

# Apuntes de Estructuras Algebraicas

E. Hernandis et al.  
Curso 2018-2019 @ UAM

Revisión del 16 de enero de 2019 a las 01:13.

# Índice general

<b>I Grupos</b>	<b>5</b>
<b>1. Grupos</b>	<b>7</b>
1.1. Grupos	7
1.2. Subgrupos	9
1.2.1. Retículo de subgrupos	10
1.2.2. Subgrupos generados	10
1.3. Presentación de un grupo. Más ejemplos de grupos.	11
1.4. Grupos de permutaciones	12
1.4.1. Notación cíclica para permutaciones	13
1.5. Grupos cíclicos	14
1.6. Sobre los órdenes	14
1.7. El teorema de Lagrange	15
1.7.1. Subgrupos normales y grupo cociente	16
<b>2. Homomorfismos de grupos</b>	<b>17</b>
2.1. Homomorfismos de grupos	17
2.1.1. Ejemplos de homomorfismos de grupos	18
2.2. Retículo de subgrupos	19
2.3. Teoremas de la isomorfía	21
<b>3. Clasificación de grupos de orden pequeño</b>	<b>23</b>
3.1. Producto directo de grupos	23
3.2. Producto libre de grupos	23
3.3. Clasificación de grupos finitos	25
3.3.1. Teorema de clasificación de grupos finitos de orden pequeño	25
3.4. Extra	27
<b>4. El teorema de Cauchy</b>	<b>29</b>
4.1. Consideraciones previas	29
4.1.1. Conjugación	29
4.1.2. Centro de un grupo	30
4.1.3. Centralizador de un elemento.	31
4.2. Teorema de Cauchy	31
4.2.1. P-grupos	32
4.3. Más sobre la conjugación, el centro y los centralizadores.	33
4.4. Normalizador de un subconjunto	34
<b>5. Biyecciones</b>	<b>39</b>
5.1. El por qué de la notación cíclica	39
5.2. De permutaciones a composiciones de ciclos	41
5.3. Sobre las conjugaciones de una descomposición en ciclos	42
5.4. Trasposiciones	43
5.4.1. Paridad de las trasposiciones	43
5.5. Clases de equivalencia de permutaciones en $S_n$	44
5.5.1. Estudio de un caso: descomposición detallada del grupo $S_4$	45
5.6. Clases de equivalencia de subgrupos en $S_n$	46
5.7. [Sub]grupos alternados	46
5.8. Grupos simples	47
<b>6. Teoremas de Sylow</b>	<b>49</b>
6.1. Nuevas estructuras de grupo en el producto directo	49

6.2. Producto semidirecto . . . . .	50
6.3. Teoremas de Sylow . . . . .	52
<b>7. Grupos abelianos</b>	<b>59</b>
7.1. Descomposición en suma directa . . . . .	59
7.2. P-grupos abelianos finitos . . . . .	60
7.3. Teorema de estructura de grupos abelianos finitos . . . . .	61
<b>II Anillos</b>	<b>63</b>
<b>8. Anillos (y cuerpos)</b>	<b>65</b>
8.1. Definición y propiedades básicas . . . . .	65
8.1.1. Extensiones de anillos . . . . .	66
8.1.2. Unidades en anillos . . . . .	66
8.2. Subanillos . . . . .	67
8.3. Producto directo . . . . .	68
8.3.1. Unidades en el producto directo de anillos . . . . .	68
8.4. Divisores de $\mathbf{0}$ . Dominios de integridad. . . . .	68
8.5. Ideales . . . . .	69
8.5.1. Ideales generados. Ideales principales. Dominios de ideales principales. . . . .	70
8.5.2. Ideales primos . . . . .	71
8.5.3. Ideales maximales . . . . .	71
8.5.4. Ideales y el producto directo . . . . .	72
<b>9. Homomorfismos de anillos</b>	<b>73</b>
9.1. Extensión desde los homomorfismos de grupos. . . . .	73
9.2. Homomorfismos de anillos y divisores de $\mathbf{0}$ . . . . .	73
9.3. Homomorfismos de anillos e ideales . . . . .	74
9.3.1. Relación de equivalencia inducida por los ideales . . . . .	74
9.3.2. Retículo de ideales . . . . .	75
9.3.3. Correspondencia entre ideales por un epimorfismo de anillos . . . . .	75
9.4. Primer teorema de isomorfía para anillos . . . . .	77
9.5. Cuerpo de fracciones de un anillo . . . . .	78
<b>10. Anillos de polinomios</b>	<b>81</b>
10.1. Definiciones básicas y primeros resultados . . . . .	81
10.2. Factorización e irreducibilidad en anillos de números . . . . .	82
10.3. Factorización e irreducibilidad en anillos de polinomios . . . . .	84
10.3.1. Criterios de irreducibilidad . . . . .	84
10.3.2. Construcción de anillos de polinomios finitos . . . . .	84
<b>11. Por clasificar</b>	<b>87</b>
11.1. Clase de equivalencia por el grupo de biyecciones . . . . .	87
11.2. Por revisar . . . . .	89
<b>III Apéndices</b>	<b>93</b>
<b>A. Ejercicios</b>	<b>95</b>
A.1. Hoja 1 . . . . .	95
A.2. Hoja 2 . . . . .	96
A.3. Hoja 4 . . . . .	98
A.4. Hoja 5 . . . . .	98
<b>B. Índices</b>	<b>101</b>

# Parte I

## Grupos



# 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** Hay dos notaciones para hablar sobre grupos. La utilizada para dar la definición es la multiplicativa (salvo el símbolo utilizado para la operación que es uno especial y el uso de la  $e$  para el elemento neutro). También existe la notación aditiva.

Concepto	Notación aditiva	Notación multiplicativa
elemento neutro	<b>0</b>	<b>1</b>
inverso de $a$	$-a$	$a^{-1}$
$a$ operado consigo mismo $k$ veces	$k \cdot a = ka$	$a^k$

Figura 1.1: Diferencias entre notaciones para grupos

Cuando escribimos  $ka = a^k$  también podemos estar refiriéndonos a un entero  $k$  no positivo. Denotamos por  $a^k$ :

- si  $k > 0$ ,  $a^k = \underbrace{a * a * \dots * a}_{k \text{ veces}}$
- si  $k = 0$ ,  $a^0 = e$
- si  $k < 0$ ,  $a^k = \underbrace{a^{-1} * a^{-1} * \dots * a^{-1}}_{-k \text{ veces}}$

Veamos ahora algunos ejemplos de grupos infinitos (que tienen un número infinito de elementos).

**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
- $GL_2(\mathbb{R}) = \{A \in \mathbb{R}^{2 \times 2} \mid \det A \neq 0\}$  las matrices reales no singulares  $2 \times 2$  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  $\iff \det A \neq 0$ )

Y a continuación una serie de grupos finitos

**Ejemplo 2** (Grupo de las clases módulo  $n$ ).  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$  con la suma es un grupo.

**Ejemplo 3.** El conjunto  $(\mathbb{Z}^*/n\mathbb{Z}, \cdot)$  formado por  $\{1, 2, \dots, n\}$  con el producto no da un grupo, porque hay elementos que no tienen inverso. Es interesante considerar el conjunto de unidades en este conjunto:

$$\mathcal{U}(\mathbb{Z}^*/n\mathbb{Z}) = \{a \in \mathbb{Z}^*/n\mathbb{Z} \mid \exists a^{-1}, aa^{-1} = 1\}$$

que sí es un grupo con el producto<sup>1</sup>.

Los elementos de este grupo son tales que  $\forall m \in \mathcal{U}(\mathbb{Z}^*/n\mathbb{Z}), \exists a \in \mathbb{Z}^*/n\mathbb{Z} \mid m \cdot a \equiv 1 \pmod n \iff ma + nb = 1 \iff \text{mcd}(m, n) = 1$ . De esta manera tenemos un método fácil para obtener los elementos de  $\mathcal{U}(\mathbb{Z}^*/n\mathbb{Z}) = \{m \in \mathbb{Z}^*/n\mathbb{Z} \mid \text{mcd}(m, n) = 1\}$ . Aquí van algunos ejemplos:

- $\mathcal{U}(\mathbb{Z}^*/6\mathbb{Z}) = \{1, 5\}$
- $\mathcal{U}(\mathbb{Z}^*/12\mathbb{Z}) = \{1, 5, 7, 11\}$
- $\mathcal{U}(\mathbb{Z}^*/23\mathbb{Z}) = \{1, 2, 3, \dots, 22\}$  ya que 23 es primo

Hay muchos más grupos. Algunos de los grupos que hemos visto son en realidad el mismo grupo, solo que con dos maneras de verlo. De lo que va esta asignatura es de clasificar los grupos y de deducir propiedades comunes entre varios de ellos.

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

$$a * b = a * c \implies b = c \tag{1.1}$$

$$c * a = b * a \implies a = b \tag{1.2}$$

*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 2** (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 3** (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:

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

**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  $G$ ,  $|G| = |\{a_1, a_2, \dots, a_n\}| = n$ .

<sup>1</sup>Este grupo es en realidad una simplificación de un concepto que aparece en los anillos que son estructuras algebraicas con dos operaciones. En anillo no hace falta hacer la distinción de quitar el 0 y no solamente tenemos la noción de grupo de unidades para las clases de los enteros módulo  $n$



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

De los ejemplos vistos anteriormente, son abelianos aquellos en los que la operación es conmutativa. Por ejemplo,  $(\mathbb{R}, +)$  es abeliano porque  $\forall a, b \in \mathbb{R}, a + b = b + a$ . Por el contrario el grupo  $GL_2(\mathbb{R})$  no es abeliano porque el producto de matrices no es conmutativo.

**Teorema 4.** Sea  $G$  un grupo tal que  $\forall g \in G, g * g = e$ . Entonces  $G$  es abeliano.

**Corolario 1.**  $\forall a \in G, o(a) = 2 \implies G$  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  $(a * b) * (a * b) = e \implies (a * b) = (a * b)^{-1} = b^{-1} * a^{-1} = b * a$ . ♣

## 1.2. Subgrupos

**Definición 5** (Subgrupo). Sea  $(G, *)$  un grupo,  $S \subseteq G, S \neq \emptyset$ . 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.)

En caso de que el grupo del que elegimos el subgrupo sea finito, la clausura no es tan complicada de probar y suele merecer la pena empezar por ahí. De hecho en el caso finito, es suficiente para garantizar que el subconjunto sea un subgrupo. Véase el siguiente teorema / ejercicio.

**Teorema 5** (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  $s^r = e \implies s * s^{r-1} = e \implies s^{r-1} = s^{-1}$ . ♣

**Teorema 6.** 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 [DH96].

- ( $\implies$ ). 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  $xy = x(y^{-1})^{-1} \in H$ .

**Proposición 7.** Si  $\{S_i\}_{i \in \mathbb{N}}$  es una familia de subgrupos de  $G$ , entonces  $\bigcap S_i$  también es un subgrupo de  $G$ .

*Demostración.* Es claro que se verifican las tres propiedades:

1. Clausura: si los elementos están en cada uno de los subgrupos entonces están en su intersección.
2. Elemento neutro: existe pues está en todos los subgrupos.

3. Elemento inverso: existe por la clausura.



### 1.2.1. Retículo de subgrupos

**Definición 6** (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. Es un diagrama de Hasse para la relación de inclusión.

**Ejemplo 4** (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  $6\mathbb{Z}$ .

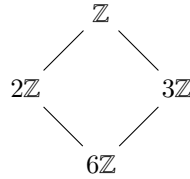



Figura 1.2: Una parte del retículo de subgrupos de  $\mathbb{Z}$ , en concreto la de los  $n\mathbb{Z}$  con  $n \mid 6$ .

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 8.** 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  $H = n\mathbb{Z}$ . 

### 1.2.2. Subgrupos generados

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

$$\langle S \rangle = \{s_1^{\alpha_1} * s_2^{\alpha_2} * \dots * s_n^{\alpha_n} \mid s_1, s_2, \dots, s_n \in S, \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}\} \quad (1.4)$$

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

**Proposición 9.** El subgrupo generado por  $S$ ,  $\langle S \rangle$  es el más pequeño que contiene a  $S$ .

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

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\} \quad (1.5)$$

**Proposición 10.** 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 11.** 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. ♣

**Teorema 12.** 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  $G$ ,  $g \in H \implies g^k, \forall k \in \mathbb{Z}$ . ♣

### 1.3. Presentación de un grupo. Más ejemplos de grupos.

Con la noción de subgrupo generado ya tenemos tres maneras de dar los elementos de un grupo (o subgrupo):

1. Por su nombre, por ejemplo, los reales con la suma  $(\mathbb{R}, +)$ .
2. Explícitamente, citando todos los elementos, por ejemplo  $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$
3. Con la noción de grupo generado, por ejemplo  $\mathbb{Z}/5\mathbb{Z} = \langle \bar{1} \rangle$ .

Sin embargo, esto no suele ser suficiente para conocer un grupo. Por ejemplo, si nos hablan del grupo generado  $\langle \bar{1} \rangle$  pueden estar refiriéndose a varios grupos, por ejemplo a  $\mathbb{Z}/5\mathbb{Z}$  o a  $\mathbb{Z}/2\mathbb{Z}$ . Necesitamos una manera de dar la operación entre los elementos de un grupo. De esta manera tanto si enumeramos los elementos como si damos un grupo a partir de un generador, sabemos exactamente cómo se comporta el grupo.

Una manera de hacer esto es dar una tabla con todas las posibles operaciones entre cualesquiera dos elementos. Por la propiedad asociativa, esta tabla nos daría todas las operaciones necesarias para obtener el valor de cualquier palabra en los elementos de un grupo. Otra opción es dar una **presentación**.

**Definición 9** (Presentación de un grupo). Una presentación de un grupo  $G$  es un par de conjuntos  $G = \langle S \mid R \rangle$  donde  $S$  es un conjunto de elementos generadores y  $R$  es un conjunto de relaciones -igualdades- entre elementos del grupo.

En ocasiones el conjunto de relaciones se omite o se da por separado. Para las relaciones del tipo  $a^k = e$ , donde  $a$  es un elemento de  $G$ , en ocasiones se escribe  $o(a) = k$ , que viene a ser lo mismo.

La definición anterior no hace comentario alguno sobre los requisitos de los conjuntos que intervienen en la presentación. La definición formal es complicada. Ver [Wik].

Veamos ahora ejemplos de dos grupos importantes dados por su presentación.

**Ejemplo 5** (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 1.3: Órdenes de los elementos de  $H$

Utilizando la notación estricta para la presentación tendríamos

$$H = \langle A, B \mid o(A) = o(B) = 4 \wedge A^2 = B^2 \wedge BA = AB^3 \rangle \quad (1.6)$$

y lo más importante: ya no hace falta decir quienes son  $A$  y  $B$ . De hecho, podían ser cualquier otra cosa que se comportara como las matrices que hemos dado antes y los teoremas que obtengamos para el grupo  $H$  aplicarían a esa otra cosa.

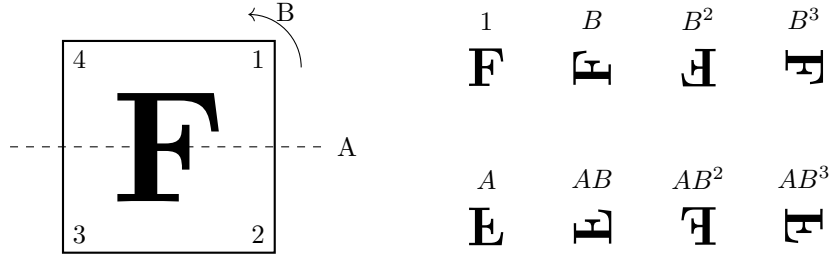


Figura 1.4: Simetría  $A$  y rotación  $B$  que compuestas forman los elementos del grupo  $D_4$

**Ejemplo 6** (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.

Geoméricamente,

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

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.

$$D_4 = \langle A, B \rangle \text{ donde } o(A) = 2, \quad o(B) = 4, \quad BA = AB^3 \quad (1.7)$$

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	2	2	2

Figura 1.5: Órdenes de los elementos de  $D_4$

**Nota:** lo que hemos hecho con un cuadrado también se puede hacer con un triángulo, con un pentágono o con cualquier polígono regular.

**Ejemplo 7** (Grupos diédricos de orden  $n$ ). Generalizando, podemos escribir cualquier grupo  $D_n$  con la presentación

$$D_n = \langle a, b \mid o(a) = 2, \quad o(b) = n, \quad ba = ab^{-1} = ab^{n-1} \rangle$$

Todos estos grupos son no abelianos de orden  $2n$ .

Vistos estos ejemplos, continuamos con más definiciones y teoremas que se apoyan en la noción de grupo generado.

## 1.4. Grupos de permutaciones

Los grupos que se presentan a continuación fueron en realidad el germen de toda la teoría de grupos [DH96]. Se llaman grupos de permutaciones, de sustituciones o de biyecciones. Cuando son finitos a veces se llaman grupos simétricos de  $n$  elementos.

**Definición 10** (Grupo de permutaciones de  $n$  elementos). Definimos  $S_n$ , el grupo de permutaciones de  $n$  elementos como el grupo formado por las biyecciones entre dos conjuntos de  $n$  elementos con la operación de composición.

Por simplicidad tomamos siempre los conjuntos  $\{1, 2, \dots, n\}$ . Para referirnos a sus elementos  $\alpha \in S_n$  utilizamos la notación

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}$$

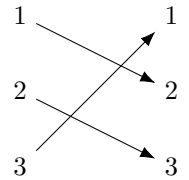


Figura 1.6: Elemento  $\alpha$  de  $S_3$

**Observación 1.** El grupo de permutaciones  $S_n$  tiene orden  $|S_n| = n!$ .

**Ejemplo 8.** Consideramos el grupo  $S_3$  de las biyecciones de  $\{1, 2, 3\}$  en sí mismo. Un elemento de este grupo es

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Se correspondería con la aplicación dada por (ver Figura 1.6)

**Ejemplo 9.** Consideramos ahora los elementos  $\alpha$  y  $\beta$  de  $S_3$  dados por

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Observamos que como la operación en  $S_3$  es la composición, el resultado  $\alpha \circ \beta$  se obtiene de aplicar primero  $\beta$  y luego  $\alpha$  (ver Figura 1.7)

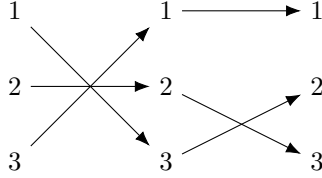


Figura 1.7: Resultado de la composición  $\alpha \circ \beta$

### 1.4.1. Notación cíclica para permutaciones

La notación vista hasta ahora es muy redundante porque la primera fila siempre se repite. Mejor utilizamos otra notación basada en *ciclos*.<sup>2</sup>

Veremos esta notación con una permutación de  $S_8$ :

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 7 & 5 & 1 & 8 & 6 & 3 \end{pmatrix}$$

Por convención, tomamos primero el 1. Para obtener el primer ciclo vemos las imágenes sucesivas de  $\alpha$  sobre el 1:

$$\alpha^0(1) = Id(1) = 1 \quad \alpha^1(1) = \alpha(1) = 4 \quad \alpha^2(1) = \alpha(4) = 5 \quad \alpha^3(1) = \alpha(5) = 1$$

Si siguiéramos aplicando  $\alpha$  sucesivamente obtendríamos de nuevo estos tres números ( $\alpha^4(1) = \alpha^1(1) = \alpha(1) = 4$ , y en general  $\alpha^j = \alpha^{j-3}$ ,  $\forall j > 3$ ). Así hemos obtenido nuestro primer ciclo al que llamaremos  $\sigma_1$  y denotaremos con  $(145)$ .

Para seguir, cogemos en la fila de arriba, al siguiente elemento que no hayamos recorrido ya, es decir que no esté en  $\sigma_1$ : es el 2. Repetimos el procedimiento

$$\alpha^0(2) = 2 \quad \alpha^1(2) = 2 \quad \alpha^j(2) = 2 \quad \dots$$

Este segundo ciclo solo tiene un elemento así que escribimos  $\sigma_2 = (2)$ .

Continuamos con el 3

$$\alpha^0(3) = 3 \quad \alpha^1(3) = 7 \quad \alpha^2(3) = 6 \quad \alpha^3(3) = 8 \quad \alpha^4(3) = 3$$

y obtenemos  $\sigma_3 = (3768)$  y ya no quedan más números en la fila de arriba por asignar a un ciclo. Lo bueno de este proceso es que ahora podemos escribir

$$\alpha = \sigma_3 \circ \sigma_2 \circ \sigma_1 = (3768)(2)(145)$$

Como el ciclo  $\sigma_2$  es la aplicación identidad lo podemos eliminar sin que afecte al resultado por lo que nos queda  $\alpha = (3768)(145)$ .

La razón por la que se utiliza esta notación va aún más allá de la economía de tinta y papel. Próximamente se darán propiedades de esta notación que permitirán calcular los órdenes de elementos de  $S_n$  de manera inmediata entre otras muchas.

Acabamos con un ejemplo del uso de esta notación.

**Ejemplo 10** (Grupo de biyecciones  $S_3$ ). Consideramos los elementos  $a = (123)$  y  $b = (12)$  de  $S_3$ . Podemos presentar el grupo con

$$S_3 = \langle a, b \mid o(a) = 3, o(b) = 2, ba = ab^2 \rangle$$

Ocurre que esta es la misma presentación que la del grupo  $D_3$  así que podremos dar un isomorfismo (cuando sepamos lo que son los isomorfismos) entre ellos y por tanto  $S_3 \simeq D_3$ .

<sup>2</sup>La definición de ciclo es algo complicada y vendrá más adelante. Básicamente, un ciclo es un elemento de una partición de  $S_3$

## 1.5. Grupos cíclicos

El objetivo de la teoría de grupos es clasificar todos los grupos sea cual sea su orden. En esta sección extinguimos la primera familia de grupos a clasificar: concluiremos con un teorema que nos clasifica los grupos cíclicos de cualquier orden.

**Definición 11** (Grupo cíclico). Sea  $(G, *)$  un grupo. Diremos que  $G$  es cíclico si  $\exists g \in G \mid \langle g \rangle = G$ .

Los grupos cíclicos ocuparán una parte central más adelante.

**Teorema 13.** 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  $i, j \in \mathbb{Z} \implies ab = a^i a^j = a^{i+j} = a^{j+1} = a^j a^i = ba$ . ♣

**Proposición 14.** 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. ♣

**Proposición 15.** 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. ♣

El siguiente resultado requiere que anticipemos el concepto de isomorfismo que se da en cuanto introduzcamos las funciones entre grupos: los homomorfismos. Básicamente se puede interpretar como igualdad.

**Teorema 16** (Teorema de clasificación de grupos cíclicos). De [DH96]. Sea  $G$  un grupo cíclico

1. Si  $|G| = \infty$  entonces  $G \simeq (\mathbb{Z}, +)$
2. Si  $|G| = n < \infty$  entonces  $G \simeq (\mathbb{Z}/n\mathbb{Z}, +)$

## 1.6. Sobre los órdenes

**Teorema 17.** 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 2.** 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 11.** 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,  $\langle 1 \rangle = \langle 3 \rangle$ .

