orden del producto libre 17 tenemos que  $|\langle a \rangle \langle b \rangle| = |\langle a \rangle| |\langle b \rangle| = 4 \cdot 4 = 16$ , pero esto no puede ocurrir puesto que el orden del producto puede ser como máximo 8. Es decir, que  $\langle a \rangle \cap \langle b \rangle \neq \{e\}$ .
    - c) Ahora bien, la intersección de subgrupos debe ser un subgrupo, luego el orden debe ser divisor del orden de los grupos intersecados. El orden de  $\langle a \rangle \cap \langle b \rangle$  puede ser 1, 2 o 4.
    - d) Ya hemos visto que no puede ser 1. Tampoco puede ser 4 porque... por qué? Luego  $o(\langle a \rangle \cap \langle b \rangle) = 2$  por lo que  $\langle a \rangle \cap \langle b \rangle$  tiene 2 elementos.
    - e) Uno de ellos es el neutro (1). El otro no puede ser ni  $a$ , ni  $b$  porque al tener estos orden 4 tendría que haber más elementos. Tampoco puede ser ni  $a^3$ , ni  $b^3$  porque también tienen orden 4 por el teorema 6. Luego  $\langle a \rangle \cap \langle b \rangle = \{1, a^2\} = \{1, b^2\} \implies a^2 = b^2$ .
    - f) Recopilando  $o(a) = 4$ ,  $o(b) = 4$ ,  $a^2 = b^2$ ,  $ba = ab^{-1}$  tenemos que  $G \simeq H$  ♣

## 3.2. Otras cosas

**Definición 20** (Grupo de automorfismos). Sea  $G$  un grupo. Llamamos grupo de automorfismos al grupo

$$\text{Aut}(G) = \{f \mid f : G \rightarrow G \text{ isomorfismo}\} \quad (3.3)$$

**Proposición 21.** La función  $\gamma : G \rightarrow \text{Aut}(G)$  definida con  $\gamma(g) \mapsto \gamma_g$ , donde  $\gamma_g : G \rightarrow G$ ,  $\gamma_g(x) = gxg^{-1}$ , es un homomorfismo.

*Demostración.* Verifica la definición: para  $g, g' \in G$  ♣

**Definición 21** (Elementos conjugados). Sean  $a, b \in G$ . Decimos que  $a$  y  $b$  son conjugados  $\iff \exists g \in G \mid \gamma_g(a) = b$ .

**Nota:** La relación de conjugación solo merece la pena en grupos no abelianos, porque en un grupo abeliano, cualquier par de elementos es conjugado.

**Ejemplo 27.** En  $S_3$  afirmamos lo siguiente:

- que 1 solo tiene como conjugado a sí mismo,
- que  $\{(12), (13), (23)\}$  son conjugados entre sí,
- y que  $\{(123), (132)\}$  también son conjugados entre sí.

Es decir, que la conjugación nos genera una partición con 3 cajas disjuntas.

**Proposición 22.** La relación de conjugación es una relación de equivalencia  $aRb \iff a$  y  $b$  son conjugados.

*Demostración.* Comprobamos que  $R$  es una relación de equivalencia:

1. Reflexiva:  $\forall a \in R$ ,  $aRa$ : tomamos  $g = e$  y automáticamente tenemos que  $eae^{-1} = a$ .
2. Simétrica:  $\forall a, b \in R$ ,  $aRb \implies bRa$ :  $\exists g, gag^{-1} = b$ . Tomamos  $\gamma_{g^{-1}}$  y tenemos que  $\gamma_{g^{-1}}(b) = a \implies bRa$ .
3. Transitiva:  $\forall a, b, c \in G$ ,  $aRb \wedge bRc \implies aRc$ . Por hipótesis tenemos que  $\exists g \in G \mid \gamma_g(a) = b \wedge \exists g' \in G \mid \gamma_{g'}(b) = c$ . Por tanto  $\gamma_{gg'}(a) = (\gamma_{g'}\gamma_g)(a) = \gamma_{g'}(b) = c$ .

♣

En esta relación de equivalencia, las clases de equivalencia son de la forma  $\bar{a} = \{gag^{-1} \mid g \in G\}$  (conjuntos de los elementos que son conjugados de  $a$ ). Queremos saber cuántos elementos hay en cada clase de equivalencia.

Fijamos  $a \in G$  y definimos

**Definición 22** (Centralizador de un elemento). Sea  $a \in G$ . Llamamos centralizador de  $a$  al conjunto

$$C(a) = \{g \in G \mid \gamma_g(a) = gag^{-1} = a\} \quad (3.4)$$

Se tiene que  $\forall a \in G$ ,  $e \in C(a)$ , es decir que  $C(a)$  no es vacío.

**Proposición 23.**  $C(a)$  es un subgrupo de  $G$

*Demostración.* Por el teorema 9 solo necesitamos probar la clausura, es decir, tenemos que probar que  $\forall g, g' \in G$ ,  $g \in C(a) \wedge g' \in C(a) \implies gg' \in C(a)$ . Sale solo  $(gg')agg'^{-1} = gg'a(g')^{-1}g^{-1} = gag^{-1} = a \in C(a)$ . ♣

**Proposición 24.**  $|\{gag^{-1} \mid g \in G\}| = [G : C(a)] = r$  (el número de elementos de una clase de equivalencia es el índice de un representante)

*Demostración.* Fijamos  $a \in G$  y definimos  $H = C(a) = \{g \in G \mid gag^{-1} = a\}$ . ♣

### 3.3. Teorema de Cauchy

**Teorema 39** (de Cauchy). Sea  $G$  un grupo finito con  $|G| = n$ . Si  $p$  es primo y  $p \mid n$  entonces  $G$  contiene un elemento de orden  $p$ .