**Proposición 18.** 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  $n$  tenemos que  $ir \in \mathbb{N}$ . ♣

**Teorema 19** (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 17 tenemos que  $o(g^{N/d}) = o(g) = n$ . Por la proposición 18 tenemos que  $o((g^{N/d})^d) = \frac{o(g^{N/d})}{d} = \frac{n}{d}$ . ♣

**Teorema 20.** Sean  $\bar{k}, \bar{k}' \in \mathbb{Z}/n\mathbb{Z}$ . Entonces  $o(\bar{k}) = o(\bar{k}') = d \implies \langle \bar{k} \rangle = \langle \bar{k}' \rangle$

## 1.7. El teorema de Lagrange

Previamente, introducimos una definición crucial a lo largo del curso.

**Definición 12** (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 21.** 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 22.** 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 21, como  $|g * H| = |H|$  la partición divide  $G$  en cajas iguales (ver cuadro 1.8). 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 1.8: Partición de  $G$  en  $r$  cajas iguales

Esto nos permite a su vez enunciar de manera natural el resultado que se conoce como Teorema de Lagrange: si un subgrupo da una relación de equivalencia que partición  $G$  en  $r$  cajas disjuntas, cada una con  $|H|$  elementos, entonces  $|H| \mid |G|$ .

**Teorema 23** (de Lagrange). Sea  $G$  un grupo finito y  $H < G$ . Entonces  $|H| \mid |G|$  (el orden de  $H$  divide al orden de  $G$ ).

**Corolario 3.** Sea  $G$  un grupo y  $g \in G$ . Entonces  $o(g) \mid |G|$  (el orden de un elemento divide al orden del grupo).

**Corolario 4.** 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. ♣

Sabiendo ahora que  $H < G \implies |H| \mid |G| \implies |G| = r \cdot |H|$ ,  $r \in \mathbb{N}$  vamos a ponerle un nombre a dicha  $r$ .

**Definición 13** (Índice de un subgrupo en un grupo). Sea  $H < G$ . Definimos el **índice de  $H$  en  $G$** , y lo representamos mediante  $[G : H]$ , como el cardinal del conjunto cociente  $G/H$ . [DH96]

### 1.7.1. Subgrupos normales y grupo cociente

**Definición 14** (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 24.** Si  $G$  es abeliano entonces todos sus subgrupos son normales.

**Definición 15** (Conjunto cociente en grupos). Sea  $H < G$ . Definimos

$$G/H = \{gH \mid g \in G\} \quad (1.8)$$

**Proposición 25.** Sea  $H \triangleleft G$ .  $(G/H, *)$  con la operación  $* : G/H \times G/H \rightarrow G/H, (xH)(yH) \mapsto (xy)H$  es un grupo.

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

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  $\forall \bar{x} \in G/H, \bar{x}\bar{x}^{-1} = xHx^{-1}H = xx^{-1}H = eH = \bar{e}$ . 

**Teorema 26.** De [DH96, p. 91]<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.

**Proposición 27.** Si  $H < G$  con  $|H| = n < \infty$  y además  $H$  es el único subgrupo de orden  $n$  entonces  $H \triangleleft G$ .

*Demostración.* Ver [DH96, p. 91]. 



## Capítulo 2

# Homomorfismos de grupos

### 2.1. Homomorfismos de grupos

Como en cualquier estructura algebraica, es interesante establecer correspondencias entre grupos. Los homomorfismos son funciones definidas de manera que la operación del grupo se preserve.

**Definición 16** (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  $G_1 \simeq G_2$ .

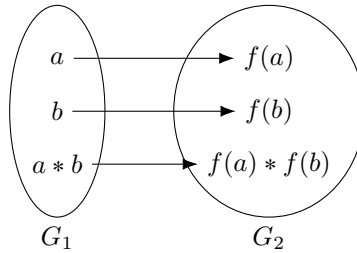


Figura 2.1: Homomorfismo de grupos

**Definición 17** (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 18** (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 28.** 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 29.** Sea  $f : G_1 \rightarrow G_2$  un homomorfismo.  $\text{Im } f < G_2$ .

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

**Teorema 30.** 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 31.** 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 32.** 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 33.** Sea  $f : G_1 \rightarrow G_2$  un homomorfismo de grupos. Entonces  $o(f(g))$  divide a  $o(g)$ .

**Teorema 34.** 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. Ejemplos de homomorfismos de grupos

**Ejemplo 12** (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 13.** 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 14.** En  $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  podemos construir  $n$  homomorfismos 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 15.** 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  $\text{Isom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ . Profundizamos en esto más adelante al hablar del producto semidirecto.

**Proposición 35** (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 16** (Automorfismo conjugación). Este ejemplo se utiliza tantísimo en lo que viene en el siguiente capítulo que tiene nombre propio.

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,  $\phi_g \circ \phi_{g^{-1}} = id$  luego  $\phi_g$  es un automorfismo (e isomorfismo) de grupos.

**Nota:** en ocasiones lo denotamos con  $\gamma_g$ .

**Ejemplo 17.** 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 18.** TODO: esto creo que es mentira.

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  $1 = e$ )

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

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 19** (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  $\ker f = \mathbb{Z}/4\mathbb{Z}$ . 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  $\bar{0} = \bar{n} \mapsto a^n = e$ .

## 2.2. Retículo de subgrupos

Los homomorfismos de grupos pueden ser de gran utilidad para encontrar el retículo de subgrupos.

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 36** (de correspondencia entre subgrupos mediante homomorfismos). Sea  $f : G_1 \rightarrow G_2$  un homomorfismo de grupos. Se tiene [DH96]:

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  $\forall x, y \in H_1$ ,  $xy \in H_1 \implies \forall f(x), f(y) \in H_2$ ,  $f(x)f(y) = f(xy) \in H_2$ .

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 37.** <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 [DH96] pero en dicha proposición no se exige que  $f$  sea sobre.

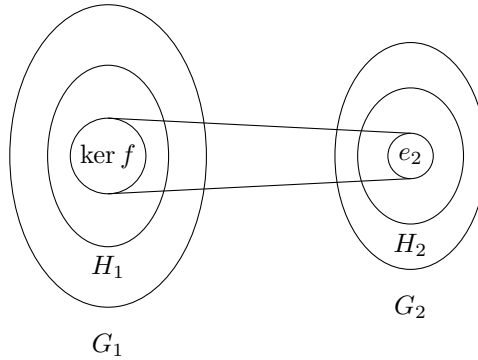
*Demostración.* Sabemos que por ser  $f$  homomorfismo,  $H_1 < G_1 \implies f(H_1) < G_2$ .

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.  $H_1 \subset f^{-1}(f(H_1))$  es evidente pues  $h \in H_1 \implies f(h) \in f(H_1)$ . Ahora probamos  $\ker f \subset H_1 \implies H \subset f^{-1}(f(H_1))$ .

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



**Ejemplo 20** (Retículo de subgrupos de  $\mathbb{Z}/8\mathbb{Z}$ ). 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  $f(8\mathbb{Z}) = \mathbb{Z}/8\mathbb{Z}$ ,  $f(4\mathbb{Z}) = \mathbb{Z}/4\mathbb{Z}$ ,  $f(2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ ,  $f(\mathbb{Z}) = \{e\}$ .

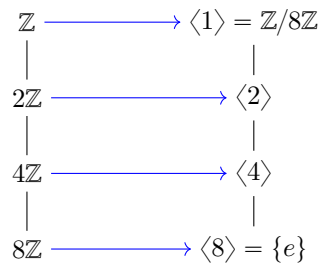


Figura 2.2: Retículo de subgrupos de  $\mathbb{Z}/8\mathbb{Z}$

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

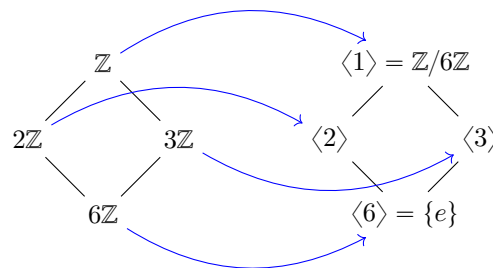


Figura 2.3: Retículo de subgrupos de  $\mathbb{Z}/6\mathbb{Z}$

## 2.3. Teoremas de la isomorfía

**Teorema 38.** (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  $f = \pi \circ \bar{f}$ .

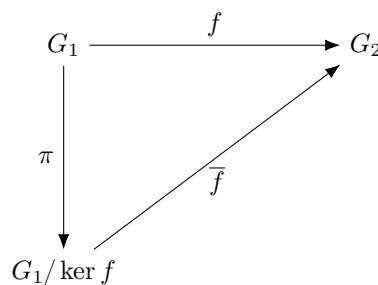


Figura 2.4: Primer teorema de la isomorfía.

**Teorema 39.** (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

$$G/H/K/H \simeq G/K \quad (2.1)$$

**Teorema 40** (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,

$$HK/K \simeq H/(H \cap K) \quad (2.2)$$



## Capítulo 3

# Clasificación de grupos de orden pequeño

El objetivo final de la teoría de grupos es clasificar los grupos según sus propiedades. Durante el resto del curso veremos formas cada vez más sofisticadas de clasificar los grupos. Empezaremos con algunos resultados que permiten clasificar grupos finitos de orden pequeño.

### 3.1. Producto directo de grupos

El producto directo de grupos permite generar otro grupo a partir de otros.

**Definición 19** (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  $\sim: (G_1 \times G_2) \times (G_1 \times G_2) \rightarrow G_1 \times G_2$ ,  $(g_1, g_2) \sim (g'_1, g'_2) = (g_1 * g'_1, g_2 \bullet g'_2)$ . En general, dados  $(G_1, *_1), \dots, (G_n, *_n)$  podemos definir el producto directo con

$$(G_1, *_1) \times \dots \times (G_n, *_n) = \bigtimes_{i=1}^n (G_i, *_i) = \left( \bigtimes_{i=1}^n G_i, \sim \right)$$

donde  $\sim: (\bigtimes_{i=1}^n G_i) \times (\bigtimes_{i=1}^n G_i) \rightarrow \bigtimes_{i=1}^n G_i$  con  $(g_1, \dots, g_n) \sim (g'_1, \dots, g'_n) = (g_1 *_1 g'_1, \dots, g_n *_n g'_n)$ .

Cuando se utiliza la notación aditiva es común llamarlo suma directa (ver definición 35).

El producto directo se trata con detalle más adelante pero aquí van un par de teoremas.

**Teorema 41.** 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  $m \cdot n$ . ♣

Este teorema puede ser útil combinado con el resultado anterior (teorema 16), para dar isomorfismos a productos directos que sean cíclicos.

**Teorema 42.** 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 más adelante (en la sección sobre clasificación de grupos finitos 3.3.1). ♣

### 3.2. Producto libre de grupos

**Definición 20** (Producto libre de grupos). Sean  $S, T$  subconjuntos del grupo  $G$ . Definimos  $ST = \{s * t \mid s \in S \wedge t \in T\}$ .

A veces, cuando se utiliza notación aditiva es común denotarlo por  $S + T$  (ver ??).

Es importante remarcar el **el producto libre de [sub]grupos no siempre es un grupo, a diferencia del producto libre que siempre funciona. En general solo es un conjunto.** Ver el teorema 44

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

$$|H_1H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|} \quad (3.1)$$

*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  $h'_1 = h_1\alpha$  y  $h'_2 = h_2\alpha$ ,  $\alpha \in H_1 \cap H_2$ . Entonces  $|f^{-1}(h_1h_2)| = |(h_1\alpha, h_2\alpha), \alpha \in H_1 \cap H_2| = |H_1 \cap H_2| \implies |H_1||H_2| = |H_1H_2||H_1 \cap H_2|$  ♣

**Teorema 44.** Sean  $H_1, H_2$  subgrupos de  $G$ , con  $G$  finito. Si  $H_2 \triangleleft G$  entonces  $H_1H_2 < G$  (si uno de los subgrupos es normal, entonces el producto es subgrupo).

*Demostración.* Observamos que podemos escribir  $H_1H_2 = \bigcap_{h \in H_1} h * H_2$ . Como  $H_2 \triangleleft G$ ,  $h * H_2 \cdot h' * H_2 = hh' * H_2 \forall h \in H_1$ . Si nos fijamos  $H_1H_2$  es cerrado por la operación pues  $hh' * H_2 \in H_1H_2$  y como  $G$  es finito y por tanto  $H_1, H_2$  también,  $H_1H_2$  es un subgrupo. ♣

**Teorema 45.** Si  $H_1 \triangleleft G$  y  $H_2 \triangleleft G \implies H_1H_2 \triangleleft G$  (si los dos subgrupos son normales, entonces el producto también es normal).

*Demostración.*  $H_1, H_2 < G$  luego  $\forall g \in G$ ,  $gH_1H_2g^{-1} = gH_1g^{-1}gHg^{-1} = H_1H_2$ . ♣



### 3.3. Clasificación de grupos finitos

#### 3.3.1. Teorema de clasificación de grupos finitos de orden pequeño

**Teorema 46** (Grupos notables de distintos órdenes finitos.).

- $|G| = 2, 3, 5, 7, 11, \dots, p$  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 23.
- $|G| = 4$ :
  - 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 grupos no abelianos de orden menor que 4.
- $|G| = 6$ :
  - 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 23).
- $|G| = 8$ :
  - 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 6) o bien con el grupo de cuaterniones  $H$  (ver ejemplo 5). Ver ejemplo 24

*Demostración.* En lo que resta de sección se dan algunos ejemplos de los razonamientos que llevan a estas afirmaciones. ♣

Vamos a aplicar el teorema 42 a grupos abelianos.

**Teorema 47.** Sea  $G$  abeliano con  $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ . Entonces

$$G \simeq \mathbb{Z}/p_1^{\beta_{11}}\mathbb{Z} \times \mathbb{Z}/p_1^{\beta_{1s_1}}\mathbb{Z} \times \dots \times \mathbb{Z}/p_n^{\beta_{ns_1}}\mathbb{Z} \times \mathbb{Z}/p_1^{\beta_{ns_n}}\mathbb{Z} \text{ donde } \alpha_i = \sum_{j=1 \dots s_i} \beta_{ij} \quad (3.2)$$

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

**Teorema 48.** Sea un número  $n$  y su factorización en primos:  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ . Entonces

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \times \dots \times \mathbb{Z}/p_n^{\alpha_n}\mathbb{Z} \quad (3.3)$$

*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  $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \times \dots \times \mathbb{Z}/p_n^{\alpha_n}\mathbb{Z}$  ♣

Lo que nos dice este teorema es que si un grupo es cíclico de orden  $n$  entonces es isomorfo a  $\mathbb{Z}/n\mathbb{Z}$  y a su vez a un producto directo en el que cada uno de los factores tiene como orden un factor de  $n$ , sin separarlos con la multiplicidad.

**Ejemplo 21.** Si un grupo de orden 12 es cíclico entonces es isomorfo a  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ , y no es isomorfo a  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ .

**Teorema 49.** 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 43 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 22.** 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 28).

**Ejemplo 23.** 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 (23)).

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 43) 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 26).

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 24.** Probar que si  $G$  es un grupo no abeliano con  $|G| = 8$  entonces o bien  $G \simeq D_4$  o bien  $G \simeq H$  donde  $H$  es el grupo de cuaterniones (ver ejemplo 5).

*Demostración.*

1. Tenemos que  $G$  no es abeliano. Por el contrarrecíproco del teorema 13 tenemos que no puede ser cíclico por lo que  $\nexists g \in G \mid o(g) = 8$ .

2. Por el teorema 4 sabemos que  $\exists b \in G \mid o(b) \neq 2 \implies o(b) = 4$ .

3. Por el teorema de Lagrange 23 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 26).

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 43 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 17. Luego  $\langle a \rangle \cap \langle b \rangle = \{1, a^2\} = \{1, b^2\} \implies \mathbf{a^2 = b^2}$ .
- f) Recopilando  $o(a) = 4$ ,  $o(b) = 4$ ,  $a^2 = b^2$ ,  $ba = ab^{-1}$  tenemos que  $G \simeq H$  ♣

### 3.4. Extra

**Ejemplo 25** (Retículo de subgrupos de  $D_4$ ). 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 6).

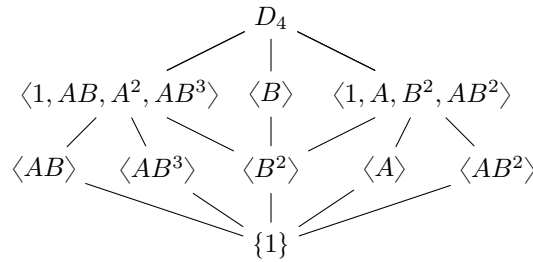


Figura 3.1: Retículo de subgrupos de  $D_4$

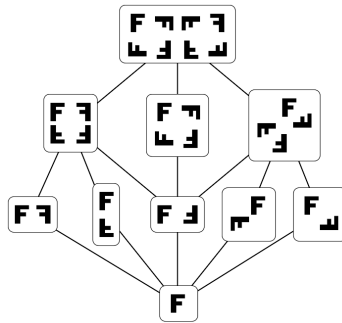


Figura 3.2: Retículo de subgrupos de  $D_4$  de [Epp]

Nos ayudamos de la imagen para sacarlos. La manera de hacerlo sin tener más información que la presentación del grupo es hacerse todos los subgrupos generados por cada elemento y descartar los que son iguales. Luego hacerse todos los subgrupos generados por dos elementos y descartar los que son iguales. Por alguna razón no hace falta probar con los generados por más de dos elementos. Una vez obtenidos estos grupos establecemos las relaciones de inclusión y creamos el diagrama de Hasse.

**Ejemplo 26.** Retículo de subgrupos del grupo de cuaterniones  $H$  (figura 3.3)

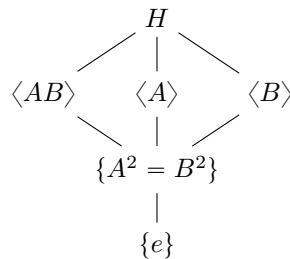


Figura 3.3: Retículo de subgrupos del grupo de cuaterniones  $H$ .

Para este ejemplo hemos probado con los posibles subgrupos que podían generar varios elementos.

- Siempre se tiene que  $\{e\} = \langle 1 \rangle < H$
- Además, como  $H = \langle A, B \rangle$  tenemos por definición que  $\langle A \rangle < H \wedge \langle B \rangle < H$ .

- De calcular los órdenes de los elementos tenemos que el único con orden 2 es  $B^2 = A^2$  por lo tanto su generado  $\langle B^2 \rangle = \{1, B^2\} < H$  (ver ejemplo 5 para los órdenes).
- Cualquier grupo generado con una  $A$  y una  $B$  nos genera automáticamente todo  $H$  por definición. Luego una posible estrategia es ver si algún otro elemento genera un subgrupo que no contenga a  $A$  y a  $B$ .
  - Nos damos cuenta después de muchas cuentas que  $\langle AB^2 \rangle = \{1, AB^2 = A^3, A^2 = B^2, A\} = \langle A \rangle < H$  pero no es nuevo así que no ha habido suerte.
  - Probamos con  $\langle AB \rangle = \{1, AB, A^2 = B^2, AB^3\} < H$  y tenemos suerte porque hemos encontrado uno que no estaba. Ocurrirá que  $\langle AB \rangle = \langle AB^3 \rangle$ .
  - Nos quedan por probar  $\langle B \rangle$  y  $\langle B^3 \rangle$ . Está claro que serán subgrupos y no serán el total porque no hay  $A$ s pero ocurre que son el mismo subgrupo.
- Así, hemos mirado todos los subgrupos generados por un elemento y hemos identificado los que son iguales. ¿Qué nos garantiza que grupos generados por dos elementos no serán alguno de los que hemos encontrado? Pues no sé.

El retículo de subgrupos de  $D_5$  lo veremos más adelante (para no llenar todo esto de retículos).

**Ejemplo 27.** 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 43 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 43)
  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 28.** 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 29.** 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 30.** 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 4

## El teorema de Cauchy

### 4.1. Consideraciones previas

#### 4.1.1. Conjugación

Cuando introducimos los homomorfismos de grupos hicimos especial hincapié en un automorfismo al que llamábamos  $\phi_g$  o  $\gamma_g$  y que para un  $g \in G$  dado se definía como

$$\begin{aligned}\phi_g : G &\rightarrow G \\ x &\mapsto gxg^{-1}\end{aligned}$$

Diremos a partir de ahora que dos elementos son conjugados si cumplen la siguiente definición.

**Definición 21** (Conjugados). Sea  $G$  un grupo,  $a, b \in G$ . Diremos que  $b$  es conjugado de  $a \iff \exists g \in G \mid b = gag^{-1}$ , es decir, si existe un  $g \in G$  para el que el automorfismo conjugación  $\phi_g$  cumple  $\phi_g(a) = b$ .

Observemos que la conjugación es una relación de equivalencia.

**Proposición 50.** Sea  $R$  una relación de equivalencia definida con

$$\forall a, b \in G, \quad aRb \iff \exists g \in G \mid b = gag^{-1}$$

Probamos las tres propiedades de las relaciones de equivalencia:

1. Reflexiva:  $\forall a \in G, \quad aRa$

*Demostración.* Tomando  $g = e$  se tiene  $\forall a, a = eae^{-1} = eae = a$ . ♣

2. Simétrica:  $\forall a, b \in G, \quad aRb \iff bRa$

*Demostración.* Se verifica la doble implicación tomando  $g' = g^{-1}$  utilizado en el otro lado:

$$aRb \implies \exists g \mid b = gag^{-1} \iff g^{-1}bg = a \iff g' = g^{-1} \wedge a = gb'g^{-1} \iff bRa$$

Hacia el otro lado es igual. ♣

3. Transitiva:  $\forall a, b, c \in G, \quad aRb \wedge bRc \implies aRc$

*Demostración.*

$$\begin{aligned}aRb \implies \exists g_1 \mid b &= g_1ag_1^{-1} \quad \wedge \quad bRc \implies \exists g_2 \mid c = g_2bg_2^{-1} \\ c &= g_2bg_2^{-1} = g_2g_1ag_1^{-1}g_2^{-1} \implies c = g'ag'^{-1} \text{ con } g' = g_1g_2 \implies aRc\end{aligned}$$
♣

**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 31.** 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.

En esta relación de equivalencia, las clases de equivalencia son de la forma  $cl(a) = \{gag^{-1} \mid g \in G\}$  (conjuntos de los elementos que son conjugados de  $a$ ). Queremos saber cuántos elementos hay en cada clase de equivalencia. Para ello introduciremos la noción de centralizador de un elemento y posteriormente daremos un teorema (proposición 59) que relaciona el número de elementos del centralizador de un elemento con el número de elementos de la clase de equivalencia de un elemento.

### 4.1.2. Centro de un grupo

**Definición 22** (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 ya que, en grupos abelianos, el centro es todo el grupo como veremos en la proposición 55.

**Proposición 51.** 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 52.** Sea  $G$  un grupo.  $Z(G)$  es un subgrupo y además es un subgrupo normal.

*Demostración.* Es un subgrupo porque es cerrado (ver proposición 51), contiene siempre al neutro (el centro conmuta con todos) y para todo  $a \in Z(G)$ , se tiene que  $\forall b \in G, ab = ba \iff aba^{-1} = b \iff ba^{-1} = a^{-1}b \iff a^{-1} \in Z(G)$ .

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

**Proposición 53.** Si  $H < Z(G)$  entonces  $H$  es abeliano y normal.

*Demostración.* Es abeliano porque  $\forall g, g' \in Z(G), gg' = g'g$  y en particular esto se cumple para  $g, g' \in H < Z(G)$ .

Es normal porque  $\forall g \in G, gH = \{ga \mid a \in H \wedge \forall b \in G, gb = bg\} = \{ag \mid a \in H \wedge \forall b \in G, bg = gb\} = Hg$ . ♣

**Proposición 54.** 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 55.**  $G$  es abeliano  $\iff G = Z(G)$

*Demostración.* 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  $1 = n - 1 \implies n = 2$ . ♣

La siguiente proposición es crucial para sacar conclusiones sobre los grupos sabiendo sobre sus órdenes y su centro.

**Proposición 56.** 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  $G/Z(G) = \{\overline{\alpha_i}, i = 1, \dots, n\}$  donde  $\overline{\alpha_i} = \alpha^i Z(G)$ . 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. ♣

## 4.1.3. Centralizador de un elemento.

**Definición 23** (Centralizador de un elemento). Sea  $a \in G$ . Llamamos centralizador de  $a$  al conjunto

$$C(a) = \{g \in G \mid \gamma_g(a) = gag^{-1} = a\} \quad (4.1)$$

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

**Proposición 57.**  $a \in Z(G) \iff C(a) = G \iff [G : C(a)] = 1$

*Demostración.* Es cristalina de las definiciones. ♣

**Proposición 58.**  $C(a)$  es un subgrupo de  $G$

*Demostración.* Por el teorema 5 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 59.**  $|cl(a)| = |\{gag^{-1} \mid g \in G\}| = [G : C(a)]$  (el número de elementos de una clase de equivalencia es el índice del centralizador de un representante)

De la proposición anterior se deduce que

**Corolario 5.**  $|C(a)| = [G : cl(a)]$

La prueba de la proposición se ve clara después de ver la prueba del teorema de Cauchy, así que la dejamos para después.

## 4.2. Teorema de Cauchy

**Teorema 60** (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 42,  $G \simeq \mathbb{Z}/p_1^{\beta_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\beta_2}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{\beta_r}\mathbb{Z}$  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  $\bar{c} = \{gcg^{-1} \mid g \in G\}$ . 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  $cl(e)$  tiene un único elemento.

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

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

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

Supongamos que la partición está dada por subconjuntos  $cl(a_1), cl(a_2), \dots, cl(a_s)$ . 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:

$$|G| = \sum_{i=1}^s |cl(a_i)| = \sum_{i=1}^n |\{ga_i g^{-1} \mid g \in G\}|$$

Ahora bien, por la proposición 59 tenemos que  $|cl(a_i)| = [G : C(a_i)]$ . Por tanto decir que  $|cl(a_i)| = 1 \implies [G : C(a_i)] = 1 \implies G = C(a_i)$ .

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

$$|G| = |Z(G)| + \sum_{i=r+1}^s [G : C(a_i)] \text{ donde } |Z(G)| = r \text{ y } [G : C(a_i)] \geq 2, \forall i = r+1, \dots, s \quad (4.2)$$

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  $n = 2$ . Son grupos cíclicos por lo que  $\exists \alpha \in G \mid o(\alpha) = 2$ .
3. 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  $p$ . Pues ya está:  $C(a_i) < G$  porque  $\alpha \in C(a_i) \mid o(\alpha) = p \implies \alpha \in G$  también. ♣
  - o bien  $p \nmid |C(a_i)|, \forall i = r+1, \dots, s$ . No podemos proceder por inducción. Por hipótesis  $|G| = [G : C(a_i)] \cdot |C(a_i)| \wedge p \nmid |G| \implies p \nmid [G : C(a_i)], \forall i = r+1, \dots, s$ .  
Como  $|G| = |Z(G)| + \sum_{i=r+1}^s [G : C(a_i)]$  y por hipótesis  $p \mid |G| \wedge p \nmid [G : C(a_i)], \forall i = r+1, \dots, s \implies p \mid |Z(G)| \implies |Z(G)|$  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 32.** 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 producto libre (43),  $|\langle a \rangle \langle b \rangle| = pq$ . No sabemos si se tendrá que  $G = \langle a \rangle \langle b \rangle$  ya que al no saber si alguno es normal, no podemos afirmar que el producto libre sea un grupo. 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 33.** 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

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

#### 4.2.1. P-grupos

Una aplicación inmediata del teorema de Cauchy es la caracterización de los  $p$ -grupos.

**Definición 24** (P-grupo). Sea  $p$  primo. Decimos que  $G$  es un  $p$ -grupo si  $|G| = p^r$ .

**Teorema 61.** 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 4.2 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. ♣

Véase un ejemplo de aplicación de esta anterior proposición en el ejercicio H2.22 y en el ejercicio H1.33

**Ejemplo 34.** Tenemos que  $Z(D_4) = \{1, B^2\}$  y  $Z(H) = \{1, B^2\}$  donde  $H$  es el grupo de cuaterniones (ejemplo 5) y  $D_4$  es el famoso grupo (ejemplo 6).

**Proposición 62.** 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 56) que  $G/Z(G)$  no puede ser cíclico. Por lo tanto  $|Z(G)| = p^2 \implies Z(G) = G \implies G$  es abeliano. ♣

### 4.3. Más sobre la conjugación, el centro y los centralizadores.

Antes de introducir el teorema de Cauchy hablábamos de la conjugación que era una relación de equivalencia que partía un grupo  $G$  en cajas. Nos gustaría saber cuántos elementos había en la clase de equivalencia de cada uno de los elementos de  $G$  y para eso introducíamos el concepto de centralizador de un elemento:  $C(a)$  el conjunto de los elementos de  $G$  que no mueven a  $a$  por conjugación. La proposición 59 nos aseguraba que  $|cl(a)| = [G : C(a)]$  y dijimos que retrasaríamos la prueba hasta ahora. Pues aquí va.

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 23) como  $C(a) = \{h \in G \mid hah^{-1} = a\} < G$ . Queremos probar que  $|cl(a)| = [G : C(a)] = r$ .

*Demostración de la proposición 59.* 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  $G = C(c_i) = \{\forall g \in G, gcg^{-1} = c\} \iff c \in Z(G)$ .

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 35.** Consideramos  $D_3$  (ver ejemplo 7). 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  $\phi_g(x) = gxg^{-1}$  (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  $\{1, A\} \in C(A)$  y en realidad no puede haber más porque si hubiese un tercero,  $\{1, A\}$  es un subgrupo de orden 2  $\implies o(\{1, A\})$  no divide a 3  $\implies$  si hubiese más,  $C(A) = D_3$  y eso no puede ser  $\implies C(A) = \{1, A\} \implies |cl(A)| = [D_3 : C(A)] = 6/2 = 3$ . Como las clases son disjuntas los tres elementos sobrantes forman la última caja.

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 36.** El caso del famoso grupo  $D_4$  (ver ejemplo 6) es mucho más interesante porque  $Z(D_4)$  no es trivial. Elegimos por ejemplo el elemento  $B^2$ . Probar que  $\phi_g(B^2) = gB^2g^{-1} = B^2$ ,  $\forall g \in D_4$  es complicado. Pero fijémonos en que  $\phi_B(B^2) = BB^2B^{-1} = B^2$  y que  $\phi_A(B^2) = AB^2A^{-1} = B^2$ . 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 56). 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  $\phi_g(B) = gBg^{-1}$  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  $C(c_i)$ .

Segundo intento.

1. Como siempre  $cl(e) = \{e\}$
2. Veamos  $cl(B)$ . Queremos ver cuántos elementos tiene. Sabemos que  $|cl(B)| = [D_4 : C(B)]$ . Veamos quién es  $C(B)$ . En primer lugar  $B \in C(B) \implies \langle B \rangle \in C(B)$ . Así ya tenemos que  $|C(B)| \geq 4$ . ¿Puede haber algún elemento más en  $C(B)$ ? No, porque si hubiera uno más, su orden ya sería  $|C(B)| = 8$  pues  $C(B) < D_4$ . Así concluimos que  $|cl(B)| = [D_4 : C(B)] = 8/4 = 2$ . Además sabemos que  $[D_4 : C(B)] = 2 \implies C(B) \triangleleft D_4 \iff gC(B)g^{-1} = C(B) \forall g \in D_4 \implies gBg^{-1} \in C(B)$ . Además como  $gxg^{-1}$  es un isomorfismo que lleva elementos de orden  $n$  en elementos de orden  $n$  obtenemos que  $o(gBg^{-1}) = o(B) = 2$ . Sabemos que  $B \in cl(B) \wedge cl(B) = \{gBg^{-1} \mid g \in D_4\} \wedge gBg^{-1} \in C(B) \implies gBg^{-1} = B^3$ . Por tanto  $cl(B) = \{B, B^3\}$ .
3. Veamos  $cl(A)$ . Queremos ver cuántos elementos tiene. Sabemos que  $|cl(A)| = [D_4 : C(A)]$ . Veamos quién es  $C(A)$ . En primer lugar  $A \in C(A) \implies \langle A \rangle \subset C(A)$ . Si  $B \in C(A)$  entonces  $C(A) = G$  pues  $B$  y  $A$  generan. Esto no puede ser porque  $C(A) = G \implies A$  conjuaga con todos los demás elementos pero sabemos que  $AB \neq BA$ . Ocurre lo mismo con  $B^3$ . Probamos con  $B^2$ .  $B^2AB^2 = BBAB^2 = BAB^3B^2 = BAB = AB^3B = A$  luego  $B^2 \in C(A)$ . Como  $C(A) < D_4$  sabemos que es cerrado y por tanto  $AB^2 \in C(A)$ . Ya no puede haber más elementos porque si hubiera más, entonces  $|C(A)| = 8$  y eso no puede ser. Por tanto  $|cl(A)| = [D_4 : C(A)] = 8/4 = 2$ . Sabemos que  $A \in cl(A)$ . ¿Quién es el otro elemento? Como antes,  $[D_4 : C(A)] = 2 \implies C(A) \triangleleft D_4 \iff gC(A)g^{-1} = A$ . Como  $gxg^{-1}$  es un isomorfismo mantiene el orden y por tanto los conjugados de  $A$  pueden ser  $B^2$  o  $AB^2$  (los únicos de orden 2 en  $C(A)$ )

## 4.4. Normalizador de un subconjunto

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:

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

que tiene  $r$  subconjuntos distintos.

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

**Definición 25** (Normalizador de un subconjunto). Fijado  $S \subset G$ , definimos el normalizador de  $S$ :

$$N(S) = \{g \in G \mid gSg^{-1} = S\} \tag{4.3}$$

<sup>1</sup>A veces tomate frito llama a este isomorfismo  $\gamma_g$

Se parece mucho a la definición de centralizador de un elemento (definición 23). En el caso en que  $S = \{a\}$  tenemos que  $N(S) = \{g \in G \mid gag^{-1} = a\} = C(a)$ .

Ojo, decir que  $gSg^{-1} = S$  no significa que  $\forall b_i \in S, gb_i g^{-1} = b_i$ , sino que  $gb_i g^{-1} \in S$  (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 63.** 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 64.**  $\{gSg^{-1} \mid g \in G\} = \{S = S_1, S_2, \dots, S_r\}$  son  $r$  subconjuntos distintos. Es decir que  $r = [G : N(S)]$ .

*Demostración.* A la izquierda del lector.<sup>2</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). Es por esto que la afirmación equivalente a la proposición anterior sería:

**Proposición 65.** Sea  $S < G$ . Entonces  $\{gSg^{-1} \mid g \in G\} = \{S = S_1, S_2, \dots, S_r\}$  son  $r$  subgrupos distintos.

**Teorema 66.** 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 6.**  $H \triangleleft G \iff N(H) = G$

*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 67.** Si  $H < G$  entonces<sup>3</sup>  $Z(G) < N(H)$

*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  $Z(G) < N(H)$ .

♣

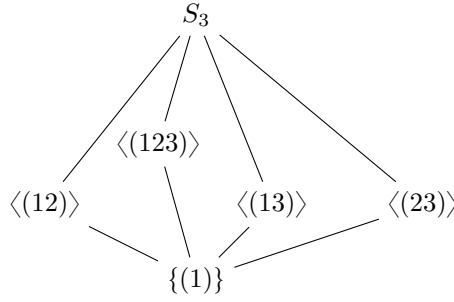
**Proposición 68.** Sea  $g \in G$ . Entonces  $C(g) < N(\langle g \rangle)$

**Ejemplo 37.** 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  $N(\langle(123)\rangle) = S_3$ .
- 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  $(13)(12)(13)^{-1} = (32) = \langle(23)\rangle$ , luego  $\langle(12)\rangle$  no es normal en  $S_3$ , ya que hemos

<sup>2</sup>Left to the reader.

<sup>3</sup>No sé si la hipótesis aquí es que  $H < G$  o que  $H \subset G$

Figura 4.1: Retículo de subgrupos de  $S_3$ 

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  $N(\langle(12)\rangle) = \langle(12)\rangle^4$

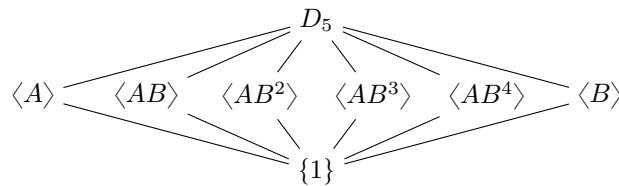
**Ejemplo 38.** Seguimos por El famoso grupo  $D_4$ . Vimos anteriormente (ejemplo 36) que  $Z(D_4) = \{1, B^2\}$ . Tenemos su retículo en Figura 3.1. Queremos ver de entre los subgrupos de  $D_4$ , cuáles son los que conmutan.

- Empecemos por  $\langle B \rangle = \{1, B, B^2, B^3\}$ . 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 39.** Vamos ahora con el grupo de cuaterniones  $H$  descrito en el ejemplo 5.

1. Nos dibujamos el retículo. Se puede consultar en Figura 3.3.
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 (teorema 43) 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 40.** Consideramos ahora  $D_5$  que funciona como el  $D_4$  (ver ejemplo 7 para más información sobre los grupos  $D_n$ ).

Figura 4.2: Retículo de subgrupos de  $D_5$ .

- 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.

<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.

- 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.



# Capítulo 5

## Bijecciones

### 5.1. El por qué de la notación cíclica

**Definición 26** (Conjunto de biyecciones). Sea  $X$  un conjunto. Definimos

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

Como coinciden dominio y codominio ( $f : X \rightarrow X$ ) 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). Lo escribimos en forma de teorema.

**Teorema 69.** Sea  $X$  un conjunto. El par  $(\text{Biy}(X), \circ)$  es un grupo.

Nos concentraremos en el caso en el que  $|X| = n < \infty$  que nos da  $\text{Biy}(X) = S_n$ . Ver definición 10 para una explicación detallada del grupo  $S_n$ .

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. Veamos un ejemplo particular.

**Ejemplo 41.** Supongamos  $G = X$ ,  $|G| = n$  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.

Ahora pasamos al caso general.

**Proposición 70.** Sea  $\alpha : G \rightarrow \text{Biy}(X)$ ,  $g \mapsto \alpha(g)$  un homomorfismo de grupos<sup>1</sup>. Definimos la relación de equivalencia  $R$  en el conjunto  $X$

$$aRb \iff \exists g \in G \mid \alpha(g)(a) = b \tag{5.1}$$

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

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

1. Reflexiva:  $\forall x \in X, xRx$ . 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  $\alpha(g^{-1})(b) = (\alpha(g))^{-1}(b) = a$ .

<sup>1</sup>Ojo: aquí las imágenes de los elementos  $g \in G$  son biyecciones  $f : G \rightarrow G$ , por eso tendrá sentido la notación  $\alpha(g)(a)$  que significa aplicar la función que nos devuelve  $\alpha$  al elemento  $a \in G$ .

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  $g'g \in C$  y tenemos que  $\alpha(g'g)(a) = \alpha(g')(\alpha(g)(a)) = \alpha(g')(b) = c$  por composición de biyecciones.

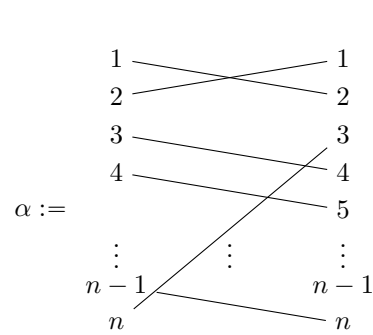


¿Cómo son las clases que da la partición?

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

- En el caso en que  $X = G$ , es decir, que el conjunto  $X$  tiene dentro *elementos* de  $G$ , tenemos que  $H_a = C(a)$  donde  $C(a)$  es el centralizador de  $a$  (definición 23).
- En el caso en que  $X = \{H < G\}$ , es decir, que el conjunto  $X$  tiene dentro *subgrupos* de  $G$ , tenemos que  $H_a = N(a)$  donde  $N(a)$  es el normalizador de  $a$  (definición 25).

Vista la definición abstracta, lo que nos interesa de esto es aplicarlo a los grupos  $S_n$  de los que hablábamos antes. En particular, ahora daremos una definición formal de ciclo para la notación que introdujimos en la Subsección 1.4.1.



Fijamos  $\sigma \in S_n$  y definimos  $G = \langle \sigma \rangle$  el subgrupo generado por  $\sigma$  en  $S_n$ . Definimos ahora el homomorfismo

$$G = \langle \sigma \rangle \rightarrow S_n = \text{Biy}(X), \quad X = \{1, 2, 3, \dots, n\}$$

Las clases  $cl(i)$  para  $i \in \{1, 2, \dots, n\}$  son de la forma<sup>2</sup>

$$cl(i) = \{\sigma^k(i) \mid k \in \mathbb{Z}\}$$

**Ejemplo 42.** Consideramos la permutación  $\alpha \in S_n$  dada por (ver Figura 5.1)

$$\alpha = \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & \dots & n-1 & n \\ 2 & 1 & 4 & 5 & \dots & n & 3 \end{array}$$

Figura 5.1: La permutación  $\alpha$  de  $S_n$

que en la notación cíclica podríamos escribir como  $\alpha = (345 \dots n)(12)$ .

En este caso la clase  $cl(1) = \{1, 2\} = cl(2)$  está formada por los elementos que podemos obtener de aplicar  $\alpha$  al elemento 1. Ya se intuye la utilidad de la notación cíclica: la permutación  $\alpha$  nunca mezcla elementos de la caja  $\{1, 2\}$  con elementos de la caja  $\{3, 4, 5, \dots, n\}$ . Así, también tendremos que  $cl(3) = cl(4) = \dots = cl(n) = \{3, 4, 5, \dots, n\}$ . Los elementos que hay en estas dos clases coinciden con los elementos que hay en cada uno de los ciclos en los que hemos descompuesto  $\alpha$ .

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 27** (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.

La definición quiere decir que, en el fondo, un ciclo es un tipo de permutación que al aplicarla sucesivamente sobre el conjunto  $X$  lo particiona en varias cajas pero de manera que todas tienen un elemento excepto una, que tiene todos los elementos que se mueven entre ellos por la acción del ciclo. Un ejemplo en el conjunto  $X = \{1, 2, 3, \dots, n\}$  sería

1	5	...	⋮
2	6	⋱	⋮
3	⋱	⋱	⋮
4	...	...	n

Observemos que por la notación que hemos elegido, los ciclos tienen la estructura  $(\sigma^0(a) \sigma^1(a) \sigma^2(a) \dots \sigma^s(a))$  donde  $\sigma$  es un elemento de  $S_n$  y  $a$  un elemento de  $X$ . Dado que si  $\sigma^k = Id$  entonces  $\sigma^{k+i} = \sigma^i$ , si *rotamos* los números que definen el ciclo no estamos haciendo nada. Esto es, el ciclo  $(1234) = (2341) = (3412) = (4123)$ .

<sup>2</sup>Las clases serían de la forma  $\alpha(g)(i)$  pero es que en este caso todos los  $\alpha(g)$  son elementos de  $G = \langle \sigma \rangle$  y por tanto son de la forma  $\sigma^k$ .



## 5.2. De permutaciones a composiciones de ciclos

**Proposición 71.** Toda biyección  $\alpha \in S_n$  se puede expresar como composición de ciclos disjuntos dos a dos:

$$\alpha = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_s$$

**Proposición 72.** La composición de dos ciclos disjuntos conmuta, es decir, si  $\sigma_1$  y  $\sigma_2$  son ciclos disjuntos (que no comparten ningún elemento entre los paréntesis) entonces  $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$

**Corolario 7.** Toda descomposición de una permutación  $\alpha \in S_n$  en ciclos disjuntos  $\alpha = \sigma_s \circ \sigma_{s-1} \circ \cdots \circ \sigma_2 \circ \sigma_1$  se puede reordenar sin cambiar el resultado.

**Ejemplo 43.** Antes de seguir veamos un ejemplo más de cómo una biyección de  $S_n$  particiona el conjunto  $X = \{1, 2, \dots, n\}$ .

Consideramos  $\alpha \in S_n$  definida con

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 1 & 5 & 6 & 4 & 7 & 9 & 8 & 10 \end{pmatrix}$$

La partición que nos da  $\alpha$  de  $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$  es la siguiente:

1	4	7	10
2	5	8	
3	6	9	

Partición de  $X$  dada por  $\alpha = (123)(456)(89)$

Esto lo obtenemos de buscar las clases de cada elemento. Empezamos por el que queramos, por ejemplo, el 1:

$$cl(1) = \{\alpha^k(1) \mid k \in \mathbb{Z}\} = \{\alpha^0(1) = 1, \alpha^1(1) = 2, \alpha^2(1) = 3, \alpha^3(1) = 1, \alpha^4(1) = 2, \dots\}$$

Eliminando duplicidades obtenemos que  $cl(1) = \{1, 2, 3\}$ . Análogamente obtenemos  $cl(4) = \{4, 5, 6\}$ ,  $cl(7) = \{7\}$ ,  $cl(8) = \{8, 9\}$ ,  $cl(10) = \{10\}$ . Lo que hemos hecho es seguir el algoritmo descrito en la Subsección 1.4.1, esta vez entendiendo el significado. Obtenemos que  $\alpha = (123)(456)(89)$  o cualquier reordenación de los ciclos anteriores, ya que al ser disjuntos, cambiar el orden en el que los rotamos no afecta al resultado.