*Demostración.* Procedemos por casos:

- Si  $G$  es abeliano. Descomponemos  $|G| = n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ . Por el teorema 35,  $G \simeq \mathbb{Z}/p_1^{\beta_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\beta_2}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{\beta_s}\mathbb{Z}$  donde cada  $\alpha_i$  es la suma de algunos  $\beta_r$ . ♣
- Si  $G$  no es abeliano. Particionamos  $G$  con la relación de equivalencia dada anteriormente (definición 21),  $aRb \iff \exists g \in G \mid gag^{-1} = b$ . Recordemos que cada clase de equivalencia es de la forma  $\bar{c} = \{gag^{-1} \mid g \in G\}$ . Observamos que si partimos de  $e$ , el elemento neutro,  $eRb \implies \exists g \mid geg^{-1} = b$  pero  $\forall g \in G$ ,  $geg^{-1} = e$  por lo que  $\bar{e}$  tiene un único elemento.

Tomemos ahora una clase de equivalencia, la que contenga a  $a \in G$ . La clase es  $\bar{a} = \{gag^{-1} \mid g \in G\}$ . Es claro que  $a \in \bar{a}$  por la propiedad reflexiva de  $R$ , luego por lo menos en  $\bar{a}$  tiene un elemento.

$$\begin{aligned} \bar{a} = \{gag^{-1} \mid g \in G\} = \{a\} &\iff gag^{-1} = a, \forall g \in G \\ &\iff ga = ag, \forall g \in G \end{aligned}$$

$$\begin{aligned} |\bar{a}| = 1 &\iff \bar{a} = 1 \\ &\iff a \in Z(G) \end{aligned}$$

Supongamos que la partición está dada por subconjuntos  $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_s$ . Por ser una partición, cualquier elemento vive en una sola caja, luego para saber cuantos elementos tiene  $G$  nos vale con sumar los elementos de cada caja:

$$|G| = \sum_{i=1}^s |\bar{a}_i| = \sum_{i=1}^s |\{ga_i g^{-1} \mid g \in G\}|$$


Ahora bien, por la proposición 24 tenemos que  $|\bar{a}_i| = [G : C(a_i)]$ . Por tanto decir que  $|\bar{a}_i| = 1 \implies [G : C(a_i)] = 1 \implies G = C(a_i)$ .

Ahora vamos a dividir el sumatorio en dos: por un lado las cajas de un solo elemento y luego las cajas de varios elementos:

$$|G| = |Z(G)| + \sum_{i=r+1}^s [G : C(a_i)] \text{ donde } |Z(G)| = r \text{ y } [G : C(a_i)] \geq 2, \forall i = r+1, \dots, s \quad (3.5)$$

Ahora para probar el teorema de Cauchy procedemos por inducción en  $n = |G| = [G : C(a_i)] \cdot |C(a_i)|$ .

1. Caso  $n = 1$ .  $G = \{e\}$  que es obvio.
2. Caso  $n \implies n+1$ . Pueden pasar dos cosas:
  - o bien  $p \mid |C(a_i)|$  para algún  $i = r+1, \dots, s$  entonces, por hipótesis inductiva,  $C(a_i)$  contiene algún elemento de orden  $p$ . Ahora bien,  $C(a_i) < G \implies G \implies$  el elemento también está en  $G$ . Podemos proceder por inducción y todo es genial ♣

- o bien  $p \nmid |C(a_i)|$ ,  $\forall i = r+1, \dots, s$ . No podemos proceder por inducción. En este caso  $[G : C(a_i)] \cdot |C(a_i)| = |G| \implies p \mid [G : C(a_i)]$ ,  $i = r+1, \dots, s$ . No  
Como  $|G| = |Z(G)| + \sum_{i=r+1}^s [G : C(a_i)]$  y por hipótesis  $p \mid |G| \wedge p \mid [G : C(a_i)]$ ,  $\forall i = r+1, \dots, s \implies p \mid |Z(G)| \implies |Z(G)|$  es múltiplo de  $p$ . Como  $Z(G)$  es abeliano,  $\exists \alpha \in Z(G) \mid o(\alpha) = p$ . Luego se reduce al caso abeliano y ya estaría 

**Ejemplo 28.** Sea  $G$  tal que  $|G| = pq$ . Entonces por el teorema de Cauchy  $\exists a, b \in G \mid o(a) = p \wedge o(b) = q$ . Como  $p$  y  $q$  son primos los ordenes de  $\langle a \rangle$  y  $\langle b \rangle$  son coprimos y por tanto  $\langle a \rangle \cap \langle b \rangle = \{e\}$ . Por el teorema del orden de conjunto<sup>1</sup> producto libre (17),  $|\langle a \rangle \langle b \rangle| = pq$ . Lo que si que sabemos es que  $G = \{a^i b^j \mid 0 \leq i < p-1 \wedge 0 \leq j < q-1\} = \langle a, b \rangle$ .

**Ejemplo 29.** Sea  $G$  tal que  $|G| = 2q$ . Análogamente al caso anterior llegamos a que  $o(a) = 2$ . Como  $\langle b \rangle$  tiene índice 2 entonces  $\langle b \rangle \triangleleft G$ . Esto nos permite saber como operar con las palabras  $a^i b^j$  una vez tenemos un isomorfismo que lleva  $aba^{-1} = b^j$  (tiene que ir a algún  $b^j$  porque por ser isomorfismo tiene que llevar elementos de orden  $q$  en elementos de orden  $q$ : los  $b \in \langle b \rangle$ )

Dada la relación de equivalencia de conjugación (definición 21), definimos  $C$  como el conjunto de los representantes de las clases de equivalencia. Entonces podemos decir

$$G = \bigcup_{c_i \in C} \{a \in G \mid a R c_i\}$$

Observemos que  $d \in Z(G) \iff \{a \in G \mid a R d\} = \{gdg^{-1} \mid g \in G\} = \{d\}$ . Y por tanto podemos escribir

$$C = Z(G) \cup (C \setminus Z(G))$$

que aunque parezca obvio quiere decir que  $C$  se puede expresar como la unión disjunta de las cajas que tienen solo un elemento que se corresponden con elementos que están en el centro y las cajas que tienen más de uno. Y por lo visto en la demostración del teorema de Cauchy tenemos que

$$|G| = \sum_{c_i \in C} |\bar{c}_i| = |Z(G)| + \sum_{i=r+1}^s [G : C(a_i)] \text{ donde } [G : C(a_i)] \geq 2$$

### 3.4. P-grupos

**Definición 23** (P-grupo). Sea  $p$  primo. Decimos que  $G$  es un p-grupo si  $|G| = p^r$ .

Nos interesan sobre todo los p-grupos no abelianos


**Teorema 40.** Si  $G$  es un p-grupo entonces  $Z(G)$  es no trivial (no es el vacío).

*Demostración.* Podemos escribir sin distinguir entre cajas de uno o varios elementos

$$|G| = |C(c_i)| | [G : C(c_i)] |$$


es decir que tenemos una factorización de  $|G| = p^r$  luego  $|C(c_i)|$  y  $| [G : C(c_i)] |$  son ambas potencias de  $p$ . Y aplicando esto a la expresión 3.5 tenemos que

$$\underbrace{|G|}_{\text{múltiplo de } p} = |Z(G)| + \sum_{i=r+1}^s \underbrace{[G : C(a_i)]}_{\text{múltiplo de } p} \text{ donde } [G : C(a_i)] \geq 2$$

por lo que  $|Z(G)|$  tiene que ser múltiplo  $p$  por lo que  $Z(G)$  no puede ser el trivial. 

**Ejemplo 30.** Tenemos que  $Z(D_4) = \{1, B^2\}$  y  $Z(H) = \{1, B^2\}$  donde  $H$  es el grupo de cuateriones (ejemplo 3) y  $D_4$  es el famoso grupo (ejemplo 4).

**Teorema 41.** Si  $p$  es primo y  $|G| = p^2$  entonces  $G$  es abeliano.

*Demostración.* Por el la demostración del teorema anterior tenemos que o bien  $|Z(G)| = p$  o bien  $|Z(G)| = p^2$ . Afirmamos que  $|Z(G)| \neq p$  ya que si fuera así  $|G/Z(G)| = p \implies G/Z(G)$  cíclico pero hemos probado (proposición 19) que  $G/Z(G)$  no puede ser cíclico. Por lo tanto  $|Z(G)| = p^2 \implies Z(G) = G \implies G$  es abeliano. 

<sup>1</sup>No sabemos si alguno es normal, luego no tenemos garantías de que el producto sea un grupo

Sea  $\sim$  una relación de equivalencia definida por  $a \sim b \iff \exists g \in G \mid gag^{-1} = b$  para  $a, b \in G$ . Esta relación da una partición de  $G$  en clases de la forma  $cl(a) = \{gag^{-1} \mid g \in G\}$ . En el caso abeliano esta relación es la de igualdad, por lo que no nos merece la pena liar este pifostio para saber que  $a \sim b \iff a = b$ .

Es muy importante saber cómo contamos los elementos de una clase, es decir, de cuantas formas podemos *mover* el elemento  $a$  con  $g \in G$ . Para ello definimos el centralizador (definición 22) como  $C(a) = \{h \in G \mid hah^{-1} = a\} < G$ . Queremos probar que  $|cl(a)| = [G : C(a)] = r$ .

Lo probamos tomando clases laterales a la izquierda (por ejemplo) y partiendo  $G$  en  $r$  cajas. Las cajas son de la forma  $\alpha_i C(a)$ ,  $i = 1, \dots, r$ . Esta partición no tiene que ver con la partición anterior. Observemos que para cualquier  $g \in \alpha_i C(a)$ ,  $g = \alpha_i h$ , tenemos que  $gag^{-1} = \alpha_i hah^{-1} \alpha_i^{-1} = \alpha_i a \alpha_i^{-1}$  es decir que los  $g \in C(a)$  no se mueven fuera de la caja. Es decir, que si  $\alpha_i \neq \alpha_j$  para  $i \neq j$  entonces hay  $r$  maneras de mover a  $g$  y por tanto  $|cl(a)| = r$ .

Probaremos que en efecto los  $\alpha_i$  son distintos.

Sean  $g_1, g_2 \in G$ .  $g_1 a g_1^{-1} = g_2 a g_2^{-1} \iff (g_2^{-1} g_1) a (g_1^{-1} g_2) = a \iff (g_2^{-1} g_1) a (g_2^{-1} g_1)^{-1} \iff C(a) g_2^{-1} g_1 \in C(a) \iff g_1 \in g_2 C(a)$ .

Si  $G/\sim$  tiene  $N$  elementos, tomamos  $\{c_1, \dots, c_N\}$  como el conjunto de los representantes, donde  $c_i$  es un representante de cada conjunto de la partición. Entonces podemos expresar

$$G = \bigcup_{c_i \in C} cl(c_i)$$

donde  $|cl(c_i)| = [G : C(c_i)]$ . Por tanto decir que  $|cl(c_i)| = 1$  es equivalente ( $\iff$ ) a decir que  $G = C(c_i) = \{\forall g \in G, g c g^{-1} = c\} \iff c \in Z(G)$ .

Afirmábamos que

$$|G| = \sum_{c_i \in C} |cl(c_i)| = |Z(G)| + \sum_{c_i \in C \setminus Z(G)} [G : C(c_i)]$$

descomponiendo la suma en las clases con solo un elemento y las clases con más de dos elementos.

**Ejemplo 31.** Consideramos  $D_3$  (ver ejemplo ??). Nos fijamos en que  $B \notin Z(D_3)$  es decir que en  $cl(B)$  hay más de un elemento. En particular por lo visto anteriormente  $|cl(B)| = [G : C(B)]$ . Ahora bien  $C(B) = \{1, B, B^2\}$  luego  $|cl(B)| = [G : C(B)] = 2$ . La pregunta es ¿quién es el compañero de  $B$  en su clase? Es fácil, recordamos que  $\phi_g(x) = g x g^{-1}$  (el isomorfismo conjugación) es un isomorfismo y que  $\{1, B, B^2\}$  es normal, por lo que  $o(B) = o(\phi_g(B)) = 2$ . Entonces  $\phi_g(B) \neq 1$  porque no coinciden los órdenes, de manera que  $\phi_g(B) = B^2$  por necesidad. Luego el otro elemento es el  $B^2$ .