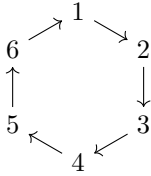


Figura 5.2: El ciclo  $\sigma = (123456)$

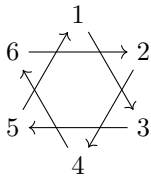


Figura 5.3: El ciclo  $\sigma^2 = (123456)^2$

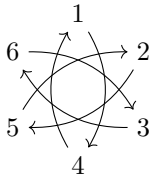


Figura 5.4: El ciclo  $\sigma^3 = (123456)^3$

Veamos ahora cómo se relacionan los órdenes de los ciclos con su longitud.

**Ejemplo 44.** Consideramos  $\sigma = (123456) \in \mathfrak{S}_n$ . Observamos que  $\sigma^6 = Id$  es decir que  $\sigma$  tiene orden 6.

De esta manera si nos preguntan por  $\sigma^{122} = (123456)^{122} = (123456)^{6 \cdot 20} \circ (123456)^2 = (123456)^2$  no nos asustamos.

Si nos hubieran dado  $\sigma$  con la notación habitual, aparte de que hubiera ocupado mucho, no podríamos haber resuelto esta operación tan rápido.

**Ejemplo 45.** Nos preguntamos ahora por las potencias de  $\sigma = (123456)$  menores que 6 =  $o(\sigma)$ .

- $\sigma^2$  equivaldría a aplicar  $\sigma$  dos veces a cada número  $\{1, \dots, 6\}$  (los demás números no nos interesan porque sabemos que  $\sigma$  no los mueve). Ayudándonos del dibujo obtenemos que  $\sigma^2 = (135)(246)$ .

Se verifica que  $\sigma^2$  tiene  $o(\sigma^2) = 3$  y además si recordamos el teorema 19 comprobamos que se verifica  $o(\sigma^2) = \frac{o(\sigma)}{\text{mcd}(o(\sigma), 2)} = \frac{6}{2} = 3$ .

- En cuanto a  $\sigma^3$  observamos que al aplicar  $\sigma$  3 veces nos quedan 3 ciclos y que se vuelve a verificar que  $o(\sigma^3) = \frac{o(\sigma)}{\text{mcd}(o(\sigma), 3)} = \frac{6}{3} = 2$

Esto nos lleva a enunciar el siguiente teorema

**Teorema 73.** Sea  $\sigma = (i_1 i_2 i_3 \dots i_n)$  un ciclo de longitud  $n$ . Sea  $m \in \mathbb{Z}$  y  $d = \text{mcd}(n, m)$ . Entonces  $\sigma^m$  es un producto de  $d$  ciclos de longitud  $\frac{n}{d}$  y estos son disjuntos dos a dos.

Poder averiguar los órdenes de ciclos es una herramienta muy potente. Por ejemplo, podemos hacer lo siguiente.

**Ejercicio (H3.8).** Demuestra que el subgrupo  $G < S_4$  generado por los elementos  $\sigma = (1432)$  y  $\tau = (24)$  es isomorfo a  $D_4$ .

*Demostración.* Sabemos que  $o(\sigma) = 4$  y que  $o(\tau) = 2$ . Trabajando un poco vemos que

$$\begin{aligned}\langle \sigma \rangle &= \{\sigma = (1432), \sigma^2 = (13)(24), \sigma^3 = (4321), \sigma^4 = Id\} \\ \langle \tau \rangle &= \{\tau = (24), \tau^2 = Id\}\end{aligned}$$

Faltaría ver que  $\sigma\tau = \tau\sigma^3$  es decir que  $(1432)(24) = (24)(4321)$  (spoiler: es verdad) y ya podríamos identificar  $\sigma$  con  $B$  y  $\tau$  con  $A$  para obtener la presentación del famoso grupo  $D_4$ :

$$D_4 \simeq G = \langle \sigma, \tau \mid o(\sigma) = 4 \wedge o(\tau) = 2 \wedge \sigma\tau = \tau\sigma^3 \rangle$$



**Teorema 74.** Sea  $\alpha$  una permutación expresada como composición de ciclos disjuntos  $\alpha = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_n$ . Entonces el orden de  $\alpha$  es el mínimo común múltiplo de los órdenes de cada  $\sigma_i$ :

$$\alpha = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_n \text{ disjuntos} \implies o(\alpha) = mcm(\sigma_1, \dots, \sigma_n)$$

*Demostración.* Ver [DH96, p. 120].



### 5.3. Sobre las conjugaciones de una descomposición en ciclos

Antes de seguir, vamos a introducir dos proposiciones que nos serán de gran ayuda al calcular conjugados de una permutación, por ejemplo, para cuando queramos calcular centralizadores.

**Proposición 75.** Sea  $\alpha \in S_n$  una permutación con descomposición en ciclos disjuntos

$$\alpha = \left( i_1^{(1)} i_2^{(1)} \dots i_{s_1}^{(1)} \right) \left( i_1^{(2)} i_2^{(2)} \dots i_{s_2}^{(2)} \right) \dots \left( i_1^{(r)} i_2^{(r)} \dots i_{s_r}^{(r)} \right)$$

y sea  $\omega \in S_n$ . Entonces el conjugado de  $\alpha$  por  $\omega$  es  $\alpha'$  y se obtiene de

$$\alpha' = \omega\alpha\omega^{-1} = \left( \omega(i_1^{(1)}) \omega(i_2^{(1)}) \dots \omega(i_{s_1}^{(1)}) \right) \left( \omega(i_1^{(2)}) \omega(i_2^{(2)}) \dots \omega(i_{s_2}^{(2)}) \right) \dots \left( \omega(i_1^{(r)}) \omega(i_2^{(r)}) \dots \omega(i_{s_r}^{(r)}) \right)$$

Se ve mejor con un ejemplo:

**Ejemplo 46.** Sea  $\alpha = (123)(45) \in S_5$  y sea  $\omega \in S_5$  alguna permutación. Entonces

$$\alpha' = \omega\alpha\omega^{-1} = \omega(123)(45)\omega^{-1} = (\omega(1) \omega(2) \omega(3)) (\omega(4)\omega(5))$$

También podemos ir en la otra dirección. Es decir, dados  $\alpha$  y  $\alpha'$  obtener  $\omega$ :

**Proposición 76.** Sean  $\alpha, \alpha' \in S_n$  dos permutaciones cuyas descomposiciones en ciclos disjuntos son del mismo tipo y se denotan por

$$\begin{aligned}\alpha &= \left( i_1^{(1)} i_2^{(1)} \dots i_{s_1}^{(1)} \right) \dots \left( i_1^{(r)} i_2^{(r)} \dots i_{s_r}^{(r)} \right) \\ \alpha' &= \left( j_1^{(1)} j_2^{(1)} \dots j_{s_1}^{(1)} \right) \dots \left( j_1^{(r)} j_2^{(r)} \dots j_{s_r}^{(r)} \right)\end{aligned}$$

Entonces  $\exists \omega \in S_n$  tal que  $\alpha' = \omega\alpha\omega^{-1}$  y  $\omega$  se puede construir (en notación no cíclica)

$$\omega = \begin{pmatrix} i_1^{(1)} & i_2^{(1)} & \dots & i_{s_1}^{(1)} & \dots & i_1^{(r)} & i_2^{(r)} & \dots & i_{s_r}^{(r)} \\ j_1^{(1)} & j_2^{(1)} & \dots & j_{s_1}^{(1)} & \dots & j_1^{(r)} & j_2^{(r)} & \dots & j_{s_r}^{(r)} \end{pmatrix}$$

**Ejemplo 47.** Sean  $\sigma, \sigma' \in S_5$ . Busco  $\tau \in S_5$  tal que  $\sigma'$  sea conjugada de  $\sigma$  por  $\tau$ , es decir,  $\tau \in S_n \mid \sigma' = \tau\sigma\tau^{-1}$ . Pues utilizamos el método

$$\begin{cases} \sigma &= (123)(45) \\ \sigma' &= (245)(13) \end{cases} \longrightarrow \omega = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

o en notación cíclica:  $\omega = (124)(35)$ .

## 5.4. Trasposiciones

**Definición 28** (Trasposición). Una trasposición es un ciclo de orden 2. Cualquier trasposición tiene orden 2.

Las trasposiciones tienen la forma  $(a b)$  pero observemos que también se pueden escribir como  $(b a)$  ya que lo que estamos haciendo es *rotar* (o empezar en otro lugar del ciclo).

**Proposición 77.** La inversa de cualquier trasposición es ella misma.

**Teorema 78.** El grupo  $S_n$  está generado por las trasposiciones  $\sigma \in S_n$ .


Ya sabemos que cualquier permutación se puede expresar como producto de ciclos [disjuntos]. Para probar este teorema probaremos la siguiente proposición:

**Proposición 79.** Cualquier ciclo se puede expresar como composición de trasposiciones.

La prueba es constructiva y describe la manera de expresar un ciclo como composición de trasposiciones.

*Demostración.* Sabemos que un ciclo  $\sigma$  se escribe como  $\sigma = (\sigma^0(a) = a \ \sigma^1(a) \ \sigma^2(a) \ \dots \ \sigma^s(a))$ . Pues basta con observar que la composición

$$\sigma = (a \ \sigma^s(a))(a \ \sigma^{s-1}(a)) \dots (a \ \sigma^2(a))(a \ \sigma(a))$$

tiene el mismo efecto. 

**Ejemplo 48.** La permutación  $\sigma = (1234)$  se puede expresar como  $\sigma = (14)(13)(12)$ .

### 5.4.1. Paridad de las trasposiciones

**Teorema 80.** Si  $\sigma \in S_n$  se puede descomponer como un número par de trasposiciones entonces toda expresión en  $\sigma$  expresada como una composición de un número par de trasposiciones.

Análogamente para las permutaciones que se pueden expresar como una composición de un número impar de trasposiciones.

*Demostración.* Definimos una función

$$S_n \rightarrow GL_n(\mathbb{N})$$

$$\sigma \mapsto \begin{pmatrix} e_\sigma(1) & \dots & e_\sigma(n) \\ \vdots & \vdots & \vdots \end{pmatrix}$$

Esta función es un homomorfismo de grupos.

Entonces si expresamos  $\sigma$  como composición de trasposiciones  $\sigma = (i_1^{(1)} i_2^{(1)})(i_1^{(2)} i_2^{(2)}) \dots (i_1^{(r)} i_2^{(r)})$  y aplicamos la función que hemos definido nos queda

$$A = \begin{pmatrix} e_\sigma(1) & \dots & e_\sigma(n) \\ \vdots & \vdots & \vdots \end{pmatrix} = \underbrace{\begin{pmatrix} i_1^{(1)} & \dots & i_2^{(1)} \\ \vdots & \vdots & \vdots \end{pmatrix}}_{\det=-1} \dots \underbrace{\begin{pmatrix} i_1^{(r)} & \dots & i_2^{(r)} \\ \vdots & \vdots & \vdots \end{pmatrix}}_{\det=-1}$$

y entonces

$$\det A = (-1)^r = \begin{cases} 1 & \text{si } r \text{ es par} \\ -1 & \text{si } r \text{ es impar} \end{cases}$$



Visto que la paridad de una permutación va a ser invariante por la expresión como composición de trasposiciones que elijamos vamos a darle nombre ya que parece importante

**Definición 29** (Paridad de una permutación). Sea  $\sigma \in S_n$ .

- Diremos que  $\sigma$  es par si se puede descomponer como una composición de un número par de trasposiciones.
- Diremos que  $\sigma$  es impar si se puede descomponer como una composición de un número impar de trasposiciones.

En otros textos, esto se define con la *signatura*

**Definición 30** (Signatura de una permutación). Sea  $\sigma \in S_n$  una permutación que podemos descomponer como una composición de  $r$  trasposiciones:  $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_r$ . Llamamos signatura de  $\sigma$  al número  $(-1)^r$  y lo denotamos por  $\text{sig}(\sigma) = (-1)^r$ .

Es muy interesante la manera en la que hemos demostrado el teorema 80. El homomorfismo que hemos construido de  $S_n$  a  $GL_n(\mathbb{N})$  se puede extender para llegar al determinante:

$$\begin{aligned} \varphi : S_n &\rightarrow GL_n(\mathbb{R}) && \rightarrow (\{-1, 1\}, \cdot) \\ \sigma &\mapsto A = \begin{pmatrix} e_\sigma(1) & \cdots & e_\sigma(n) \\ \vdots & \vdots & \vdots \end{pmatrix} && \mapsto \det(A) \end{aligned}$$

Si consideramos el homomorfismo desde  $S_n$  hasta  $(\{-1, 1\}, \cdot)$  nos damos cuenta de que hemos definido un homomorfismo de grupos que además es sobreyectivo.

El núcleo de dicho isomorfismo  $\ker \varphi = \{\sigma \in S_n \mid \varphi(\sigma) = 1\}$  es un subgrupo por el teorema de correspondencia entre familias de subgrupos bajo un epimorfismo (ver teorema 36). Además este subgrupo es normal y de índice 2. Tan importante es que le daremos nombre en la sección 5.7.

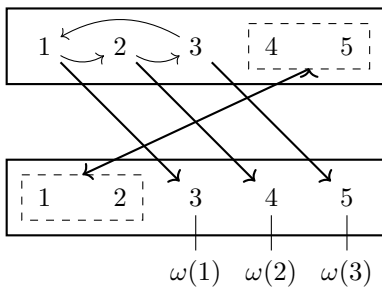
## 5.5. Clases de equivalencia de permutaciones en $S_n$

**Definición 31** (Tipo de una permutación). Sea  $\alpha \in S_n$  una permutación que descomponemos en composición de ciclos disjuntos

$$\alpha = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_r \text{ donde } o(\sigma_i) = \lambda_i \text{ y además } \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq 1 \wedge \sum_{i=1}^r \lambda_i = n$$

Entonces decimos que  $\alpha$  es de tipo o estructura  $(\lambda_1, \dots, \lambda_r)$ . A veces lo denotamos con  $\alpha$  es de tipo  $\lambda_1 + \cdots + \lambda_r$ .

**Ejemplo 49.** En  $S_8$  la permutación  $\alpha = (123)(45)(67)$  tiene tipo  $(3, 2, 2, 1)$  o bien  $3 + 2 + 2 + 1$ .



¿Por qué es interesante esto? Porque los elementos de  $cl(\alpha)$  son todas las permutaciones del mismo tipo que  $\alpha$ . Lo vemos con un ejemplo.

**Ejemplo 50.** Consideramos  $\alpha \in S_5$ ,  $\alpha = (123)$ . Los elementos de la clase de equivalencia son de la forma  $cl(\alpha) = \{\omega(123)\omega^{-1} \mid \omega \in S_5\}$ . Es decir que, por ejemplo:

$$\begin{aligned} cl((123)(45)) &= \{(i_1 \ i_2 \ i_3)(i_4 \ i_5) \mid \text{totalidad de elementos de tipo } (3, 2)\} \\ cl((12)) &= \{\text{elementos de clase } (2, 1, 1, 1)\} \end{aligned}$$

Observemos que  $\omega(123)\omega^{-1} = (\omega(1) \ \omega(2) \ \omega(3))$ . Con  $\omega = (12345)$  tenemos

$$\begin{aligned} \omega(123)\omega^{-1}(\omega(1)) &= \omega(123)\omega^{-1}(3) = \omega(123)(\omega(1)) = \omega(2) \\ \omega(123)\omega^{-1}(\omega(2)) &= \omega(123)\omega^{-1}(2) = \omega(123)(\omega(2)) = \omega(3) \\ \omega(123)\omega^{-1}(\omega(3)) &= \omega(123)\omega^{-1}(1) = \omega(123)(\omega(3)) = \omega(4) \end{aligned}$$

**Ejemplo 51.** ¿Cuántos elementos hay en la clase de equivalencia del elemento  $(123) \in S_3$ ?

- En  $S_3$  los posibles tipos son  $(3)$ ,  $(2, 1)$ ,  $(1, 1, 1)$ . El elemento  $(123)$  que es de tipo 3.
- Por lo visto anteriormente sabemos que  $cl((123)) = \{\text{totalidad elementos de tipo 3 en } S_3\}$ . Por tanto, la pregunta en los grupos de permutaciones es ¿cuántos 3-ciclos hay en  $S_3$ ?

- Recordemos que  $|cl((123))| = [S_3 : C((123))]$ , luego solo necesitamos saber cuántos elementos hay en  $C((123))$ .
  - Por el teorema de Lagrange (teorema 23) sabemos que los posibles órdenes del subgrupo  $C((123))$  son 1, 2, 3, 6 (los divisores de  $|S_3| = 6$ ).
  - Sabemos que siempre  $(123) \in C((123))$ . Además  $C((123))$  es un grupo, luego por clausura es necesario que  $\langle(123)\rangle \subset S_3$ . Esto nos dice que  $|C((123))| \geq 3$ .
  - ¿Puede haber algún elemento más? No, porque  $C((123))$  es un subgrupo propio. Esto quiere decir que tiene menos elementos que  $S_3$  luego  $|C((123))| < 6$ .
  - Entonces,  $C((123))$  solo puede tener 3 elementos (y por tanto  $C((123)) = \langle(123)\rangle$ ).
- Concluimos que  $|cl((123))| = [S_3 : C((123))] = \frac{6}{3} = 2$ . De hecho, los elementos son  $cl(123) = \{(123), (132)\}$ .

### 5.5.1. Estudio de un caso: descomposición detallada del grupo $S_4$

A lo largo de los siguientes ejemplos veremos cómo se descompone  $S_4$  en clases disjuntas de acuerdo a los tipos de sus permutaciones.

**Ejemplo 52.** Consideramos el grupo  $S_4$ . Queremos ver cómo se descompone  $S_4$  en clases de equivalencia según los tipos de sus permutaciones.

- Los posibles tipos en  $S_3$  son  $4, 3 + 1, 2 + 2, 2 + 1 + 1, 1 + 1 + 1 + 1$ . Recordemos que por la demostración del Teorema de Cauchy tenemos que

$$S_4 = cl((1234)) \cup cl((123)) \cup cl((12)(34)) \cup cl((12)) \cup cl(Id)$$

Aquí, hemos tomado un representante de cada clase para escribirla más cómodamente. Lo que dice la ecuación de arriba es que  $S_4$  está formado por todas las permutaciones de cada posible tipo que se puede dar en  $S_4$ .

- Nos preguntamos, por ejemplo, ¿cuántos elementos hay en  $C((1234))$ ? Para averiguarlo utilizaremos que  $[S_4 : cl((1234))] = |C((1234))|$ . El problema se reduce a averiguar  $|cl((1234))|$  puesto que ya sabemos que  $|S_4| = 4!$ .
  - En  $cl((1234))$  están todos los 4-ciclos. ¿Cuántos hay? Tenemos que ver de cuántas maneras distintas podemos escribir 4 números ( $i_1 i_2 i_3 i_4$ ) de manera que todas representen 4-ciclos diferentes.
  - Como una *rotación* de los números de un ciclo no cambia la permutación que describe (esto es,  $(1234) = (2341)$ ) lo que buscamos es, fijado un número, de cuántas maneras podemos ordenar los demás. Es decir, ¿de cuántas maneras podemos ordenar 3 números distintos? Pues de  $3! = 6$  maneras.
  - Por último nos queda ver qué valores pueden tomar los 4 números que escribimos en el ciclo. Pues tenemos disponibles 4 números para elegir (del 1 al 4) y tenemos que coger 4, así que solo hay una manera, o lo que es lo mismo, hay  $\binom{4}{4}$  maneras.
  - Concluimos que en  $cl((1234))$  hay  $3! \binom{4}{4} = 6 \cdot 1 = 6$  4-ciclos, y por tanto en  $C((1234))$  hay  $[S_4 : cl((1234))] = \frac{24}{6} = 4$  elementos.
- Ahora nos preguntamos lo mismo pero para los 3-ciclos, es decir, las permutaciones de tipo  $3 + 1$ . Procediendo de la misma manera obtenemos que el número de 3 ciclos es

$$|cl((123))| = \# \text{ elementos a ordenar} \times \# \text{ posibles valores} = (3 - 1)! \times \binom{4}{3} = 2! \cdot \frac{4!}{1!3!} = 8$$

$$\text{Con lo cual } |C((123))| = [S_4 : cl((123))] = \frac{24}{8} = 3$$

Podríamos seguir con el ejemplo anterior pero le daremos una vuelta más. En vez de pedir solo el orden del subgrupo  $C((12)(34))$  como nos tocaría si siguiéramos el orden lógico, pedimos los generados de ese subgrupo.

**Ejemplo 53.** Halla los generadores del subgrupo  $C((12)(34)) < S_4$ .

- Una buena manera de empezar, es preguntarse cuántos elementos hay en  $C((12)(34))$  y para ello necesitamos saber cuántos elementos hay en  $cl((12)(34))$ . Esta vez es un poco más complicado.
  - El número de posibles primeras parejas (primeros 2-ciclos) que podemos poner para obtener un elemento de tipo  $2 + 2$  es  $1! \times \binom{4}{2} = 6$ .
  - Observemos que al elegir la primera pareja queda determinada la segunda (solo hay 4 elementos para elegir).
  - Observemos también que al ser ciclos disjuntos, reordenaciones de estas dos parejas no dan permutaciones distintas. Dividimos entre 2.

- Queda que  $|cl((12)(34))| = 3$
- Una manera alternativa de pensar este caso es decir: fijo el 1 como primer elemento de la primera pareja. Para elegir el segundo solo me quedan 3 elementos y la segunda pareja me queda determinada en cuanto lo haga. Así que hay 3 permutaciones de tipo  $2 + 2$ .
- Finalmente tenemos que  $C((12)(34)) = \frac{24}{3} = 8$ . Ya sabíamos que  $\langle(12)(34)\rangle \subset C((12)(34))$  pero  $o((12)(34)) = 2$  luego con los elementos de  $\langle(12)(34)\rangle$  no tenemos suficientes para llenar  $C((12)(34))$ .
- Probamos con otros elementos  $\tau$  de  $S_4$  a ver si verifican  $\tau(12)(34)\tau^{-1} = (12)(34)$ :

$$\begin{aligned}\tau_1 &= (1234) & \tau_1(12)(34)\tau_1^{-1} &= (1234)(12)(34)(1234)^{-1} = (34)(12) = (12)(34) \\ \tau_2 &= (12) & \tau_2(12)(34)\tau_2^{-1} &= (12)(12)(34)(12)^{-1} = (34)(12) = (12)(34)\end{aligned}$$

De las ecuaciones anteriores tenemos que  $(1234) \in C((12)(34)) \wedge (12) \in C((12)(34))$ . Además, por clausura,  $\langle(1234)\rangle = \{(1234), (12)(34), (4321), Id\} \subset C((12)(34)) \wedge \langle(12)\rangle = \{(12), Id\} \subset C((12)(34))$ .

- Como  $|\langle(1234)\rangle \cap \langle(12)\rangle| = 1$  tenemos, por el teorema 43, que  $|\langle(1234)\rangle \times \langle(12)\rangle| = |\langle(1234), (12)\rangle| = 4 \cdot 2 = 8 = |C((12)(34))| \implies C((12)(34)) = \langle(1234), (12)\rangle$

**Ejemplo 54.** Halla los generadores del subgrupo centralizador del elemento  $(12)$  en  $S_4$

- $|C((12))| = [S_4 : cl((12))]$ . Obtenemos  $cl((12))$  de la manera habitual: número de 2-ciclos  $= (2-1)! \times \binom{4}{2} = 6$ . Por tanto  $|C((12))| = 24/6 = 4$ .
- Sabemos que  $\langle(12)\rangle \subset C((12))$  luego necesitamos otros dos elementos para rellenar  $C((12))$ .
- Pues vamos a probar a ver qué pasa con  $(34)$ :

$$(34)(12)(34)^{-1} = (12)(34)(34)^{-1} = (12) \implies (34) \in C((12)) \implies \langle(34)\rangle \subset C((12))$$

- Como en el ejemplo anterior aplicamos el teorema 43 y obtenemos que  $|\langle(12)\rangle \times \langle(34)\rangle| = |\langle(12), (34)\rangle| = \frac{|\langle(12)\rangle| |\langle(34)\rangle|}{|\langle(12)\rangle \cap \langle(34)\rangle|} = \frac{2 \cdot 2}{1} \implies C((12)) = \langle(12), (34)\rangle$

Recapitulando comprobamos que  $S_4$  se descompone en

- 6 4-ciclos (tipo 4),
- 8 3-ciclos (tipo  $3 + 1$ ),
- 3 2-ciclos + 2-ciclos (tipo  $2 + 2$ ),
- 6 2-ciclos (tipo  $2 + 1 + 1$ ), y
- 1 identidad o 1-ciclo (tipo  $1 + 1 + 1 + 1$ ).

En total suman 24 elementos.

## 5.6. Clases de equivalencia de subgrupos en $S_n$

Ahora haremos lo mismo que hemos hecho para permutaciones pero con subgrupos. Recordemos que el normalizador es lo mismo que el centralizador pero aplicado a subgrupos: el normalizador de un subgrupo son las permutaciones que mandan a un subgrupo en sí mismo mientras que en el caso del centralizador eran los elementos que mandan un elemento en sí mismo.

Conviene recordad la definición 25 y la proposición 68.

**Ejemplo 55.** Entender y copiar ejemplo pág 100 santorum

## 5.7. [Sub]grupos alternados

Recordemos que existía un homomorfismo de grupos  $S_n \rightarrow (\{-1, 1\}, \cdot)$  y que defíamos la paridad de una permutación  $\sigma \in S_n$  como par si  $\sigma \mapsto 1$  y como impar si  $\sigma \mapsto -1$ . Esto tenía sentido porque una permutación par se descomponía siempre en un número par de transposiciones y ocurría lo mismo con las permutaciones impares.

Pues resulta que nos interesa mucho el conjunto formado por las trasposiciones de orden par. Este conjunto es en realidad un subgrupo (recordar que la paridad se mantiene si operamos con trasposiciones de la misma paridad) y además veremos que es un subgrupo normal de  $S_n$ .

**Definición 32** (Grupo alternado). Sea  $\varphi : S_n \rightarrow (-1, 1, \cdot)$  el homomorfismo de grupos definido arriba. Definimos el grupo alternado o alternante  $A_n$  como

$$A_n = \ker \varphi = \{\sigma \in S_n \mid \sigma \text{ es par}\}$$

Recogemos los resultados que hemos dejado caer antes de la definición:

**Proposición 81.**  $A_n \triangleleft S_n$  y además  $[S_n : A_n] = 2$

**Corolario 8.** Todo grupo  $S_n$  tiene un subgrupo normal de orden 2.

Hay dos resultados más que aún no entiendo para qué sirven:

**Proposición 82.**

$$S_n/A_n \simeq (\{-1, 1\}, \cdot)$$

**Proposición 83.** Todo subgrupo normal de  $S_n$  se puede expresar como unión de cajas.

Pasado esto seguimos con nuestras vidas. Veamos ejemplos.

**Ejemplo 56.** Consideramos  $|S_5| = 5! = 120$ . Haciendo lo mismo que hicimos para  $S_4$  en la sección 5.5.1 obtenemos lo siguiente:

<b>tipo 5</b>	$ cl((12345))  = 4!\binom{5}{5} = 24$	$C((12345)) = \langle (12345) \rangle \simeq \mathbb{Z}/5\mathbb{Z}$
<b>tipo 4 + 1</b>	$ cl((1234))  = 3!\binom{5}{4} = 30$	$C((1234)) = \langle (1234) \rangle \simeq \mathbb{Z}/4\mathbb{Z}$
<b>tipo 3 + 2</b>	$ cl((123)(45))  = 2!\binom{5}{2} = 20$	$C((123)(45)) = \langle (123), (45) \rangle \simeq \mathbb{Z}/6\mathbb{Z}$
<b>tipo 3 + 1 + 1</b>	$ cl((123))  = 2!\binom{5}{2} = 20$	$C((123)) = \langle (123), (45) \rangle \simeq \mathbb{Z}/6\mathbb{Z}$
<b>tipo 2 + 2 + 1</b>	$ cl((12)(34))  = 15$	$C((12)(34)) = \langle (1234), (13) \rangle \simeq D_4$
<b>tipo 2 + 1 + 1 + 1</b>	$ cl((12))  = 1!\binom{5}{2} = 10$	$C((12)) = \langle (12345) \rangle \simeq H \times \mathbb{Z}/2\mathbb{Z}$
<b>tipo 1 + 1 + 1 + 1</b>	$ cl((1) = Id)  = 1$	$C(Id) = S_5$

Cuadro 5.1: Descomposición de  $S_5$  en clases. Nota: aquí  $H \simeq S_3$  o bien  $H = \{\sigma \in S_5 \mid \sigma(1) = 1 \wedge \sigma(2) = 2\}$

¿Cuáles son los tipos que estarían en  $A_5$ ? Pues aquellos que se puedan descomponer en un número par de trasposiciones. A saber: tipo 5, tipo 3 + 1 + 1, tipo 2 + 2 + 1, tipo 2 + 1 + 1 + 1. Por tanto en  $|A_5| = 24 + 20 + 15 + 1 = 60 \implies [S_5 : A_5] = 2 \implies A_5 \triangleleft S_5$ .

**Observación 2.** En  $S_n$  siempre hay un subgrupo isomorfo a  $D_n$ .

Lo construimos buscando un elemento  $B \in S_n$  de orden  $n$  (pista, el elemento  $(123 \dots n)$  siempre vale) y otro elemento  $A \in S_n$  de orden dos tal que  $BA = AB^{-1}$ . Con esto llegamos a la presentación de  $D_n$ . Ver ejemplo 7 para más detalles sobre esta presentación.

## 5.8. Grupos simples

**Definición 33** (Grupo simple). Sea  $G$  un grupo, decimos que  $G$  es un grupo simple si los únicos grupos normales son  $G$  y el grupo neutro  $\{e\}$ .

A continuación demostraremos que el grupo alternante  $A_n$ , es simple para  $n \geq 5$ . La demostración de este resultado requiere distintas proposiciones.

**Proposición 84.** Sea  $G$  un grupo. Si  $G$  es finito y abeliano  $\implies G$  es simple.

**Proposición 85.** Sea  $A_n$  un grupo alternante,  $A_n$  es generado por 3-ciclos para  $n \geq 3$ .

*Demostración.* Sea  $\sigma \in A_n$ , entonces  $\sigma = (i_1^1 i_2^2)(i_1^2 i_2^2) \dots (i_1^{2n} i_2^{2n})$  una composición de un número par de composiciones.

Vamos a ver que para cualquier par de transposiciones  $(i\ j)(k\ l)$  podemos expresarla como un 3 – ciclo.

$$\begin{aligned} (i\ j)(k\ l) &= (i\ k\ j)(i\ k\ l) && \text{si los elementos son diferentes.} \\ (i\ j)(i\ l) &= (i\ l\ j) && \text{si tienen un elemento en comun.} \end{aligned}$$

Por tanto, como  $\forall \sigma \in A_n$  puede ser expresado como un 3 – ciclo o una composición de estos,  $A_n$  está generado por los ciclos de longitud 3. ♣

**Proposición 86.** Sea  $A_n$  el grupo alternante de un conjunto de  $n$  elementos,  $A_n$  es generado por 3-ciclos de la forma  $(s\ t\ i)$  con  $s, t \in \{1 \dots n\}$  fijos e  $i \in \{1 \dots n\} \setminus \{s, t\}$

*Demostración.* Cada 3-ciclo es el producto de 3-ciclos del tipo  $(s\ t\ i)$  con  $s, t$  fijos e  $i$  variable, pues:

$$\begin{aligned} (s\ a\ t) &= (s\ t\ a)^2 \\ (s\ a\ b) &= (s\ t\ b)(s\ t\ a)^2 \\ (t\ a\ b) &= (s\ t\ b)^2(s\ t\ a) \\ (a\ b\ c) &= (s\ t\ a)^2(s\ t\ c)(s\ t\ b)^2(s\ t\ a) \end{aligned}$$

Entonces, como  $A_n$  está generado por 3-ciclos,  $A_n$  está generado por ciclos de la forma  $(s\ t\ i)$  ♣

**Teorema 87** (Igualdad entre subgrupos y grupos alternantes). Si un subgrupo normal  $H$  de  $A_n$  contiene un 3-ciclo  $\implies H = A_n$

*Demostración.* Supongamos que  $H$  es no trivial y contiene un 3-ciclo de la forma  $(s\ t\ a)$ . Usando la normalidad de  $H$  vemos que:

$$[(s\ t)(a\ i)](s\ t\ a)^2[(s\ t)(a\ k)]^{-1} = (s\ t\ i)$$

está en  $H$ . Luego,  $H$  debe contener todos los ciclos  $(s\ t\ i)$  para  $1 \geq i \geq n$ . Por la proposición 86, estos 3-ciclos generan  $A_n$ ; luego  $H = A_n$ . ♣

**Proposición 88.** Para  $n \geq 5$ , todo  $H \triangleleft A_n$  contiene un 3-ciclo.

*Demostración.* Sea  $e \neq \sigma \in H$ , existen varias posibles estructuras de ciclos para  $\sigma$ .

- $\sigma$  es un 3-ciclo.
- $\sigma$  es el producto de ciclos disjuntos,  $\sigma = \tau(a_1\ a_2 \dots a_r) \in H$ , con  $r \geq 3$ .
- $\sigma$  es el producto de ciclos disjuntos,  $\sigma = \tau(a_1\ a_2\ a_3)(a_4\ a_5\ a_6)$ .
- $\sigma = \tau(a_1\ a_2\ a_3)$ , donde  $\tau$  es el producto de 2-ciclos disjuntos.
- $\sigma = \tau(a_1\ a_2)(a_3\ a_4)$ , donde  $\tau$  es el producto de un número par de 2-ciclos disjuntos.

La demostración sigue con el desarrollo de cada uno de los casos, utilizando la normalidad de  $H$  para ver que en todos los casos se llega a que  $H$  contiene un 3-ciclo. ♣

**Teorema 89** (Simplicidad del grupo alternante). Sea  $(A_n, \circ)$  el grupo alternante de un conjunto de  $n$  elementos.  $A_n$  es simple  $\forall n \geq 5$ .

*Demostración.* Sea  $H$  un subgrupo normal no trivial de  $A_n$ , por la proposición 88,  $H$  contiene un 3-ciclo. Por el teorema 87,  $H = A_n$ ; por tanto,  $A_n$  no contienen ningún subgrupo normal que sea propio y no trivial para  $n \geq 5$ . ♣



# Capítulo 6

## Teoremas de Sylow

### 6.1. Nuevas estructuras de grupo en el producto directo

Sean  $G_1, G_2$  grupos, queremos definir nuevas estructuras de grupo en el producto  $G_1 \times G_2$ . Para ello comenzaremos definiendo una operación  $*_\alpha$ . Fijamos un homomorfismo de grupos  $\alpha : G_2 \longrightarrow \text{Aut}(G_1)$ , con  $\text{Aut}(G_1)$  el grupo de automorfismos de  $G_1$ .

Sean  $(a, b), (c, d) \in G_1 \times G_2$ , definimos  $*_\alpha$  como:

$$(a, b) *_\alpha (c, d) = (a \cdot \alpha(b) \cdot c, b \cdot d).$$

Donde  $b \in G_2$ ,  $\alpha(b) \in G_1$  y  $\alpha(b) \cdot c \in G_1$ .

Vamos a ver que  $(G_1 \times G_2, *_\alpha)$  es un grupo.

**Teorema 90** (Grupo producto semidirecto).  $(G_1 \times G_2, *_\alpha)$  es un grupo.

Vamos a demostrar cada una de las propiedades del grupo:

- Asociatividad.

*Demostración.*

$$\begin{aligned}(a \cdot \alpha(b) \cdot c, bd) *_\alpha (h, f) &= (a \cdot \alpha(b) \cdot c \cdot \alpha(bd) \cdot h, b \cdot d \cdot h) \\ (a, b) *_\alpha (c \cdot \alpha(d) \cdot h, df) &= (a \cdot \alpha(b) \cdot c \cdot \alpha(d) \cdot h, b \cdot d \cdot h)\end{aligned}$$

Entonces, falta ver que  $\alpha(d) \cdot h = \alpha(bd) \cdot h$ . Definimos el isomorfismo de grupo:

$$\begin{aligned}\alpha(b) : G_1 &\longrightarrow G_1 \\ c &\longmapsto \alpha(b) \cdot c \\ \alpha(d) \cdot h &\longmapsto \alpha(b) \cdot (\alpha(d) \cdot h) = \alpha(bd) \cdot h.\end{aligned}$$

Por tanto, son iguales y la operación es asociativa. ♣

- Existencia del elemento neutro.

*Demostración.* Sean  $e_1$  y  $e_2$  elementos neutros de  $G_1$  y  $G_2$  respectivamente. Recordamos que por el argumento anterior  $\alpha(b) \cdot e_1 = e_1$ .

$$(a, b) *_\alpha (e_1, e_2) = (a \cdot \alpha(b) \cdot e_1, b \cdot e_2) = (a, b)$$

♣

- Existencia del inverso.

*Demostración.* Hemos de hallar  $(c, d) \mid (a, b) *_\alpha (c, d) = (e_1, e_2)$ . Entonces, hemos de hallar  $c$  y  $d$  tal que:

$$\begin{aligned}a \cdot \alpha(b) \cdot c &= e_1 \\ b \cdot d &= e_2\end{aligned}$$

Es fácil ver que  $\exists d$  y  $d = b^{-1}$ . Como  $\alpha(b)$  es un isomorfismo  $\implies \exists(\alpha(b))^{-1}$ , entonces,  $c = \alpha(b^{-1}) \cdot a^{-1} = a^{-1}$ , por tanto  $\exists c$  y  $c = a^{-1}$ . ♣

Por tanto, el par  $(G_1 \times G_2, *_\alpha)$  tiene estructura de grupo.

Vamos a ver ahora ciertas relaciones del producto cruz con la operación que acabamos de definir. Para abreviar, al par  $(G_1 \times G_2, *_\alpha)$  lo denominaremos por  $G_1 \times_\alpha G_2$ .

Sean  $G_1, G_2$  grupos finitos, definimos:

$$\begin{aligned}\underline{G_1} &= \{(a, e_2) \mid a \in G_1\} \\ \underline{G_2} &= \{(e_1, b) \mid b \in G_2\}\end{aligned}$$

Es fácil ver que  $\underline{G_1} < G_1 \times_\alpha G_2$  y  $\underline{G_2} < G_1 \times_\alpha G_2$ . Además,

$$\begin{aligned}|\underline{G_1} \cdot \underline{G_2}| &= \frac{|\underline{G_1}| \cdot |\underline{G_2}|}{|\underline{G_1} \cap \underline{G_2}|} = \frac{|\underline{G_1}| \cdot |\underline{G_2}|}{1} = |G_1| \cdot |G_2| = |G_1 \times_\alpha G_2| \\ \underline{G_1} \cap \underline{G_2} &= (e_1, e_2)\end{aligned}$$

Y podemos probar que  $\underline{G_1}$  es normal, sean  $g_1 \in G_1$  y  $g_2 \in G_2$ :

$$(g_1, g_2) *_\alpha (a, e_2) *_\alpha (g_1, g_2)^{-1} = (g_1, g_2) *_\alpha (\dots, e_2 \cdot g_2^{-1}) = (\dots, e_2).$$

**Corolario 9.** Por lo que acabamos de ver:

- $\hat{G}_1$  y  $\hat{G}_2$  son subgrupos.
- $\hat{G}_1$  es normal.
- $\underline{G_1} \cap \underline{G_2} = \{(e_1, e_2)\}$
- $\underline{G_1} \cdot \underline{G_2} = G_1 \times_\alpha G_2$

Si ahora tomamos  $G_1 = N, G_2 = H$  con  $N \triangleleft G, H < G$ , entonces:

- $H \cap N = \{e\}$
- $H \cdot N = G$
- $\alpha : H \longrightarrow \text{Aut}(N)$
- $G \cong H \times_\alpha N$

En particular, podemos definir:

$$\begin{aligned}\phi : H &\longrightarrow \text{Aut}(N) \\ h &\longmapsto \gamma_h|_N (n) = h \cdot n \cdot h^{-1}\end{aligned}$$

**Ejemplo 57.** Sea el famoso grupo  $D_4 = \{1, B, B^2, B^3, A, AB, AB^2, AB^3\}$  (ver ejemplo 6). Tomamos  $N = \langle B \rangle = \{1, B, B^2, B^3\}$ ,  $H = \langle A \rangle = \{1, A\}$ . Entonces:

$$\begin{aligned}\phi : H &\longrightarrow \text{Aut}(N) \\ A &\longmapsto ABA^{-1} = B^3\end{aligned}$$

Entonces como hemos visto:  $D_4 \cong \{1, A\} *_\phi \{1, B, B^2, B^3\}$ .

## 6.2. Producto semidirecto

De [DH96]

Sea  $G$  un grupo. Sea  $N \triangleleft G, H < G, N \cap H = \{e\}$  y  $NH = G$  (recordemos que por ser  $N$  normal,  $NH$  es grupo). Entonces  $G \simeq N \times H$ .

Veamos quién es ese isomorfismo  $\gamma : G \rightarrow N \times H$ . Recordemos que considerando dos grupos  $G_1, G_2$  y su producto directo  $G_1 \times G_2$  existe un  $\alpha : G_2 \rightarrow \text{Aut}(G_1)$ . Veremos quien es este  $\alpha$  para  $H$  y  $N$ , es decir, quién es  $\alpha : H \rightarrow \text{Aut}(N)$ .

Construye  $\alpha$  a partir de 4 isomorfismos.

*Demostración.*

- Comenzamos por definir una función  $j : N \times H \rightarrow G$ ,  $(n, h) \mapsto nh$ . Es función está bien definida por teoría de conjuntos pero no es un homomorfismo de grupos<sup>12</sup>.
- Recordemos que por el teorema 43 tenemos que  $|G| = |N||H| = |N \times H|$  por ser  $N \cap H = \{e\}$ .
- Volviendo a lo de la estructura especial. Dar una estructura especial es dar una operación para  $N \times H$ .
  - Sea  $A$  un conjunto. Es claro que si tenemos una biyección  $\phi : A \rightarrow G$  podemos dotar a  $A$  de alguna estructura para que sea un grupo.
  - Para dotar a  $A$  de estructura tenemos que definir la operación. Forzamos que para cada  $a, a' \in A$  para los que se tiene  $\phi(g) = a, \phi(g') = a'$  la operación sea  $aa' = \phi(gg')$ .
  - En este caso nuestro  $A$  es  $N \times H$ . En lugar de utilizar la operación habitual del producto directo definimos otra operación. Para llegar a ella nos fijamos en  $(n, h)(n', h') \mapsto nhn'h' = nhn'h^{-1}hh' = n(hn'h^{-1})hh' = nn'hh'$  (intercalamos el neutro, que es legal).
  - Redefinimos la operación en  $N \times H$  para que cuadre con este resultado. Llamaremos al nuevo grupo con la nueva operación  $N \times_{\phi} H$ : para  $(n, h), (n', h')$  definimos  $(n, h) \cdot (n', h') = (n(hn'h^{-1}), hh')$ .
  - Comprobamos que en este caso  $j$  es un homomorfismo de grupos:

$$\begin{aligned} j : N \times_{\phi} H &\rightarrow G \\ (n, h) &\mapsto nh \\ (n', h') &\mapsto n'h' \\ (n, h) \cdot (n', h') &\mapsto n(hn'h^{-1})hh' = nn'hh' \end{aligned}$$



Es muy interesante por que es muy natural llegar a situaciones de esta manera. ¡Y les voy a dar una!<sup>3</sup>

**Ejemplo 58.** Sea  $|G| = p \cdot q$  y supongamos  $p < q$  primos. Por el teorema de Lagrange (23) tenemos que existe un subgrupo  $H_p < G$  con  $|H_p| = p$  y análogamente  $\exists H_q \mid |H_q| = q$ . A primera vista podríamos pensar que puede haber varios grupos de orden  $q$ . Pues no.

*Demostración.* Supongamos hay dos grupos  $H, H'$  de orden  $q$  distintos. La intersección tiene que dar un subgrupo y si los dos grupos tienen un número primo de elementos entonces la intersección solo puede ser el neutro,  $H \cap H' = \{e\}$ . Entonces por el teorema 43 tenemos que  $|HH'| = q^2 > p \cdot q$  lo que es imposible. Luego sabemos que a lo sumo hay un grupo de orden  $q$ .



(Sigue el ejemplo) Supongamos que ese único grupo de orden  $q$  se llama  $N$ . Entonces  $\phi_g(N) = N$  ya que un isomorfismo tiene que mandar un subgrupo de  $q$  elementos en otro subgrupo de  $q$  elementos y  $N$  es el único. Por tanto  $N \triangleleft G$ . Aplicando el teorema de antes, tenemos que  $G \cong N \times H$ .

**Ejemplo 59.** Veamos un ejemplo con más pinta de problema. Demostrar que todo grupo de orden 77 es cíclico.

*Demostración.* Comenzamos por observar que  $77 = 7 \cdot 11$ . Por el teorema de Lagrange (23) tenemos que existen  $H, N < G \mid |H| = 7, |N| = 11$  y por lo visto en el ejemplo anterior,  $N \triangleleft H$ . Como antes llegamos a que  $H \cap N = \{e\}$  y a que  $|HN| = pq$ . Para aplicar el teorema anterior vemos qué estructura tiene que tener  $N \times_{\phi} H$ , con  $\phi : H \rightarrow \text{Aut}(N)$ .

Vemos que  $\text{Aut}(N) = \text{Aut}(\mathbb{Z}/11\mathbb{Z}) = \mathcal{U}(\mathbb{Z}/11\mathbb{Z}) = \mathbb{Z}/10\mathbb{Z}$ , es decir, un grupo cíclico de 10 elementos.