¿Qué pasa con el elemento  $A$ ? Pues ocurre que  $A \in C(A)$  y  $\{1, A\} \in C(A)$ . me faltan cosaaaaasss

Para concluir queda que la relación  $\sim$  parte  $D_3$  en 3 cajas, a saber:

$$D_3 = \{\underbrace{1}, \underbrace{B, B^2}, \underbrace{A, AB, AB^2}\}$$

**Ejemplo 32.** El caso del famoso grupo  $D_4$  (ver ejemplo 4) es mucho más interesante porque  $Z(D_4)$  no es trivial. Elegimos por ejemplo el elemento  $B^2$ . Probar que  $\phi_g(B^2) = g B^2 g^{-1} = B^2$ ,  $\forall g \in D_4$  es complicado. Pero fijémonos en que  $\phi_B(B^2) = B B^2 B^{-1} = B^2$  y que  $\phi_A(B^2) = A B^2 A^{-1} = B^2$ . Entonces cualquier palabra en  $A$  y en  $B$  no mueve a  $B^2$ , por ejemplo  $AB(B^2)B^{-1}A^{-1} = B^2$ . Nos convencemos de que  $B^2 \in Z(D_4)$ . Con esto ya tenemos que  $|Z(D_4)| \geq 2$  (puesto que de momento ya sabemos que  $1, B^2 \in Z(G)$ ). Podría ser entonces  $|Z(D_4)| = 4, 8$  (probamos los divisores de  $|D_4|$ ). Como  $D_4$  no es abeliano, es claro que  $|Z(D_4)| \neq 8$ . Tampoco puede ser  $|Z(D_4)| \neq 4$  porque si tuviera 4, el cociente  $D_4/Z(G)$  tendría orden 2 y por tanto sería cíclico. Pero ya hemos probado que  $G/Z(G)$  no puede ser cíclico (ver proposición 19). Luego ya sabemos que  $Z(D_4) = \{1, B^2\}$ .

Vamos a seguir sacando cajas. Veamos  $cl(B)$ . Claramente  $B \in C(B)$  y por alguna razón que me falta  $C(B) = \{1, B, B^2, B^3\}$ . Por la fórmula tenemos que  $|cl(B)| = [D_4 : C(B)] = 2$ . Tenemos una vez más que utilizar el isomorfismo de conjugación. Sabemos que  $cl(B) = \{gag^{-1} \mid g \in G\}$ . Pero al ser  $\phi_g$  isomorfismo y  $\langle B \rangle$  normal, tenemos que  $\phi_g : \langle b \rangle \rightarrow \langle b \rangle$  también es isomorfismo y por tanto lleva elementos de orden  $n$  en elementos de orden  $n$ . Por tanto  $\phi_g(B) = g B g^{-1}$  solo puede ser  $B^3$  (a parte de  $B$ ). Luego ya tenemos que  $cl(B) = \{B, B^3\}$ .

¿Qué pasa con  $A$ ? Pues es claro que  $C(A) \supset \{1, A, B^2, AB^2\}$  ya que  $B^2 \in Z(G)$  por lo que está en todos los  $C(c_i)$ .

Vez pasada tomábamos  $a \in G$  y teníamos  $cl(a) = \{gag^{-1} \mid g \in G\} = \{a = a_1, a_2, \dots, a_r\}$  y  $C(a) = \{g \in G \mid hah^{-1} = a\}$ . Concluíamos que  $|cl(a)| = [G : C(a)]$ .

Vamos a generalizar al caso  $S \subset G$ ,  $S \neq \emptyset$ . Consideramos la familia de subconjuntos siguiente:

$$\{g S g^{-1} \mid g \in G\} = \{S = S_1, S_2, \dots, S_r\}$$

que tiene  $r$  subconjuntos distintos.

Recordemos que la conjugación dada  $\phi_g(x) = g x g^{-1}$  (el isomorfismo conjugación) es un isomorfismo<sup>2</sup>, y por tanto una biyección entre subconjuntos  $S_i \subset G$ . Por tanto  $|S| = \phi_g(S)$ .

<sup>2</sup>A veces tomate frito llama a este isomorfismo  $\gamma_g$



**Definición 24** (Normalizador de un subgrupo). Fijado  $S \subset G$ , definimos el normalizador de  $S$ :

$$N(S) = \{h \in G \mid hSg^{-1} = S\} \quad (3.6)$$

Se parece mucho a la definición de centralizador de un elemento (22). En el caso en que  $S = \{a\}$  tenemos que  $N(S) = \{h \in G \mid hah^{-1} = a\} = C(a)$ .

Ojo, decir que  $hSh^{-1} = S$  no significa que  $\forall b_i \in S, hb_ih^{-1} = b_i$ , sino que  $hb_ih^{-1} \in S$  (no mandamos cada elemento a él mismo, sino que todos quedan dentro del subconjunto). Es decir que  $N(S)$  es el conjunto de la totalidad de elementos para los que  $\phi_g$  manda el subconjunto  $S$  en sí mismo.

**Proposición 25.** Dado  $S \subset G$ ,  $N(S)$  es un subgrupo.

*Demostración.*

Como  $G$  es finito,  $N(S)$  es subgrupo  $\iff S \neq \emptyset \wedge N(S)$  es cerrado por la operación.

- Es claro que  $e \in N(S)$  pues  $eSe^{-1} = S$ , luego  $N(S) \neq \emptyset$ .
- Tenemos que probar la clausura. Si  $h_1Sh_1^{-1} = S \wedge h_2Sh_2^{-1} = S$  tenemos que  $\underbrace{(h_2Sh_2^{-1})}_{\in S}h_1^{-1} = S \implies h_1h_2 \in N(S)$ .

♣

**Proposición 26.**  $\{gSg^{-1} \mid g \in G\} = \{S = S_1, S_2, \dots, S_r\}$  son  $r$  subconjuntos distintos. Es decir que  $r = [G : N(S)]$ .

*Demostración.* A la izquierda del lector.<sup>3</sup>

♣

Supongamos ahora que en vez de ser  $S \subset G$ , tomamos  $S < G$ . Recordemos que dado  $g \in G$ ,  $\phi_g$  es un isomorfismo por tanto manda elementos de un subgrupo en otro subgrupo (si el subgrupo es normal, manda elementos de un subgrupo en sí mismo).

**Proposición 27.**  $H \subset N(H)$

*Demostración.* Si tomamos  $h \in G$ , tenemos que  $hHg^{-1} = H$  y también  $h^{-1}H(h^{-1})^{-1} = H$  (todo elemento de  $H$  también tiene a su inverso en  $H$ ).

♣

**Teorema 42.** Sea  $G$  grupo,  $H < G$ . Entonces  $H \triangleleft N(H)$  y  $N(H)$  es el mayor subgrupo de  $G$  con esta propiedad, es decir,  $H \triangleleft H' \implies H' \subset N(H)$ .

*Demostración.*

- Para probar que  $N \triangleleft N(H)$  tiene sentido olvidarse del grupo  $G$ . Tenemos que  $h \in N(H) \iff hHh^{-1} = H, \forall h \in G$ . En particular, tenemos que  $hHh^{-1} = H, \forall h \in N(H) \implies H$  es normal en  $N(H)$ .
- Para probar que  $N(H)$  es el mayor subgrupo con esta propiedad demostraremos que si  $H < H'$  y  $H \triangleleft H'$  entonces  $H' \subseteq N(H)$ . La demostración es casi una tautología. Tenemos que  $\forall h' \in H', h'Hh'^{-1} = H \implies \forall h' \in H', h' \in N(H) \implies H' \subset N(H)$ .

♣

**Corolario.**  $H \triangleleft G \iff N(H) = G$

*Demostración.* Sabemos que  $H \triangleleft H = \{gHg^{-1} \mid g \in G\}$  y dicho conjunto tiene  $[G : N(H)] = 1$  elementos, luego  $N(H) = G$ . En otras palabras, el normalizador de un subgrupo  $H < G$  normal es todo el grupo  $G$ .

♣

**Proposición 28.**  $Z(G) < N(H)$

*Demostración.* Por definición de  $Z(G)$  tenemos que los elementos  $g \in Z(G)$  fijan no solo los elementos dentro de subconjuntos, sino que los fijan uno a uno. Por lo que es claro que  $Z(G) < N(H)$ .

♣

**Ejemplo 33.** Vamos a empezar por  $G = S_3$ . En  $S_3$  tenemos los subgrupos  $\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle$  de orden 2 y el subgrupo  $\langle(123)\rangle = \{(1), (123), (132)\}$  de orden 3.

- En el caso de este último  $g\langle(123)\rangle g^{-1} = \langle(123)\rangle$  porque es el único subgrupo de orden 3. Por tanto  $\langle(123)\rangle \triangleleft S_3$  y entonces  $N(\langle(123)\rangle) = S_3$ .

<sup>3</sup>Left to the reader.

- Sin embargo en el caso de los subgrupos de orden 2 es posible que  $g\langle(12)\rangle \neq \langle(12)\rangle$ , porque hay más de un subgrupo de orden 2. Observemos por ejemplo que  $(13)(12)(13)^{-1} = (32) = (23)$ , luego  $\langle(12)\rangle$  no es normal en  $S_3$ , ya que hemos encontrado  $g = (13) \in G$  que lo mueve. Pero ¿quién es el normalizador  $N(\langle(12)\rangle)$ ? Pues ya sabemos que es un subgrupo propio, porque no puede dar todo  $S_3$ . Evidentemente  $\langle(12)\rangle \subset N(\langle(12)\rangle)$ . Luego tiene que ser que  $N(\langle(12)\rangle) = \langle(12)\rangle^4$

**Ejemplo 34.** Seguimos por el famoso grupo  $D_4$  (presentación en el ejemplo 4). Vimos anteriormente (ejemplo 32) que  $Z(D_4) = \{1, B^2\}$ . Tenemos su retículo en ???. Queremos ver de entre los subgrupos de  $D_4$ , cuáles son los que conmutan.

- Empecemos por  $\langle b \rangle = \{1, b, b^3, b^3\}$ . Observamos que  $\langle b \rangle$  es normal puesto que tiene índice 2, es decir que  $\{g\langle b \rangle g^{-1} \mid g \in G\} = \{\langle b \rangle\}$  y tiene sentido que  $[G : N(\langle b \rangle)] = 1$ . Es decir que como  $\langle b \rangle$  es normal tenemos que  $N(\langle b \rangle) = D_4$ .
- Seguimos por  $H = \{1, A, B^2, AB^2\}$ . Ocurre lo mismo, luego  $N(H) = D_4$ .
- Con el caso de  $\langle B^2 \rangle$  tenemos también que  $N(\langle B^2 \rangle) = D_4$  por ser normal.
- Agotados los subgrupos normales, nos quedan los más difíciles. Consideramos ahora  $\langle A \rangle$ . Una vez más nos preguntamos quién es el normalizador de  $\langle A \rangle$ .
  1. Es claro que  $\langle A \rangle$  conjugará con otros subgrupos de orden 2.
  2. También es claro que  $\langle A \rangle \subset N(\langle A \rangle)$  y que  $\langle B^2 \rangle \subset N(\langle A \rangle)$ . Luego  $N(\langle A \rangle)$  tiene al menos 2 elementos.
  3. También sabemos que  $N(\langle A \rangle) \subsetneq G$  puesto que  $\langle A \rangle$  no es normal, por lo que no puede tener 8 elementos. Por esto y porque  $N(\langle A \rangle) < G$ , concluimos que  $|N(\langle A \rangle)| = 4$ .
  4. ¿Cuáles mueven al  $\langle A \rangle$ ? Sabemos que no puede haber más de dos, pues el normalizador tiene 4 elementos. Pues mirando la presentación nos damos cuenta de que  $BA = AB^{-1} \iff BAB^{-1} = AB^2$ . Luego nos damos cuenta de que  $A$  se mueve a  $AB^2$ .
  5. Análogamente nos damos cuenta de que  $AB$  se mueve a  $AB^3$ .
  6. Ya tenemos los dos elementos que se mueven.