Entonces,  $\phi$  es de la forma:  $H = \mathbb{Z}/7\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/11\mathbb{Z})$ , por tanto, solo podemos definir el homomorfismo de grupos trivial. Esto hace que  $N \times_{\phi} H$  es igual a  $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ .

Por el corolario 9 sabemos que  $G \cong N \times_{\phi} H \implies G \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$  que es cíclico por ser producto de cíclicos de órdenes coprimos.



<sup>1</sup>Ojo con por qué no es homomorfismo. Si tomamos  $(n, h), (n', h') \in N \times H$  tenemos que  $j((n, h)(n', h')) = nn'hh'$ . Podríamos pensar que como  $N$  es normal, podemos conmutarlo y obtener  $nn'hh' = nhn'h' = j((n, h))j((n', h'))$ . **Pero esto está mal.** Lo que significa ser normal es que para  $h \in H$ , se tiene que  $nh = hn''$  para algún  $n'' \in N$ .

<sup>2</sup>Si los grupos son abelianos entonces sí es claro que es un homomorfismo. Lo que vamos a hacer es ver que dando una estructura especial, sí que es un homomorfismo de grupos incluso para grupos no abelianos

<sup>3</sup>Sugerencia: léelo con voz de tomatito.

### 6.3. Teoremas de Sylow

Son muchos teoremas para grupos finitos en los que el orden se puede expresar como

$$|G| = p^s m, \text{ mcd}(p, m) = 1, s \geq 1 \quad (6.1)$$

Veremos y discutiremos 3 de ellos. Sirven sobre todo para contar cosas.

**Definición 34** (P-subgrupo de Sylow). Dado  $G$  con  $|G| = p^s m$  con  $\text{mcd}(p, m) = 1$ ,  $s \geq 1$ , un p-subgrupo de Sylow de  $G$  es un subgrupo  $P < G$  con  $|P| = p^s$ .

**Teorema 91** (Primero de Sylow). Sea  $G$  un grupo tal que  $|G| = p^s m$ ,  $\text{mcd}(p, m) = 1$ ,  $s \geq 1$ ,  $p$  primo. Entonces existe un p-subgrupo de Sylow  $H_1 < G$  con  $|H_1| = p^s$ .<sup>a</sup>

<sup>a</sup>Este teorema es el recíproco de algo que ya sabíamos. Podíamos afirmar que si  $P < G$  y  $|P| = p^s$  entonces  $p^s$  dividía a  $|G|$ . Lo que dice el primer teorema de Sylow es que el recíproco es cierto.

El teorema de Cauchy (60) es una versión más débil de este primer teorema de Sylow.

**Teorema 92** (Segundo de Sylow). Sea  $G$  grupo con  $|G| = p^s m$ ,  $\text{mcd}(p, m) = 1$ ,  $s \geq 1$ . Sea  $P$  un p-subgrupo de Sylow fijado. Si  $Q$  es un p-subgrupo de Sylow de  $G$  entonces  $\exists g \in G \mid Q \subset gPg^{-1}$ .

**Teorema 93** (Tercero de Sylow). Sea  $F = \{gPg^{-1} \mid g \in G\} = \{P = P_1, \dots, P_{n_p}\}$  el conjunto de p-subgrupos de Sylow de  $G$ . Entonces  $n_p$  divide a  $m$  y  $n_p \equiv 1 \pmod{p}$ .

Hemos hecho mucho hincapié en los subgrupos normales y tenemos que si  $N \triangleleft G$  entonces existe  $\pi : G \rightarrow G/N$  homomorfismo de grupos<sup>4</sup>. Además teníamos que  $|G| = |G/N| \cdot |N|$ .

También establecíamos una biyección entre los submódulos de  $G$  que contienen a  $N$  y los submódulos de  $G/N$ . Si  $K$  es uno de ellos entonces  $N \triangleleft K \implies N \triangleleft K$ ,

$$\begin{aligned} K/N &= \overline{K} \subset K/N \\ |K| &= |\overline{K}| |N| \end{aligned}$$

Vamos a discutir el teorema. Recordemos que dado  $G$  el centro  $Z(G)$  es el conjunto de los elementos que conmutan con todos (ver definición 22). Recordamos además las proposiciones 52 y 53 que nos dicen que el centro es normal y que cualquier subgrupo del centro es abeliano y normal. El centro está bien pero tampoco es para tanto: suele ser muy pequeño. WTF.

Aquí en medio ha desvariado bastante, remontándose hasta el teorema 37.

*Demostración del teorema de Sylow.* Procedemos por inducción [fuerte] en  $|G|$ .

- Si  $|G| = 1$  no hay mucho que probar porque son grupos muy tontos.
- Suponemos que<sup>5</sup> el teorema es válido para  $|G| < n$ . Distinguimos los siguientes casos:
  1.  $|Z(G)| = 0$
  2.  $|Z(G)| \neq 0$ . Entonces  $Z(G)$  es un grupo abeliano no trivial. Es decir que  $Z(G) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_t\mathbb{Z}$ . Como  $p$  divide a  $|Z(G)|$  podemos suponer que  $p$  divide a  $n_1$ . Entonces  $(\overline{n_1/p}) \in \mathbb{Z}/n_1\mathbb{Z}$  y por tanto

$$\left( \left( \frac{n_1}{p} \right), \overline{0}, \dots, \overline{0} \right) \text{ tiene orden } p$$

Es decir que tenemos un  $H < Z(G)$  con  $|H| = p$ .

Teníamos de antes que  $|G/H||H| = |G|$ . Por inducción existe  $\overline{K} < G/H$  de orden  $p^{s-1}$ . Aplicamos  $|K| = |\overline{K}||H|$  y como  $|H| = p$ ,  $|\overline{K}| = p^{s-1}$  tenemos que  $|H| = p^s$ .

<sup>4</sup>Por teoría de conjuntos tenemos que  $\pi$  es una función que existe y está bien definida, pero aquí interesa que además es homomorfismo.

<sup>5</sup>[La clase en silencio]. Orlando: Se pueden callar por favor. [El silencio se hace más hueco]. Orlando: No hagan ruiditos. Me cuesta concentrarme [agita las manos]. [Sigue la demostración.]

Lo hemos probado para una hipótesis en concreto pero falta algo (no sé el qué). Seguimos con la demostración.

$$|G| = |Z(G)| + [G : C(a_{s+1})] + \cdots + [G : C(a_r)]$$

$|G|$  es no nulo módulo  $p$  y  $|Z(G)|$  es nulo módulo  $p$ , por lo que necesariamente tiene que ocurrir que alguno de los  $[G : C(a_i)]$  sea no nulo módulo  $p$ . Supongamos que es el primero, es decir, supongamos que  $[G : C(a_{s+1})]$  es no nulo módulo  $p$ . Además tenemos que

$$\underbrace{|G|}_{p^s m} = \underbrace{|C(a)|}_{p^s m'} \cdot \underbrace{[G : C(a)]}_{\text{no divisible por } p}$$

Como  $[G : C(a)] \geq 2$ ,  $|C(a)| = p^s m' < |G|$  por inducción el subgrupo  $C(a_{s+1})$  tiene un subgrupo de orden  $p^s$ . ♣

**Ejemplo 60.** Supongamos  $|G| = 2^2 \cdot 11 \cdot 13$ . Por el teorema de Sylow tenemos que existen subgrupos  $P_2, P_{11}, P_{13} < G$  con órdenes  $|P_2| = 2^2$ ,  $|P_{11}| = 11$ ,  $|P_{13}| = 13$ . Sin embargo no podemos garantizar que exista un  $Q$  con orden  $|Q| = 2^2 \cdot 13$ . Si ocurriera esto sería buenísimo porque existiría un  $P < G$  con  $P \cap Q = \{e\}$  y por tanto  $P \cdot Q = G$  y automáticamente  $G \simeq P \rtimes Q$ . Esto no ocurre porque en general no sabemos si  $P_2$  y  $P_{13}$  son normales y por tanto no podemos garantizar que  $Q = P_2 \cdot P_{13}$  sea siquiera un grupo.

Lo interesante del ejemplo anterior es que si tenemos  $G$  descompuesto como producto directo de dos grupos y uno de ellos es normal, entonces tenemos automáticamente un producto semidirecto. Sin embargo, si tenemos  $G$  descompuesto en 3 grupos, no basta con que uno sea normal, sino que tienen que ser normales 2. Supongamos  $G$  se descompone en  $P, Q, R$ . Necesitamos que  $P$  sea normal para que  $P \cdot Q$  sea grupo. Y necesitamos que  $R$  sea normal para que  $(P \cdot Q) \cdot R$  sea también un grupo y podamos dar un producto semidirecto.

Resultado muy fuerte que hay que saber probar.

**Teorema 94.** Sea  $G$  un grupo,  $H_1, H_2 \triangleleft G \wedge H_1 \cap H_2 = \{e\}$ . Entonces  $\forall h_1 \in H_1, h_2 \in H_2$  se tiene que  $h_1 h_2 = h_2 h_1$ .

*Demostración.* Probaremos que  $h_1 h_2 h_1^{-1} h_2^{-1} = e$ . Para ello probaremos que  $h_1 h_2 h_1^{-1} = h_2$ . Sabemos que por ser  $H_2 \triangleleft G$  tenemos que  $h_1 H_2 h_1^{-1} = H_2$ . Es decir, que  $h_1 h_2 h_1^{-1} \in H_2$ . Si multiplicamos a la derecha por  $h_2^{-1} \in H_2$  nos sigue quedando un elemento de  $H_2$ :  $h_1 h_2 h_1^{-1} h_2^{-1} \in H_2$ . Para  $H_1$  tenemos lo mismo:  $h_2 h_1 h_2^{-1} h_1^{-1} \in H_1$ . Por alguna razón estos dos elementos son el mismo y como pertenece a ambos subgrupos entonces pertenece a la intersección y por tanto  $h_1 h_2 h_1^{-1} h_2^{-1} = e$ . ♣

**Ejemplo 61.** Consideramos  $D_4$  que es un  $p$ -grupo pues  $|D_4| = 2^3$ . En este caso el centro no es el trivial:  $Z(D_4) = \{1, B^2\}$ .

**Ejemplo 62.** Consideramos  $H$  (el grupo de cuaterniones, ejemplo 5, y su retículo, figura ??) que también es un  $p$ -grupo pues  $|H| = 2^3$ . El retículo de este grupo es extraño y volvemos a tener que  $Z(H) = \{1, B^2\}$ .

**Ejemplo 63.** Si  $G$  es un  $p$ -grupo con  $|G| = p^s$  entonces  $G$  tiene subgrupos de orden  $1, p, p^2, \dots, p^s$ .

*Demostración.* Procedemos por inducción en  $s$ . Para  $s = 1$  es trivial: el subgrupo es el propio  $G$ .

Supongamos que  $|Z(G)| = p^{s'}$  con  $s' \leq s$ . Sabemos que  $Z(G) \triangleleft G$  y además todo subgrupo de  $Z(G)$  es normal en  $G$ .  $\exists \alpha \in Z(G) \mid o(\alpha) = p$ . Tenemos que  $\langle \alpha \rangle < Z(G)$  y por tanto  $\langle \alpha \rangle \triangleleft G$ . Consideramos ahora  $G \rightarrow G/\langle \alpha \rangle$ . Tenemos que  $|G/\langle \alpha \rangle| = p^{s-1}$ . ♣

**Ejemplo 64** (de aplicación de los teoremas de Sylow). Sea  $G$  con  $|G| = 3 \cdot 5$ .

- Tenemos por el primer teorema de Sylow (91) que existen  $P_3, P_5 < G$  con  $|P_3| = 3$ ,  $|P_5| = 5$  (aplicamos el teorema dos veces primero cogiendo  $p = 3$  y luego  $p = 5$ ).
- Tenemos también que  $P_3 \cap P_5 = \{e\}$  ya que los elementos de  $P_3$  tienen orden que divide a 3 y los elementos de  $P_5$  orden que divide a 5, por tanto, los elementos de la intersección tienen que tener orden que divida a 3 y a 5 por lo que solo puede ser el neutro.
- Como  $P_3 \cap P_5 = \{e\}$  sabemos por el teorema 43 que  $P_3 P_5$  tiene 15 elementos. Si fuéramos capaces de probar que alguno de ellos es normal tendríamos un producto semidirecto.
  - Aplicamos el tercer teorema de Sylow (93) para averiguar quién es  $n_3$  (el número de 3-subgrupos de Sylow en  $G$ ). Tomamos  $|G| = 3^1 \cdot 5$  (cogemos  $p = 3$ ,  $m = 5$ ). Entonces  $n_3 \in \{1, 5\}$  pues  $n_3$  tiene que dividir a  $m = 5$ . Además  $n_3 \equiv 1 \pmod{3} \implies n_3 \in \{1, 4, 7, \dots\}$ . Concluimos que  $n_3 = 1$ .
  - De aquí concluimos que el único conjugado de  $P_3$  es  $P_3$  (solo hay un 3-subgrupo de Sylow en 3, es decir,  $\{g P_3 g^{-1} \mid g \in G\} = \{P_3\} \implies g P_3 g^{-1} = P_3, \forall g \in G \implies g P = P g, \forall g$ ) luego  $P_3 \triangleleft G$ .<sup>6</sup>

<sup>6</sup>Orlando: *Esto es buenísimo!* [Se alegra muchísimo de lo que acaba de probar.]

- Hacemos lo mismo con  $n_5$  y obtenemos que  $n_5 = 1$  y concluimos que  $P_5 \triangleleft G$ .
- No solo uno de ellos es normal, sino que los dos son normales. Tenemos un producto semidirecto y concluimos que  $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ .

**Ejemplo 65.** Hacemos lo mismo con un grupo  $G$  que tiene  $|G| = 2 \cdot 7$ .

- Del primer teorema de Sylow (91) tenemos que  $\exists P_2, P_7 < G$  con órdenes  $|P_2| = 2$ ,  $|P_7| = 7$ .
- Es claro que  $P_7$  tiene que ser normal (de dibujarlo) pero aún así supongamos que no sabemos contar y somos creyentes de los teoremas de Sylow, veamos que  $P_7$  es normal.
  - Obtenemos  $n_7$  del tercer teorema:

$$\begin{cases} n_7 \text{ divide a } 2 \\ n_7 \equiv 1 \pmod{7} \end{cases} \implies n_7 = 1$$

- Análogamente obtenemos que  $n_2 = 1$ .
- Volvemos a tener dos subgrupos normales y tenemos que  $|P_2 \cdot P_7| = 2 \cdot 7$  (con un razonamiento análogo al de antes) de lo que obtenemos un producto semidirecto y por tanto  $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ .

**Ejemplo 66.** Consideramos el grupo  $S_4$  que tiene orden  $|S_4| = 4! = 4 \cdot 3 \cdot 2 = 2^3 \cdot 3$ .

- Del primer teorema de Sylow obtenemos que  $\exists P_2, P_3 < S_4$  con  $|P_2| = 8$ ,  $|P_3| = 3$ .
- ¿Será  $S_4$  un producto semidirecto? ¿Será  $P_2$  o  $P_3$  un subgrupo normal?
  - Veamos quien es  $n_3$ . Por el tercer teorema de Sylow (93) tenemos que  $n_3$  divide a  $m = 8$  y que  $n_3 \equiv 1 \pmod{p = 3}$ . Con estas condiciones tenemos que  $n_3$  puede ser o bien 1 o bien 4.  
Recordemos que  $\sigma \in S_4 \wedge o(\sigma) = 3 \iff \sigma$  es un ciclo de longitud 3. Y recordemos que en  $S_4$  había 8 ciclos de longitud 3. Entonces tenemos que  $n_3$  no puede ser 1 ya que en tal caso  $P_3 \triangleleft S_4$  y por tanto en  $S_4$  habría solo 2 ciclos de orden 3 resulta que hay ocho. Concluimos que  $n_3 = 4$ .<sup>7</sup>
  - Veamos quien es  $n_2 = \{gP_2g^{-1} \mid P\} = \{P_2 = P_2^{(1)}, \dots, P_2^{(n_2)}\}$ . Por el tercer teorema de Sylow (93) tenemos que  $n_2$  divide a  $m = 3$  y que  $n_2 \equiv 1 \pmod{p = 2}$ . Con estas condiciones tenemos que  $n_2$  puede ser o bien 1 o bien 3.  
Para  $n_2 = 1$  tendríamos que  $P_2 \triangleleft S_4$  y por tanto todos los elementos de orden par tendrían que vivir en  $P_2$ . De orden 2 hay 6 elementos y de orden 4 hay otros 6, es decir, que en  $P_2$  que es un grupo de orden 8, viven al menos  $6 + 6 = 12$  con lo cual llegamos a una contradicción. Por lo que necesariamente  $n_2 = 3$ .
- Pues no, ninguno de los p-subgrupos de Sylow que encontramos es normal.
- No hemos conseguido un producto semidirecto, pero vamos a probar que  $P_2 \simeq D_4$  (y por extensión todos sus conjugados porque tenemos el isomorfismo de conjugación entre ellos). Para eso, haremos una presentación de  $P_2$  análoga a la de  $D_4$  (ver ejemplo 6).
  - Tomamos  $A = (13), B = (1234)$ . ¿Por qué? Por el contexto geométrico de  $D_4$  que se puede ver en el ejemplo 6. Recordemos que la  $A$  es la simetría y  $B$  es el giro.
  - Vemos que todo funciona y que la presentación queda igual que la de  $D_4$ .

Cogemos un grupo de Sylow  $|G| = p^s \text{mmcd}(m, p) = 1, s \geq 1$ . Tenemos para el  $F$  del segundo tercer teorema de Sylow que  $|F| = |F_1| + |F_2| + \dots + |F_l|$  donde cada  $F_j = \{qP_{i_j}q^{-1} \mid q \in Q\}$  y  $|F_j| = [Q : N_Q(P_{i_j})]$ .

**Proposición 95.** Si  $Q$  es un p-subgrupo de Sylow y  $P'$  es un p-subgrupo de Sylow entonces el normalizador de  $P'$  en  $Q$  es

$$N_Q(P') = P' \cap Q$$

De aquí obtenemos que  $|F_j| = [Q : N_Q(P_{i_j})] = [Q : Q \cap P_{i_j}]$ . Como  $Q, P_{i_j}$  son p-subgrupos tienen órdenes que son potencias de  $p$  por lo que  $|F_j|$  es cociente de potencias de  $p$  y por tanto es potencia de  $p$ .

**Observación 3** (para la prueba del tercer teorema de Sylow).  $n_p \equiv 1 \pmod{p}$

*Demostración.* En particular, tomamos  $P = Q$ . En este caso, la clase de  $P$ ,  $F_1 = \{pPp^{-1} \mid p \in Q = P\} = \{P\}$ .  $|F_2| = [Q : N_Q(P_{i_2})] = [P : P \cap P_{i_2}] = p_{r_2}$  porque  $P$  y  $P_{i_2}$  no son iguales. ♣

**Observación 4.** Si  $Q$  es un p-subgrupo de Sylow de  $G$  entonces  $Q \subset gPg^{-1}$  para algún  $g \in G$ .

<sup>7</sup>Efectivamente, de entre los 8 ciclos de longitud 3 que hay en  $S_4$  salen 4 parejas que viven cada una en uno de los conjugados de  $P_3$ .

*Demostración.* Procedemos por refutación: supongamos que  $Q \nsubseteq F$ . Recordemos que

$$|F| = |F_1| + |F_2| + \cdots + |F_s| \quad |F_k| = [Q : Q \cap P_{i_j}]$$

Si afirmamos que  $Q \nsubseteq Q$  entonces  $|F_j|$  tiene que ser un múltiplo de  $p$  ya que al hacer la intersección  $Q \cap P_{i_j}$  obtenemos un conjunto propio. De este modo,  $|F| = \sum |F_j|$  también es un múltiplo de  $p$ . La contradicción llega con la observación anterior, ya que  $|F| \equiv 1 \pmod{p}$ . ♣

Lo interesante de verdad es el corolario que obtenemos de esta observación:

**Corolario 10.**  $F$  es el conjunto de todos los subgrupos de Sylow de  $G$ .

**Observación 5.** Por último probaremos que  $n_p \mid m$ .

*Demostración.*  $F = \{gPg^{-1} \mid g \in G\}$  y tenemos que  $|F| = [G : N_G(F)] \wedge |G| = p^s m \wedge P \subset N(P)$ . Además

$$\underbrace{|G|}_{p^s m} = \underbrace{|P|}_{p^s} \underbrace{[G : P]}_m$$

Ahora  $P \subset N(P)$  y también  $|G| = |N(P)[G : N(P)]$ . ♣

**Ejemplo 67.** Consideramos  $|S_5| = 5! = 5 \cdot 4!$  tomamos  $p = 5, m = 4!, s = 1$ .

- Por el primer teorema tenemos que existen subgrupos de orden  $p^s = 5$ . Esto ya lo sabíamos.
- De hecho hasta sabíamos que había  $4! = 24$  ciclos de longitud 5. Como  $p = 5$  es un número primo, los subgrupos de orden 5 no tienen elementos en común. Cada subgrupo tendrá 4 elementos y como hay 24 ciclos de orden 5 habrá 6 subgrupos de orden 5.

**Ejemplo 68.** Sea  $G$  un grupo,  $H < G, N < G$  subgrupos. Recordemos que si  $H \cap N = \{e\}, HN = G \wedge N \triangleleft G$  entonces existe un producto semidirecto para el que  $G \simeq H \times_\phi N$ . Si  $|G| = p^a q^b$  con  $p \neq q$  primos, entonces existen  $P_p, P_q < G$  con  $|P_p| = a, |P_q| = b$ . Además se tiene que  $P_p \cap P_q = \{e\}, |P_p P_q| = |P_p| |P_q|$  y por tanto  $P_p P_q = G$ .

Realizamos un estudio sistemático de los grupos dado el orden similar al del teorema 46 pero utilizando los teoremas de Sylow

- Si  $|G| = 1$  no tiene interés estudiarlo.
- Si  $|G| = 2, 3$  entonces  $G \simeq \mathbb{Z}/2\mathbb{Z}$  o  $G \simeq \mathbb{Z}/3\mathbb{Z}$ .
- Si  $|G| = 4 = 2^2$  entonces  $G$  es abeliano. Lo demostramos en la proposición 62 para todo grupo de orden  $p^2$  con  $p$  primo.
- Si  $|G| = 5$  entonces  $G \simeq \mathbb{Z}/5\mathbb{Z}$ .
- Si  $|G| = 6 = 2 \cdot 3$  entonces  $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  o  $G \simeq D_3$ . Sabemos por Sylow que existen  $P_2, P_3 \triangleleft G$  con  $|P_2| = 2, |P_3| = 3$ . Además del tercer teorema de Sylow obtenemos  $n_3 = 1$ , es decir que en  $F_3$  tenemos solo un grupo. Para  $n_2$  solo tenemos que  $n_2 = 1, 3$ . Ahora bien, como  $n_3 = 1$  tenemos que  $P_3 < G$ . Por tanto, existe un producto semidirecto para el que  $G \simeq P_3 \times_\phi P_2 = ? \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .<sup>8</sup>

Veamos que de este producto semidirecto nos salen dos estructuras. En primer lugar vemos quiénes son  $N$  y  $H$ . En este caso el grupo normal es  $P_3$  por lo que  $N = P_3$  y  $H = P_2$ . Veamos los automorfismos interiores  $Int : H \rightarrow Aut(\mathbb{Z}/3\mathbb{Z}) = (\{\bar{1}, \bar{2}\}, \cdot) = \mathcal{U}(\mathbb{Z}/3\mathbb{Z})$ . Como  $Aut(\mathbb{Z}/3\mathbb{Z})$  tiene dos elementos, obtenemos dos estructuras

- Si tomamos que  $e_H \mapsto e_{Aut(\mathbb{Z}/3\mathbb{Z})} = \bar{1}$  entonces encontramos que  $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .
- Si tomamos que  $e_H \mapsto \bar{2}$  ocurre que  $G \simeq D_3$ . Vamos a verlo.