**Ejemplo 35.** Vamos ahora con el grupo de cuaterniones  $H$  descrito en el ejemplo 3.

1. Nos dibujamos el retículo.
2. Primeramente nos damos cuenta de que  $\langle A \rangle \cap \langle b \rangle \supsetneq \{e\}$  porque  $H$  tiene 8 elementos y por la fórmula del producto libre 17 y porque todo producto directo de subgrupos está contenido en el grupo aunque no sea subgrupo.
3. Ocurre lo mismo con los demás subgrupos de orden 4 ( $\langle A \rangle, \langle AB \rangle$ ). Tiene que tener intersección no vacía. En concreto la intersección es el subgrupo generado  $\langle A^2 = B^2 = (AB)^2 \rangle$ .
4. En  $H$  todos los subgrupos son normales, por lo que no tienen "órbitas" de modo que es muy aburrido.

**Ejemplo 36.** Consideramos ahora  $D_5$  que funciona como el  $D_4$ :

$$D_5 = \{1, B, B^2, B^3, B^4, A, AB, AB^2, AB^3, AB^4\}$$

$$o(B) = 5$$

- Primera observación. Como  $o(B) = 5$  que es primo, tenemos que  $o(B^k) = 5$ ,  $k = 1, \dots, 4$ . Luego cualquier subgrupo generado por  $\langle B^k \rangle = \langle B \rangle$ . Aquí falta algo.
- Observemos que los subgrupos propios pueden ser de 2 o 5 elementos.
- No puede haber subgrupos generados por dos elementos de  $D_5$  (por qué?)
- Los únicos subgrupos son  $\langle B \rangle$  y los generados por  $A, AB, AB^2, AB^3, AB^4$ .
- Afirmamos que  $\{gAg^{-1} \mid g \in G\} = \{\langle A \rangle, \langle AB \rangle, \langle AB^2 \rangle, \langle AB^3 \rangle, \langle AB^4 \rangle\}$ . Vamos a probarlo.
  1. Primero nos damos cuenta de que  $\{1, A\} \in N(\langle A \rangle)$ .
  2. Además tenemos que no puede haber otro grupo por encima de  $\langle A \rangle$  y  $D_5$  por lo que tenemos que  $N(A) = \langle A \rangle$ .
  3. Por tanto en la órbita de  $A$  tenemos  $[D_5 : \langle A \rangle] = 5$  grupos.

<sup>4</sup>No tiene gracia que  $\langle(12)\rangle$  sea normal en sí mismo, lo que tiene gracia es que  $\langle(12)\rangle$  es el mayor grupo donde  $\langle(12)\rangle$  es normal.

Sea  $X$  conjunto. Consideramos

$$\text{Biy}(X) = \{f \mid f : X \rightarrow X \text{ biyección}\}$$

En el caso en que  $|X| = n$ , por ejemplo  $X = \{1, 2, 3, \dots, n\}$  tenemos que  $\text{Biy}(X) = S_n$ . Como  $f : X \rightarrow X$  si  $f$  es inyectiva entonces automáticamente es sobre y por tanto biyectiva.

En general, tiene sentido pensar en  $\text{Biy}(X)$  aunque  $|X| = \infty$ . Además, en dicho conjunto viven la biyección identidad y la biyección inversa para cada biyección. Por tanto, tiene sentido pensar en  $(\text{Biy}(X), \circ)$  como un grupo (la composición de biyecciones da una biyección).

Nos concentramos en el caso en el que  $|X| = n$  que nos da  $\text{Biy}(X) = S_n$ . Ya hemos visto que  $S_2 = \{1, \sigma\} \implies |S_2| = 2$  y para  $S_3$  tenemos  $|S_3| = 3!$  y en general  $|S_n| = n!$ .

Fijamos un conjunto  $X$  y un homomorfismo de grupos  $\alpha : X \rightarrow \text{Biy}(X)$ . A partir de estos datos definimos una relación de equivalencia que nos da una partición de  $X$ , es decir, vamos a partir  $X$  en conjuntos disjuntos.

**Ejemplo 37.** Supongamos<sup>5</sup>  $G = X$ ,  $|G| = n$  y consideramos  $\rho : G \rightarrow \text{Aut}(G) \subset \text{Biy}(X)$ . Definimos la relación en  $X = G$

$$aRb \iff \exists g \in G \mid \phi_g(a) = b, \phi_g(x) = gxg^{-1}$$

que es la relación de conjugación dada por el isomorfismo de conjugación de toda la vida.

Ahora, en lugar de pensar en  $G = X$  pensamos en  $X = \{H < G\}$  (los subgrupos de  $G$ ). Para cualquier isomorfismo de grupos  $\beta : G \rightarrow G$ , tenemos que si  $H < G$  entonces  $\beta(H) < G$ .

Lo que hemos hecho aquí es un caso particular de lo que viene ahora.

**Proposición 29.** Sea  $\alpha : G \rightarrow \text{Biy}(X)$ ,  $g \mapsto \alpha(g)$  un homomorfismo de grupos. Definimos la relación de equivalencia

$$aRb \iff \exists g \in G \mid \alpha(g)(a) = b \quad (3.7)$$

Afirmamos que la relación es de equivalencia y que nos divide  $G$  en subconjuntos disjuntos (nos particiona  $G$ ).

*Demostración.* Probamos las 3 propiedades de las relaciones de equivalencia.

1. Reflexiva:  $\forall x \in X, aRa$ . Por ser  $\alpha$  homomorfismo tenemos que  $\alpha(e_G) = id_X$  y por tanto  $\alpha(e_G)(a) = a$ .
2. Simétrica:  $aRb \implies bRa$ . Partimos de que  $\exists g \in G \mid \alpha(g)(a) = b$ . Tomamos  $g^{-1} \in G$  y por ser  $\alpha$  homomorfismo de grupos tenemos que  $\alpha(g^{-1})(b) = (\alpha(g))^{-1}(b) = a$ .
3. Transitiva:  $aRb \wedge bRc \implies aRc$ . Partimos de que  $\exists g, g' \in G \mid \alpha(g)(a) = b \wedge \alpha(g')(b) = c$ . Tomamos  $g'g \in G$  y tenemos que  $\alpha(g'g)(a) = \alpha(g')(\alpha(g)(a)) = \alpha(g')(b) = c$  por composición de biyecciones.



¿Cómo son las clases que da la partición?

Pues tenemos que  $cl(a) = \{\alpha(g)(a) \mid g \in G\}$  para un  $a \in G$ . Definimos  $H_a = \{g \in G \mid \alpha(g)(a) = a\}$ . Tenemos por lo visto anteriormente que  $H_a < G$  y  $|cl(a)| = [G : H_a]$ . Entonces tenemos lo siguiente:

- En el caso en que  $X = G$  tenemos que  $H_a = C(a)$  donde  $C(a)$  es el centralizador de  $a$  (definición 22).
- En el caso en que  $X = \{H < G\}$  tenemos que  $H_a = N(a)$  donde  $N(a)$  es el normalizador de  $a$  (definición 24).

Veremos que se pueden dar más casos.

**Ejemplo 38.** Fijamos  $\sigma \in S_n$  y  $G = \langle \sigma \rangle$  subgrupo generado por  $\sigma$  en  $S_n$ . Entonces  $G = \langle \sigma \rangle \rightarrow S_n = \text{Biy}(X)$  algo pasó. Si  $X = \{1, 2, \dots, n\}$  definimos  $\sigma(1) = 2, \sigma(2) = 1, \sigma(i) = i + 1, i = 3, \dots, n - 2, \sigma(n - 1) = 3$ . La clase  $cl(i) = \{\sigma^k(i) \mid k \in \mathbb{Z}\}$  en particular contiene a la identidad ya que  $\sigma^{n!} = id$  y  $n! \in \mathbb{Z}$ . Nos quedan dos clases

$$\begin{aligned} cl(1) &= \{1, 2\} \\ cl(3) &= \{3, 4, 5, \dots, n - 1\} \end{aligned}$$

Vemos que si fijamos  $\sigma$  se define una partición en  $\{1, \dots, n\}$  de subconjuntos disjuntos

$$F_1 \cup F_2 \cup \dots \cup F_n$$

Si  $r = |F_i| > 1$ ,  $F_i = \{i_0, i_1, \dots, i_r\}$  tal que  $\sigma(i_0) = i_1, \sigma(i_1) = i_2, \dots, \sigma(i_r) = i_0$ .

**Definición 25** (Ciclo). Diremos que  $\sigma$  es un ciclo de longitud  $r$  si en la partición definida

$$F_1 \cup F_2 \cup \dots \cup F_n$$

todas las cajas  $F_j$ ,  $j < r$  tienen un único elemento y  $F_r$  tiene  $r$  elementos.

<sup>5</sup>Por qué cojones cambia ahora la letrita?

**Proposición 30.** Toda biyección  $\sigma \in S_7$  se puede descomponer como composición de ciclos.

**Ejemplo 39.** Consideramos<sup>6</sup>

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 5 & 6 & 3 & 7 \end{pmatrix}$$

que nos divide  $X = \{1, 2, 3, 4, 5, 6, 7\}$  en tres subconjuntos disjuntos  $\{1, 2\}$ ,  $\{3, 4, 5, 6\}$ ,  $\{7\}$ . Por tanto podemos decir

$$\sigma = (12)(3456)(7) = (12)(3456) = (3456)(12)$$

(podemos conmutar porque al ser ciclos disjuntos lo que toque uno no lo toca el otro).

Proximamente veremos que a partir de la descomposición en ciclos disjuntos es fácil obtener el orden de  $\sigma$ .

Falta la semana fatídica de ANAMAT

- Recordemos que fijado  $\sigma \in S_5$  podemos dar una descomposición en ciclos  $\sigma = (123)(45)$  que es única aunque los ciclos se escriban diferente (por ejemplo  $(123) = (231)$ ).
- Fijado  $\tau \in S_5$ ,  $\tau\sigma\tau^{-1} = (\tau(1)\tau(2)\tau(3))(\tau(4)\tau(5))$  la descomposición se mantiene
- Si dos permutaciones  $\sigma, \sigma'$  tienen descomposiciones del mismo tipo (un 3-ciclo y un 2-ciclo como antes) entonces existe un  $\tau$  que hace pasar de una a otra.

**Ejemplo 40** (Posibles descomposiciones en ciclos de  $S_4$ ). ■ Para  $(1234)$

$$cl((1234)) = \{\tau(1234)\tau^{-1} \mid \tau \in S_4\}$$

- A la hora de definir  $\tau$  tenemos varias posibilidades. En este caso, si empezamos por el 1, para fijar el segundo elemento solo tenemos 3 posibilidades, para el tercero 2 y para el último una. Por tanto

$$|cl((1234))| = 4$$

- Recordemos que el centralizador

$$C_{S_4}((1234)) = \{\sigma \in S_4 \mid \sigma(1234)\sigma^{-1} = (1234)\} < S_4$$