Supongamos que  $P_3 = \langle a \rangle, o(a) = 3$ . Si para algún  $h \in H$  definimos la conjugación  $h x h^{-1}$  para  $x \in G$  tenemos que como  $P_3 \triangleleft G$  entonces  $h P_3 h^{-1} = P_3$ . Ahora supongamos que  $H = P_2 = \langle b \rangle, o(b) = 2$ . Entonces para un  $b$ , con el automorfismo seleccionado  $a \mapsto b a b^{-1} = a^2 \implies ab = b a^2$  y llegamos a la presentación de  $D_3$  (con las  $a$ 's y las  $b$ 's cambiadas.)

- Si  $|G| = 7$  entonces  $G \simeq \mathbb{Z}/7\mathbb{Z}$ .
- Si  $|G| = 8$  Sylow dice poco. Lo vimos en algún sitio
- Si  $|G| = 9$  tampoco tenemos mucho que decir

<sup>8</sup>Por convención ponemos el normal primero, para poder aplicar directamente la construcción sin liarnos.

- Si  $|G| = 10 = 2 \cdot 5$ . Como de costumbre sabemos que existen  $P_2, P_5 < G$  con los ordenes correspondientes. Por el tercer teorema llegamos a que  $n_5 = 1$  y por tanto a que  $P_5 < G$ . Para  $P_2$  no tenemos nada, pero solo por ser  $P_5$  normal existe un producto semidirecto para el que  $G \simeq P_5 \times P_2 \simeq \mathbb{Z}/5\mathbb{Z} \times_{\phi} \mathbb{Z}/2\mathbb{Z}$ . Como en el caso de  $|G| = 6$  obtendremos dos estructuras.

Tomamos  $N = P_5, H = P_2$ . Tenemos que definir morfismos  $Int : \mathbb{Z}/2\mathbb{Z} \rightarrow Auto(\mathbb{Z}/5\mathbb{Z}) = (\{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}, \cdot) = \mathcal{U}(\mathbb{Z}/5\mathbb{Z})$ . Para ver cuantos morfismos salen veamos el orden de los elementos de  $Aut(\mathbb{Z}/5\mathbb{Z})$ : Los elementos  $\{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$  tienen órdenes 1, 4, 4, 2 respectivamente. En  $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$  tenemos dos posibilidades<sup>9</sup> Un automorfismo viene dado por donde enviamos el generador de  $\mathbb{Z}/2\mathbb{Z}$  en este caso el  $\bar{1}$ .

- Si  $\bar{1} \mapsto \bar{1}$  obtenemos el homomorfismo trivial y por tanto la estructura dada por la presentación  $o(a) = 5, o(b) = 2, bab^{-1} = a \implies G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$  abeliano.
- Si  $\bar{1} \mapsto \bar{4}$  la estructura que obtenemos es  $o(a) = 5, o(b) = 2, bab^{-1} = a^4 = a^{-1}$ . Esta presentación es la del grupo  $D_5$ .
- Si  $|G| = 11$  pasa la historia de los primos.
- Si  $|G| = 12 = 2^2 \cdot 3$ . Entonces del tercero de Sylow tenemos  $n_3 = 1, 4$  y  $n_2 = 1, 3$ . Tristeza.<sup>10</sup>

Ahora se le ocurre afirmar que no puede ocurrir que  $n_2 = 3 \wedge n_3 = 4$  simultáneamente.

Supongamos que  $n_3 = 4$  entonces habría 4 subgrupos de orden 3 y por tanto habría  $2 \cdot 4$  elementos de orden 3 (el neutro tiene orden 1). Ya tenemos 9 elementos bajo control. Para controlar los 12 nos faltan 3 elementos que llamaremos  $a, b, c$  y que podrían formar un grupo con el neutro:  $\{e, a, b, c\}$ . Efectivamente esto dice Sylow, que hay un subgrupo de orden 4 ( $a, b, c$  no pueden tener orden 3 porque si no no podrían pertenecer a un grupo de orden 4). Como ya hemos agotado los elementos, no es posible que haya más subgrupos de orden 4, por lo que necesariamente  $n_2 = 1$ .

- Así podemos seguir hasta  $|G| = 29$  ya que cualquier orden menor que 30 es producto de como máximo dos primos.

**Ejemplo 69.** Sea  $G$  abeliano y  $|G| = 20 = 2^2 \cdot 5$ .

- Por el primer teorema de Sylow tenemos que  $\exists P_4 < G, |P_4| = 4$ .
- Por el segundo teorema, tenemos que todo subgrupo de orden 4 está en  $F_4 = \{gP_4g^{-1} \mid g \in G\}$ . Como  $G$  es abeliano,  $F_4$  solo tiene un elemento luego  $P_4$  es el único subgrupo de orden 4.
- Análogamente concluimos que  $P_5 < G$  es el único subgrupo de orden 5.

**Ejemplo 70.** Estudiamos el grupo  $G = \langle a, b \rangle$  con presentación  $o(b) = 4, o(a) = 3, bab^{-1} = a^2$ .

Pendiente, posible ejercicio de examen.

**Ejemplo 71.** Sea  $|G| = 30$ . Entonces  $G$  no es un grupo simple.

*Demostración.* Recordemos que  $G$  es simple si sus únicos subgrupos normales son  $G$  y  $\{e\}$  (ver definición 33).

Tenemos que  $|G| = 30 = 2 \cdot 3 \cdot 5$ . Por el primer teorema de Sylow tenemos que  $\exists P_5$  con  $|P_5| = 5$ . Además por el tercer teorema tenemos que  $n_5 = 1, 6$ . Análogamente tenemos  $|P_3| = 3$  y  $n_3 = 1, 10$ .

Supongamos que  $n_5 = 6, n_3 = 10$ . Sean  $S_1, \dots, S_6$  los 6 subgrupos de orden 5. Como 5 es primo entonces cada  $S_i$  es cíclico de orden 5 y necesariamente  $S_i \cap S_j = \{e\}$ , porque si  $S_i$  y  $S_j$  compartieran algún elemento, entonces serían el mismo grupo pero hemos supuesto que había 6 subgrupos de orden 5. Cada  $S_i = \{1, a, a^2, a^3, a^4\}$  por ser 5 primo  $\implies S_i$  cíclico, es decir, que tenemos  $4 \cdot 6 = 24$  elementos distintos de orden 5 (en cada grupo tenemos el neutro que tiene orden 1 y otros cuatro que deben tener orden 5 por ser  $S_i$  cíclico). Sean ahora  $H_1, \dots, H_{10}$  los subgrupos de orden 3. Aplicando el mismo argumento,  $H_i \cap H_j = \{e\}$ ,  $H_i = \{e, b, b^2\} \implies$  hay  $2 \cdot 10 = 20$  elementos distintos de orden 3. Con esto llegaríamos a que en  $G$  hay al menos  $20 + 24 = 44 > 30$  elementos por lo que llegamos a una contradicción. Es decir, que necesariamente tiene que ocurrir que  $n_3 = 1$  o  $n_5 = 1$ , por lo que existe un subgrupo normal distinto de  $G$  o  $\{e\} \implies G$  no puede ser simple. ♣

**Ejemplo 72.** Sea  $|G| = 48$ . Entonces o bien  $G$  tiene un subgrupo de orden 8 o bien  $G$  tiene un subgrupo de orden 16.

*Demostración.* Tenemos  $|G| = 2^4 \cdot 3$ . Por el primer teorema de Sylow tenemos que  $\exists P_2, |P_2| = 2^4$  y por el tercer teorema tenemos que  $n_2 = 1, 3$ .

ESTO TIENE UNAS LAGUNAS...

- Supongamos que  $n_2 = 3$ . Entonces  $F_3 = \{gP_3g^{-1} \mid g \in G\} = \{P_{2_1} = P_2, P_{2_2}, P_{2_3}\}$ . Probaremos que algún elemento de  $F_3$  tiene un subgrupo normal, es decir,  $\exists H < P_{2_i}$  para algún  $i = 1, 2, 3$ .

<sup>9</sup>Estamos abusando un poco de la notación de clases, ir con cuidado.

<sup>10</sup>Orlando: Sylow nunca dice toda la verdad, se puede hilar más fino.



- Consideramos la intersección  $P_{2_2} \cap P_{2_3}$ . Tenemos que  $|P_{2_2} \cap P_{2_3}| = 1, 2, 4, 8$ . Supongamos que  $|P_{2_2} \cap P_{2_3}| = 4$ . Entonces  $|P_{2_2} \cdot P_{2_3}| = \frac{|P_{2_2}||P_{2_3}|}{|P_{2_2} \cap P_{2_3}|} = \frac{16 \cdot 16}{4} = 48 = |G|$ . Esto no puede ocurrir, tiene que haber algún elemento de orden 3 y en  $P_{2_i}$  no puede haber ninguno. Por tanto concluimos que  $|P_{2_2} \cap P_{2_3}| > 4 \implies |P_{2_2} \cap P_{2_3}| = 8$ .<sup>11</sup>
- Es claro que  $P_{2_2} \cap P_{2_3} < P_{2_2}$ . Por alguna razón tenemos que  $P_{2_2} \cap P_{2_3} \triangleleft P_{2_2}$  y  $P_{2_2} \cap P_{2_3} \triangleleft P_{2_3}$ . Recordemos que  $P_{2_2} \cap P_{2_3} \triangleleft G \iff N(P_{2_2} \cap P_{2_3}) = G$  y que el normalizador  $N(H)$  siempre contiene a  $H$  y es el menor grupo en el que  $H \triangleleft N(H)$ . Entonces  $P_{2_2} \triangleleft N(P_{2_2} \cap P_{2_3}) \implies \forall g \in G, g(P_{2_2} \cap P_{2_3})g^{-1} = P_{2_2} \cap P_{2_3}$ . En particular  $\forall g \in P_2, g \in N(P_{2_2} \cap P_{2_3}) \wedge \forall g \in P_{2_3}, g \in N(P_{2_2} \cap P_{2_3})$ .



**Ejemplo 73.** Consideramos  $|S_4| = 4! = 2^3 \cdot 3$ . Podemos hacer el mismo argumento que antes para los subgrupos de orden 3.

**Proposición 96.** Sea  $G$  un grupo,  $H \triangleleft G, K \triangleleft G$  y  $H \cap K = \{e\}$ . Entonces  $\forall h, k, h \in H, k \in K \implies hk = kh$ .

**Teorema 97.** Sea  $G$  un grupo finito,  $H \triangleleft G$  y  $K \triangleleft G$ . Entonces son equivalentes

1.  $H \cap K = \{e\} \wedge HK = G$
2. la función  $H \times K \rightarrow G, (h, k) \mapsto hk$  es un isomorfismo de grupos

*Demostración.*

- 1  $\implies$  2. Lo primero decir que la función  $H \times K \rightarrow G$  existe por teoría de conjuntos. Tenemos por el teorema 43 que  $|HK| = |H||K|$ . Con esto tenemos que la función es sobreyectiva porque  $|H||K| = |G|$ . Además es claro que la función es inyectiva. Además como  $H \cap K = \{e\} \wedge H \triangleleft G \wedge K \triangleleft G$  tenemos que la función es un homomorfismo de grupos. Concluimos que la función es un isomorfismo de grupos.
- 2  $\implies$  1. Sea  $H \times e = \{(h, e) \mid h \in H\}$ . Es claro que  $H < H \times K$ : es subgrupo porque es finito y es cerrado. Análogamente sea  $e \times K = \{(e, k) \mid k \in K\}$  y  $e \times K < H \times K$ .

Veamos ahora que  $H \times e$ , y por extensión,  $e \times K$  son subgrupos normales en  $H \times K$ . Tenemos que probar que  $\forall (a, b) \in H \times K, (a, b)(H \times e)(a, b)^{-1} = (H \times e)$ . Sea  $h \in H$ , entonces

$$(a, b)(h, e)(a, b)^{-1} = (\underbrace{aha^{-1}}_{\in H}, \underbrace{beb^{-1}}_{=e}) \in H \times e \implies H \times e \triangleleft H \times K$$

Análogamente lo tenemos para  $e \times K$ .

Además, es claro que  $(H \times e) \cap (e \times K) = \{(e, e)\}$  que es el neutro de  $H \times K$  y por el isomorfismo de la hipótesis  $(e, e) \mapsto e \implies (H \times e) \cap (e \times K) \mapsto H \cap K = \{e\}$ .

Por último tenemos que  $(H \times e) \cdot (e \times K) = H \times K \simeq G$  por hipótesis. Además, podemos obtener cualquier elemento de  $HK$  con el mismo isomorfismo:  $\forall h \in H, k \in K, (h, e) \cdot (e, k) \mapsto hk \in HK \implies HK = G$ .



**Corolario 11.** Sea  $G$  un grupo finito,  $H \triangleleft G$  y  $K \triangleleft G, N \triangleleft G$ . Entonces son equivalentes

1.  $H \times K \times N \rightarrow G, (h, k, n) \mapsto hkn$  es un isomorfismo de grupos.
2.  $H \cap (KN) = K \cap (HN) = N \cap (HK) = \{e\}$  y  $HK N = G$ .

*Demostración.* Es análoga a la del teorema anterior.



**Corolario 12.** Dados  $H, K, N$  subgrupos normales de  $G$  entonces  $\forall g \in G$  existe una única operación para la que  $g = hkn$  y dicha operación es el isomorfismo  $H \times K \times N \rightarrow G$ .

**Teorema 98.** Sea  $G$  un grupo abeliano finito. Entonces  $G$  es suma directa de sus p-subgrupos de Sylow.

**Ejemplo 74.** Consideramos  $G = \mathbb{Z}/12\mathbb{Z}$  que tiene  $|G| = 2^2 \cdot 3$ . Se tiene que

$$P_2 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} \quad P_3 = \{\bar{0}, \bar{4}, \bar{8}\} \quad \mathbb{Z}/12\mathbb{Z} = P_2 \oplus P_3$$

<sup>11</sup>Ojo aquí, lo que está haciendo es aplicar el teorema 43 con mucho arte. Podía haber probado con  $|P_{2_2} \cap P_{2_3}| = 2$  pero en realidad no le hace falta, ya que  $|P_{2_i}| = 16$  es fijo y por tanto la única manera de cambiar  $|P_{2_2} \cdot P_{2_3}|$  es tocando el denominador. De ahí concluye que  $|P_{2_2} \cap P_{2_3}| > 4$ .

Sea ahora  $G$  un  $p$ -grupo abeliano finito, es decir que  $G$  es abeliano y que  $|G| = p^r$ . Es inmediato que  $\forall g \in G$ ,  $o(g) = p^s$  con  $s \leq r$ . Si tomamos  $n \in \mathbb{Z}$  y utilizamos notación aditiva ( $ng$  significa  $g$  operado consigo mismo  $n$  veces) tenemos que

$$\begin{aligned}\alpha_n : G &\rightarrow G \\ g &\mapsto ng\end{aligned}$$

es un homomorfismo de grupos (cuando  $G$  es abeliano). Si ahora tomamos  $p \in \mathbb{Z}$  con  $p$  primo, tenemos que  $\alpha_p(g) \mapsto pg$ . Por el teorema de Lagrange (23) tenemos que si  $|G| = n \wedge p \mid n$  entonces  $\exists \alpha \in G \mid o(\alpha) = p$ . Como  $|G| = p^r$  entonces  $\alpha_p : G \rightarrow G$  no es inyectiva y por tanto  $\emptyset \subsetneq \ker \alpha_p < G$ . Vamos a profundizar en el subgrupo  $\ker \alpha_p$ . Este subgrupo es

$$\ker \alpha_p = \{g \in G \mid o(g) \mid p\} = \{g \in G \mid o(g) = 1 \vee o(g) = p\}$$

ya que  $p$  es primo.

**Ejemplo 75.** Consideramos  $G = \mathbb{Z}/p^r\mathbb{Z}$ .

$$\begin{aligned}\mathbb{Z}/p^r\mathbb{Z} &\rightarrow \mathbb{Z}/p^r\mathbb{Z} \\ \bar{0} &\mapsto \bar{1} \\ &\vdots \\ &\vdots \\ \overline{p^{r-1}} &\mapsto \bar{0} \\ \overline{p^r - 1} &\end{aligned}$$

**Ejemplo 76.** Consideramos  $G = \mathbb{Z}/p^r\mathbb{Z} \oplus \mathbb{Z}/p^s\mathbb{Z}$ . Observemos que  $G$  nunca va a ser cíclico porque  $\text{mcd}(p^r, p^s) > 1$  (nunca serán coprimos). Definamos aquí el producto por  $p$ .

$$\begin{aligned}\alpha_p : G &\rightarrow G \\ (\bar{a}, \bar{b}) &\mapsto (p\bar{a}, p\bar{b})\end{aligned}$$

En este caso es necesario que  $\ker \alpha_p = \{(\bar{a}, \bar{b}) \mid p\bar{a} = \bar{0} \wedge p\bar{b} = \bar{0}\} = \langle \overline{p^{r-1}} \rangle \oplus \langle \overline{p^{s-1}} \rangle$  donde  $\langle \overline{p^{r-1}} \rangle \simeq \mathbb{Z}/p\mathbb{Z}$  y  $\langle \overline{p^{s-1}} \rangle \simeq \mathbb{Z}/p\mathbb{Z}$ . En este caso (en el que el  $p$ -grupo no es cíclico) se observa que hay más de 1 subgrupo de orden  $p$ .

¿Será verdad que esta observación caracteriza a los grupos cíclicos?

**Teorema 99** (de alguien 1). Sea  $G$  un  $p$ -subgrupo abeliano. Entonces  $G$  es cíclico si y solo si tiene un único subgrupo de orden  $p$ .

*Demostración.* Consideramos  $\alpha_p : G \rightarrow G$ .  $\ker \alpha_p$  consiste en  $\bar{0}$  y todos los elementos de orden  $p$ . Sea  $N$  el único subgrupo de orden  $p$ . Por tanto  $\ker \alpha_p = N$ .

La imagen  $\text{Im } \alpha_p$  es un subgrupo de  $G$  y sabemos (por los teoremas de isomorfía) que  $\text{Im } \alpha_p \simeq G/N$ . Pongamos que  $|G| = p^r$ , por hipótesis,  $\ker \alpha_p = N \wedge |N| = p$ . En particular, tenemos que  $\text{Im } \alpha_p$  es un  $p$ -grupo abeliano de orden  $|\text{Im } \alpha_p| \simeq |G/N| = \frac{p^r}{p} = p^{r-1}$ . Como  $p \mid |\text{Im } \alpha_p|$  tiene que existir un elemento de orden  $p$  en  $\text{Im } \alpha_p$  y por tanto  $N < \text{Im } \alpha_p < G$ . Es único porque si hubiera dos subgrupos de orden  $p$  en  $\text{Im } \alpha_p$ , también los habría en  $G$  y hemos partido de lo contrario. Aplicando inducción podemos suponer que el criterio es válido para  $\text{Im } \alpha_p$  y por tanto podemos suponer que  $\text{Im } \alpha_p$  es cíclico.

Sea  $\bar{g} \in \text{Im } \alpha_p$  que genera el subgrupo  $\text{Im } \alpha_p$ . Entonces  $\bar{g} \in G/N \simeq \text{Im } \alpha_p$ . Fijamos un elemento  $g \in G$  cuya imagen en  $G/N$  sea  $\bar{g}$ . Recordemos que hay una correspondencia (37) entre los subgrupos de  $G$  que contienen a  $N$  y los subgrupos de  $G/N$ . Por tanto tenemos un elemento  $g \in G$  que genera un subgrupo y quisiéramos ver que  $\langle g \rangle = G$ . Si demostramos que  $N < \langle g \rangle$  entonces  $\langle g \rangle = G$  por la correspondencia mencionada. Esta última afirmación ( $N < \langle g \rangle = G'$ ) es válida porque  $G'$  es un  $p$ -grupo  $\implies G'$  contiene un elemento de orden  $p \implies N < G' = \langle g \rangle$ . Luego  $\langle g \rangle = G$ . ♣

# Capítulo 7

## Grupos abelianos

En este capítulo utilizamos notación aditiva, la habitual para hablar de grupos abelianos. Recordemos que además de escribir  $a + b$  para la operación de dos elementos y  $r \cdot a$  para denotar el elemento  $a$  operado con sí mismo  $r$  veces, escribiremos  $G \oplus H$  para el producto directo (suma directa en este caso) y  $G + H$  para el producto libre (suma libre en este caso).

**Definición 35** (Suma directa). Sean  $(G_1, +), \dots, (G_n, +)$  grupos (abelianos) cuya operación es la suma<sup>a</sup> entonces denotamos por suma directa al producto directo de todos ellos:

$$\bigoplus_{i=1}^n (G_i, +) = \left( \bigoplus_{i=1}^n G_i, \oplus \right) = (G_1 \times \dots \times G_n, \oplus)$$

donde  $\oplus : (\bigoplus_{i=1}^n G_i) \times (\bigoplus_{i=1}^n G_i) \rightarrow \bigoplus_{i=1}^n G_i$  se define con  $g \oplus g' = (g_1 + g'_1, \dots, g_n + g'_n)$ .<sup>b</sup>

<sup>a</sup>Lo importante es que es la misma operación para todos y que utilizamos la notación aditiva, lo que *suma* signifique en realidad nos importa poco

<sup>b</sup>Aquí el  $\times$  que aparece se refiere al producto cartesiano, no al producto directo.

Es importante no confundirlas en lo que sigue.

**Definición 36** (Suma libre de grupos). <sup>a</sup> Sean  $S, T$  subconjuntos del grupo  $G$  (abeliano). Definimos  $S + T = \{s + t \mid s \in S \wedge t \in T\}$ .

<sup>a</sup>Lo de suma libre me lo he inventado completamente.

El objetivo de este capítulo es completar las proposiciones que teníamos sobre grupos abelianos para dar un teorema de clasificación válido para todo grupo abeliano finito. Con esto nos quitamos otra gran familia de grupos (ya nos habíamos quitado los cíclicos).