- Como  $S_4$  tiene  $|S_4| = 4! = 24$  y tenemos que  $|cl((1234))| = [S_4 : C_{S_4}((1234))] = 6$  necesariamente  $|C_{S_4}((1234))| = 4$ .
- Nos proponemos calcular el grupo  $C((1234))$ . Un candidato para  $\sigma \in C((1234))$  es  $\sigma = (1234)$ . En efecto  $(1234)(1234)(1234) \in C((1234))$ . Siempre ocurre que un elemento conmuta consigo mismo. Además,  $\langle(1234)\rangle < C((1234))$  pero como  $|\langle(1234)\rangle| = 4 = |C((1234))|$  tiene que ocurrir que  $\langle(1234)\rangle = C((1234))$ . Es decir que de tipo 4 solo tenemos  $(1234)$ .
- ¿Qué tipos tenemos? Pues tantos como maneras de descomponer 4 en suma de números positivos, a saber
  - $(1234)$  de tipo 4
  - $(123)$  de tipo 3+1
  - $(12)(34)$  de tipo 2+2
  - $(12)$  de tipo 2+1+1
  - $Id$  de tipo 1+1+1+1 (que es la única que tiene descomposición en 4 unos)
- En general no es difícil calcular cuantos hay, por lo que a menudo utilizamos este argumento para calcular el grupo centralizador.
- Lo importante es que estamos descomponiendo  $S_4$  de la siguiente manera:

$$\begin{aligned} S_4 &= cl((1234)) \cap cl((1223)) \cap cl((12)(34)) \cap cl((12)) \cap cl(Id) \\ |S_4| &= |cl((1234))| \cap |cl((1223))| \cap |cl((12)(34))| \cap |cl((12))| \cap |cl(Id)| \end{aligned}$$

- Ahora analizamos la clase  $cl((123))$  de los ciclos de tipo 3+1. Lo primero es saber cuantos hay. Pues tenemos que elegir 3 elementos de entre 4 y luego ordenar los dos que nos quedan por tanto

$$|cl((123))| = \binom{4}{3} \times 2 = 8$$

Por otro lado lo que sabemos es que  $(123) \in C((123))$  (porque todos conmutan consigo mismos) y como antes  $|C((123))| = 3$  (de la fórmula  $|cl((123))| = [S_4 : C((123))]$ ), luego  $C((123)) = \langle(123)\rangle$ .

<sup>6</sup>Utilizamos la notación de biyecciones de [?].

- Igual es un poco más interesante la clase de tipo 2+2. **Pregunta de examen:** halla generadores del subgrupo centralizador del elemento  $(12)(34)$ .
  - Sabemos que el conjugado de un elemento de tipo 2 tiene que ser otro de tipo 2, por tanto tenemos que ver qué elementos distintos de tipo 2 tenemos. Pues fijamos el 1 por ejemplo y vemos qué parejas podemos hacer. Nos salen 3, a saber, 1 con 2, 1 con 3 y 1 con 4 de lo que concluimos que  $|cl((12)(34))| = 3$ .
  - De la misma fórmula que antes sacamos que  $|C((12)(34))| = 8$ . De orden 8 sabemos que hay solo unos pocos grupos (ver la clasificación en 3.1). Veamos con cuál de ellos es isomorfo.
  - Como siempre sabemos que  $(12)(34) \in C((12)(34))$ . Tenemos que encontrar los demás  $\tau$  que conmutan  $\tau\sigma\tau^{-1} = \tau(12)(34)\tau^{-1} = (\tau(1)\tau(2))(\tau(3)\tau(4))$ . Probamos con  $\tau = (1324)$ <sup>7</sup>.

$$\begin{aligned} & (1324)(12)(34)(1324)^{-1} \\ & \quad (34)(21) \end{aligned}$$

Que es el mismo, luego hemos probado que  $\tau$  conmuta y por tanto  $\tau \in C((12)(34))$ . Lástima que no valga porque nos damos cuenta de que  $\tau^2 = (12)(34)$ . Vaya. Drácula ha hecho chiste con esto y todo  $(X, d)$ .<sup>8</sup>

Lo que hacemos es quitar el  $(12)(34)$  y cambiarlo por el  $(12)$ . Para evitar  $\tau^2 \neq (12)$ . En resumen, ya tenemos  $(12) \in C((12)(34))$  y  $\tau = (1324) \in C((12)(34))$ . Si vemos sus grupos generados:

$$\begin{aligned} \langle (1324) \rangle &= \{(1324), (12)(23), (4321), Id\} \\ \langle (12) \rangle &= \{(12), Id\} \end{aligned}$$

La intersección de ambos subgrupos es solo la identidad y por la fórmula del producto libre averiguamos que  $|\langle (1324) \rangle \langle (12) \rangle| = 8$  por lo  $C((12)(34)) = \langle (1324), (12) \rangle$ .

Tiene toda la pinta de ser  $D_4$  porque está generado por dos elementos, no es abeliano y los órdenes de los generadores son  $o((1324)) = 4$ ,  $o((12)) = 2$ . Solo nos quedaría probar que se sigue cumpliendo la ecuación de la presentación de  $D_4$ :

$$BA = AB^3 \iff (1324)(12) = (12)(1324)^3$$

Lo comprobamos y al final sale.

- Ahora hacemos lo mismo con  $C((12))$ . Siguiendo un razonamiento similar, llegamos a que  $C((12))$  es isomorfo con el grupo de Klein y por extensión con  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

Falta la semana fatídica de Estadística

Vez pasada considerábamos  $G_1 \times G_2$  y fijado un homomorfismo de grupos  $\phi : G_1 \rightarrow \text{Aut}(G_2)$  hacíamos lo siguiente. En  $G_1 \times_{\phi} G_2$  viven los elementos  $(a, b) \times_{\phi} (c, d)$  donde la operación cambiaba en la primera coordenada  $(a\phi_b(c), bd)$ . Probamos la última clase que  $G_1 \times_{\phi} G_2$  era un grupo (probar la asociatividad no es trivial).

<sup>7</sup>La idea de probar con este viene de decir: pues a ver qué pasa si cambio el 1 con el 3 y el 2 con el 4, que nos daría la permutación  $(1324)$ . En cualquier caso esto es prueba y error, y parar de probar cuando tengamos un grupo generado de orden 8.

<sup>8</sup>Aquí se ve claramente que la elección del  $\tau$  es casi al azar. Hemos elegido uno que prometía pero hemos tenido la mala suerte de que su cuadrado nos daba un elemento que suponíamos estaba en el grupo ( $\tau^2 = (12)(34)$ ). Podríamos haber descartado este  $\tau = (1324)$  pero hemos preferido descartar el elemento  $(12)(34)$  que sabíamos que estaba en el grupo. La razón de la sustitución de este último por el  $(12)$  es un misterio hasta la fecha.



## Parte II

### Parcial 2 - hojas 2 y 3