### 7.1. Descomposición en suma directa

**Proposición 100.** Sea  $G$  un grupo abeliano,  $H, K < G$ . Entonces son equivalentes:

1.  $H + K = G \wedge H \cap K = \{0\}$
- 2.

$$\begin{aligned} f : H \oplus K &\rightarrow G \\ (h, k) &\mapsto h + k \end{aligned}$$

es un isomorfismo de grupos

**Observación 6.** Esta proposición también es cierta para 3 subgrupos (o más) siempre que cumplan que la intersección de un subgrupo con la suma libre de los demás sea nula:

$$K, H, N < G \text{ abeliano} \wedge H + K + N = G \wedge \begin{cases} H \cap (K + N) = \{0\} \\ K \cap (H + N) = \{0\} \\ N \cap (K + H) = \{0\} \end{cases} \implies G \simeq H \oplus K \oplus N$$

Esto nos viene muy bien ya que los teoremas de Sylow justo nos proporcionan subgrupos cuya intersección es vacía: los p-grupos de Sylow, lo que nos lleva a una observación/teorema.

**Teorema 101.** Todo grupo abeliano es suma directa de sus p-subgrupos de Sylow.

**Ejemplo 77.** Sea  $G$  un grupo abeliano de orden  $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$ . Por Sylow tenemos que  $\exists P_1, P_2, P_3 < G$  tales que  $|P_1| = p_1^{\alpha_1}$ ,  $|P_2| = p_2^{\alpha_2}$ ,  $|P_3| = p_3^{\alpha_3}$ . Sabiendo que la intersección de subgrupos es un subgrupo y por tanto  $|P_1 \cap P_2|$  tiene que dividir a  $|P_1|$  y a  $|P_2|$  que son primos tenemos que  $|P_1 \cap P_2| = 1 \implies P_1 \cap P_2 = \{0\}$ . Lo mismo ocurre con las demás combinaciones de p-subgrupos de Sylow por lo que concluimos que  $G \simeq P_1 \oplus P_2 \oplus P_3$ .

**Observación 7.** Los elementos que viven en los p-subgrupos de Sylow son aquellos cuyo orden es una potencia de  $p_i$ :

$$P_i = \{g \in G \mid o(g) \text{ es una potencia de } p_i\}$$

**Ejemplo 78.** Una manera de ver esto es definiendo para un  $n \in \mathbb{N}$  fijo

$$\begin{aligned} G &\rightarrow G \\ a &\mapsto n \cdot a \end{aligned}$$

tenemos que es un homomorfismo de grupos cuando  $G$  es abeliano. En nuestro caso cogiendo  $n = p_i^{\alpha_i}$  tenemos que  $a \mapsto p_i^{\alpha_i} a = 0 \iff o(a) \mid p_i^{\alpha_i}$ . Por ejemplo para  $G = \mathbb{Z}/10\mathbb{Z}$  tenemos que  $\exists P_2, P_5 < \mathbb{Z}/10\mathbb{Z}$  donde

$$\begin{aligned} P_2 &= \ker(\text{multiplicación por } 2) = \{\bar{0}, \bar{5}\} && \simeq \mathbb{Z}/2\mathbb{Z} \\ P_5 &= \ker(\text{multiplicación por } 5) = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\} && \simeq \mathbb{Z}/5\mathbb{Z} \end{aligned}$$

Y se dan las hipótesis de la proposición 100 por lo que concluimos que  $\mathbb{Z}/10\mathbb{Z} = P_2 \oplus P_5 \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$

**Ejemplo 79.** Consideramos  $G = \mathbb{Z}/12\mathbb{Z}$ . Por Sylow tenemos  $\exists P_2, P_3 < \mathbb{Z}/12\mathbb{Z}$  tales que

$$\begin{aligned} P_2 &= \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} && = \text{elementos cuyos órdenes son potencia de } 2 \simeq \mathbb{Z}/4\mathbb{Z} \\ P_3 &= \{\bar{0}, \bar{4}, \bar{8}\} && = \text{elementos cuyos órdenes son una potencia de } 3 \simeq \mathbb{Z}/3\mathbb{Z} \end{aligned}$$

Y por tanto  $\mathbb{Z}/12\mathbb{Z} \simeq P_2 \oplus P_3 \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ .

**Observación 8.** Esta descomposición es unívoca (salvo reordenaciones de los sumandos): en grupos abelianos los p-subgrupos de Sylow son únicos ya que al ser todos normales los  $n_i = 1$ .

## 7.2. P-grupos abelianos finitos

$$\begin{array}{ccc} G \simeq \mathbb{Z}/p^r\mathbb{Z} & \xrightarrow{\alpha_p} & \mathbb{Z}/p^r\mathbb{Z} \\ \bar{0} & & \bar{0} \\ \bar{1} & \searrow & \bar{1} \\ \vdots & & \vdots \\ \overline{p^{r-1}} & \nearrow & \bar{p} \\ \overline{p^r - 1} & & \end{array}$$

Figura 7.1: El homomorfismo de grupos  $\alpha_p$ .

Sea  $G$  un grupo abeliano con  $|G| = p^r$ ,  $r \in \mathbb{N} \implies \forall g \in G, o(g) = p^s$  con  $s \leq r$ . Recordemos que si  $n \in \mathbb{Z}$  la función  $\alpha_n : G \rightarrow G$ ,  $a \mapsto n \cdot a$  es un homomorfismo de grupos cuando  $G$  es abeliano.

Para este caso nos interesa tomar  $n = p$  y observar que  $\alpha_p(a) = p \cdot a$  no es inyectiva por ser  $|G| = p^r$ .

**Proposición 102.** El homomorfismo de grupos  $\alpha_p : G \rightarrow G$  para un  $G$  p-grupo abeliano finito tiene núcleo no trivial. Es decir,  $\{0\} \subsetneq \ker \alpha_p < G$

*Demostración.* Por el teorema 23  $|G| = n \wedge p \mid n \implies \exists \alpha \in G \mid o(\alpha) = p$  (aquí  $p$  es primo). De modo que

$$\ker \alpha_p = \{g \in G \mid o(g) \mid p\} \supset \{0, \alpha \mid o(\alpha) = p\} \supsetneq \{0\}$$



**Observación 9.** El elemento  $p^{r-1}$  tiene orden  $p$  y genera el único subgrupo de orden  $p$ .

**Observación 10.**  $\text{Im } \alpha_p = \langle \alpha(\bar{1}) \rangle = \langle \bar{p} \rangle \simeq \mathbb{Z}/p^{r-1}\mathbb{Z}$ .

Si ahora consideramos  $G \simeq \mathbb{Z}/p^r\mathbb{Z} \oplus \mathbb{Z}/p^s\mathbb{Z}$  (que no es cíclico porque  $\text{mcd}(p^r, p^s) \geq p > 1$ ) veamos que lo anterior no se cumple. Sean  $\bar{a} \in \mathbb{Z}/p^r\mathbb{Z}$ ,  $\bar{b} \in \mathbb{Z}/p^s\mathbb{Z}$ .

$$\begin{aligned}\alpha_p : G &\rightarrow G \\ (\bar{a}, \bar{b}) &\mapsto (p\bar{a}, p\bar{b})\end{aligned}$$

$$\begin{aligned}\ker \alpha_p &= \{(\bar{a}, \bar{b}) \in G \mid p\bar{a} = \mathbf{0} \wedge p\bar{b} = \mathbf{0}\} \\ \ker \alpha_p &= \langle \bar{p}^{r-1} \rangle \oplus \langle \bar{p}^{s-1} \rangle \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}\end{aligned}$$

En este caso, hay más de un subgrupo de orden  $p$ . Por ejemplo

$$\begin{aligned}\langle (\bar{0}, \bar{1}) \rangle &\subset \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \text{ y tiene orden } p \\ \langle (\bar{1}, \bar{0}) \rangle &\subset \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \text{ y tiene orden } p\end{aligned}$$

Esta lista no es exhaustiva, hay más...

### 7.3. Teorema de estructura de grupos abelianos finitos

Previamente a dar el teorema gordo, veremos algunos resultados.

**Proposición 103.** Sea  $G$  un  $p$ -grupo abeliano. Entonces  $G$  es cíclico  $\iff$  tiene un único subgrupo de orden  $p$ .

*Demostración.* Pendiente de los apuntes de Santorum página 146



**Proposición 104.** Sea  $G$  un  $p$ -grupo abeliano con  $|G| = p^r$ . Sea  $L$  un subgrupo cíclico de orden máximo<sup>1</sup> en  $G$ . Entonces  $\exists H < G$  tal que  $G \simeq L \oplus H$ .

*Demostración.* Santorum pág 197



**Proposición 105** (de estructura de  $p$ -grupos abelianos). Sea  $G$  un  $p$ -grupo abeliano finito. Entonces  $G$  es suma directa de subgrupos cíclicos:

$$G \simeq L_1 \oplus L_2 \oplus \cdots \oplus L_q, \quad L_i < G \text{ cíclico} \quad (7.1)$$

**Corolario 13.** Si  $L_i = \mathbb{Z}/p_i\mathbb{Z}$  y reordenamos los índices para obtener

$$p^{r_1} \geq p^{r_2} \geq \cdots \geq p^{r_q} \quad (7.2)$$

entonces la secuencia 7.2 es intrínseca a  $G$ .

*Demostración.* Santorum pág 149



**Definición 37** (Expresión característica). Sea  $G$  un  $p$ -grupo abeliano que se descompone en  $G \simeq L_1 \oplus \cdots \oplus L_q$  con  $L_i \simeq \mathbb{Z}/p^{r_i}\mathbb{Z}$ . La expresión característica de  $G$  es la desigualdad que resulta de reordenar los índices para que se cumpla

$$p^{r_1} \geq p^{r_2} \geq \cdots \geq p^{r_q} \quad (7.3)$$

**Ejemplo 80.** Sea  $G = \mathcal{U}(\mathbb{Z}/12\mathbb{Z}) = (\{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}, \cdot)$ . Observemos que  $G$  contiene 3 elementos de orden 2. Esto nos recuerda a una presentación de  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  y concluimos que  $G \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$  y por tanto la expresión característica es  $2^1 \geq 2^1$ .

**Ejemplo 81.** Sea  $G = \mathcal{U}(\mathbb{Z}/60\mathbb{Z})$ . Se pide comprobar que  $G$  es un  $p$ -grupo y dar su expresión característica.

*Solución.* Observemos que  $\mathbb{Z}/60\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$  ya que  $\text{mcd}(12, 5) = 1$  y observemos que<sup>2</sup>

$$\begin{aligned}\mathcal{U}(\mathbb{Z}/60\mathbb{Z}) &= \{(a, b) \in \mathbb{Z}/60\mathbb{Z} \mid o(a) = 12 \wedge o(b) = 5\} \\ a \in \mathcal{U}(\mathbb{Z}/12\mathbb{Z}) &= \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \\ b \in \mathcal{U}(\mathbb{Z}/5\mathbb{Z}) &= \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\} \simeq \mathbb{Z}/4\mathbb{Z} \\ \implies \mathcal{U}(\mathbb{Z}/60\mathbb{Z}) &= \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}\end{aligned}$$

y por tanto la secuencia asociada es  $2^2 \geq 2^1 \geq 2^1$ .



<sup>1</sup>Esto significa que  $|L|$  es el mayor divisor de  $|G|$  para el que  $L$  es cíclico. Se tendrá que si  $G$  ya es cíclico entonces  $L = G$  y  $H = \{0\}$ .

<sup>2</sup>Aquí estamos medio adelantando la proposición 118 que se probará cuando se introduzcan formalmente las unidades que son un concepto de anillos.

Con esto y sabiendo que la descomposición en p-grupos de un grupo abeliano es única estamos a nada de enunciar el teorema de estructura pero antes veamos un ejemplo de aplicación de los resultados anteriores.

**Ejemplo 82.** Sea  $G = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ . Nos preguntamos cuántos subgrupos de orden  $p$  contiene  $G$ .

*Solución.* Observemos que  $|G| = p^2$  y que los elementos de  $G$  solo pueden tener orden 1 u orden  $p$ . Es decir que en  $G$  hay

$$\begin{aligned} & p^2 - 1 \text{ elementos de orden } p \\ & 1 \text{ elemento de orden 1 (el neutro)} \end{aligned}$$

Por tanto tenemos que  $\forall a \in G$ ,  $0 \neq a$  hay un  $H < G$ ,  $H = \langle a \rangle$  con  $|H| = p$ . Además  $H$  contiene 1 elemento de orden 1 (el neutro) y  $p - 1$  elementos de orden  $p$ . Además, recordemos que los elementos  $a$  de orden  $p$  solo pertenecen a uno de los subgrupos  $H$  ya que en cuanto pertenezcan a dos, los dos subgrupos son necesariamente el mismo. Por tanto el número de subgrupos de orden  $p$  se obtiene de repartir los elementos de orden  $p$ :

$$\frac{p^2 - 1}{p - 1} = \frac{(p - 1)(p + 1)}{(p - 1)} = p + 1 \text{ subgrupos de orden } p$$



**Teorema 106** (de estructura de grupos abelianos finitos). Todo grupo abeliano es isomorfo a una suma directa de p-grupos cíclicos.

## Parte II

# Anillos





## Capítulo 8

# Anillos (y cuerpos)

En este capítulo se extiende lo que sabemos de teoría de grupos a las nuevas estructuras algebraicas que introducimos que son los anillos y los cuerpos.

### 8.1. Definición y propiedades básicas

**Definición 38** (Anillo). Un anillo es una terna  $(A, +, \cdot)$  donde  $+: A \times A \rightarrow A$  es una operación a la que llamamos suma,  $\cdot: A \times A \rightarrow A$  es otra operación a la que llamamos producto y se verifican las siguientes propiedades

1. El par  $(A, +)$  es un grupo abeliano
2. El producto  $\cdot$  es asociativo
3. Se cumplen las propiedades distributivas:

$$\forall a, b, c \in A, a \cdot (b + c) = a \cdot b + a \cdot c \quad (8.1)$$

$$\forall a, b, c \in A, (a + b) \cdot c = a \cdot c + b \cdot c \quad (8.2)$$

Con la operación  $+$  tenemos las siguientes propiedades

1. Asociatividad:  $(a + b) + c = a + (b + c)$
2. Elemento neutro aditivo:  $\exists! \mathbf{0} \in A \mid \mathbf{0} + a = a$
3. Elemento inverso aditivo:  $\forall a \in A, \exists -a \in A \mid a + (-a) = \mathbf{0}$
4. Conmutatividad aditiva:  $\forall a, b \in A, a + b = b + a$

Con la operación  $\cdot$  tenemos las siguientes propiedades

1. Asociatividad:  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. No siempre existe el neutro multiplicativo:  $\mathbf{1} \in A \mid a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$
3. No siempre el producto es conmutativo.
4. No siempre existe inverso multiplicativo:  $a^{-1} \mid a \cdot a^{-1} = \mathbf{1}$
5. No siempre se da la conmutatividad multiplicativa:  $a \cdot b = b \cdot a$

**Proposición 107.**  $\forall a \in A, a \cdot \mathbf{0} = \mathbf{0}$

*Demostración.*  $a \cdot \mathbf{0} = a \cdot (\mathbf{0} + \mathbf{0}) = a \cdot \mathbf{0} + a \cdot \mathbf{0} \implies \mathbf{0} = a \cdot \mathbf{0}$



**Definición 39** (Anillo con unidad o anillo unitario). Sea  $(A, +, \cdot)$  un anillo. Decimos que es un anillo con unidad o un anillo unitario si tiene elemento neutro multiplicativo, es decir, si  $\exists \mathbf{1} \in A \mid \forall a \in A, \mathbf{1}a = a\mathbf{1} = a$ .

**Proposición 108.** El neutro multiplicativo o unidad,  $\mathbf{1}$ , si existe, es único.

**Definición 40** (Anillo conmutativo). Sea  $(A, +, \cdot)$  un anillo.  $A$  es un anillo conmutativo  $\iff \forall a, b \in A, a \cdot b = b \cdot a$ . Es decir, un anillo es conmutativo  $\iff$  el producto también es conmutativo.

**Proposición 109.** Sea  $(A, +, \cdot)$  un anillo con más de un elemento ( $|A| > 1$ ). Entonces  $\mathbf{0} \neq \mathbf{1}$  (el neutro aditivo es distinto del neutro multiplicativo).

*Demostración.* Por contradicción. Sea  $a \neq \mathbf{0} \in A$  y  $\mathbf{0} = \mathbf{1}$ . Entonces  $a = a \cdot \mathbf{1} = a \cdot \mathbf{0} = 0 \implies a = \mathbf{0}$  contradicción. ♣

Para acabar veremos ejemplos de los 4 posibles casos que se pueden dar con las dos definiciones anteriores:

**Ejemplo 83** (Anillo conmutativo con unidad). El anillo  $(\mathbb{Z}, +, \cdot)$  es un anillo con unidad y la unidad es  $\mathbf{1} = 1$ .

**Ejemplo 84** (Anillo conmutativo sin unidad). El anillo  $(2\mathbb{Z}, +, \cdot)$  no tiene unidad ya que  $\nexists \mathbf{1} \in 2\mathbb{Z} \mid \forall a \in 2\mathbb{Z}, a\mathbf{1} = \mathbf{1}a = a$ .

**Ejemplo 85** (Anillo no conmutativo con unidad). Las matrices cuadradas  $2 \times 2$  con coeficientes reales:  $(M_{2 \times 2}(\mathbb{R}), +, \cdot)$  es un anillo con unidad (el neutro multiplicativo es  $\mathbf{1} = I$ ) pero no es conmutativo.

**Ejemplo 86** (Anillo no conmutativo sin unidad). Las matrices cuadradas  $2 \times 2$  con coeficientes en  $2\mathbb{Z}$  es un anillo no conmutativo y además no tiene unidad.

El ejemplo menos enrevesado es el primero. También son ejemplos de anillos conmutativos con unidad los conjuntos habituales  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  y los conjuntos de clases  $\mathbb{Z}/p\mathbb{Z}$  con  $p$  primo (en todos ellos el neutro multiplicativo es lo que te esperas que sea el neutro multiplicativo). Además todos ellos cumplen que el conjunto con el producto es un grupo. Pues como es tan común esta cosa le damos nombre:

**Definición 41** (Cuerpo (alternativa)). Sea  $(A, +, \cdot)$  un anillo conmutativo con unidad. Diremos que  $A$  es un cuerpo si  $A \setminus \{\mathbf{0}\}$  es cerrado por la segunda operación (el *producto*).

Es decir, que  $(A \setminus \{\mathbf{0}\}, \cdot)$  es un grupo. Digo definición alternativa porque la definición que ha dado Orlando es ligeramente diferente (hay que esperar media página para conocerla pero es la definición 44).

**Ejemplo 87.**

$\mathbb{Z}/p\mathbb{Z}$  con  $p$  primo es un cuerpo

$\mathbb{Z}$  o  $\mathbb{Z}/6\mathbb{Z}$  no son cuerpos

$\mathbb{Q}$  es un cuerpo (es el primero que sale al ir añadiendo números a los naturales)

$\mathbb{R}$  y  $\mathbb{C}$  también son cuerpos

Las matrices  $2 \times 2$  invertibles que antes veíamos como un grupo solo con el producto también son un cuerpo si les añadimos la suma:  $(GL_2(\mathbb{R}), +, \cdot)$  es un cuerpo.

Antes de seguir, siempre vamos a hablar de anillos con unidad o **anillos unitarios**, aunque alguna vez se me olvide ponerlo.

### 8.1.1. Extensiones de anillos

**Definición 42** (Extensión de anillos). Sea  $(A, +, \cdot)$  un anillo. Definimos la extensión

$$A[m] = \{a + bm \mid a, b \in A\} \quad (8.3)$$

**Ejemplo 88.** La extensión de los reales con  $i = \sqrt{-1}$  son los complejos:

$$\mathbb{R}[\sqrt{-1}] = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}$$

### 8.1.2. Unidades en anillos

Además, para pulir lo de que no siempre existe inverso multiplicativo daremos la definición de Grupo de unidades en el contexto de anillos que da sentido al ejemplo 3 que hemos estado utilizando. Ojo: aquí unidades no se refiere a varios elementos neutros multiplicativos como uno podría pensar.

**Definición 43** (Unidades en anillos). Dado  $(A, +, \cdot)$  anillo. El grupo de unidades es

$$\mathcal{U}(A) = (\{a \in A \mid \exists a^{-1} \in A, a \cdot a^{-1} = \mathbf{1}\}, \cdot) \quad (8.4)$$

Los elementos del grupo de unidades se llaman **elementos invertibles**.

Para que este grupo quede bien definido estaría bien que  $a^{-1}$  fuera único.

**Proposición 110.** El inverso multiplicativo es único.

*Demostración.* Sea  $a \in A$ . Supongamos  $a', a'' \in A$  son ambos inversos multiplicativos de  $a$ :

$$aa' = \mathbf{1} \wedge aa'' = \mathbf{1} \implies \begin{cases} a''(aa') = a'' \\ (a''a)a' = a'' \end{cases} \implies a' = a''$$



**Proposición 111.** Sea  $-\mathbf{1}$  el inverso aditivo del neutro multiplicativo  $\mathbf{1}$ . Entonces  $\forall a \in A$  el inverso aditivo es  $-a = -\mathbf{1} \cdot a$  y se tiene  $-\mathbf{1} \cdot a + a = 0$ .

**Proposición 112.** Sea  $A$  un anillo. El neutro aditivo  $\mathbf{0}$  verifica  $\mathbf{0} \notin \mathcal{U}(A)$

**Proposición 113** (Propiedad cancelativa). Sea  $a \in \mathcal{U}(A)$ . Entonces  $\forall b, c$  se tiene  $b, c \in A \implies a \cdot b = a \cdot c \implies b = c$

**Proposición 114.**  $a \in \mathcal{U}(A) \iff \langle a \rangle = A$

*Demostración.*

1.  $(\implies)$   $a \in \mathcal{U}(A) \implies \exists a^{-1} \implies \langle a \rangle = A \cdot a = \{\alpha a \mid \alpha \in A\}$ . Si  $a \in \mathcal{U}(A) \implies \exists a^{-1} \implies a^{-1}a = \mathbf{1} \in \langle a \rangle \iff \langle a \rangle = A$
2.  $(\impliedby)$  Si  $\langle a \rangle = A$  entonces  $\exists b \in A \mid ba = \mathbf{1} \implies b = a^{-1} \implies a \in \mathcal{U}(A)$ .



**Ejemplo 89.** Los numeros enteros  $(\mathbb{Z}, +, \cdot)$  tienen estructura de anillo anillo y tienen unidades  $\mathcal{U}(\mathbb{Z}) = (\{-1, 1\}, \cdot)$

**Proposición 115.** Si  $K$  es un cuerpo finito entonces el grupo abeliano  $(\mathcal{U}(K), \cdot)$  es cíclico.

*Demostración.* Ver santorum p. 194.



**Ejemplo 90.** En  $K = \mathbb{Z}/13\mathbb{Z}$  tenemos que las unidades  $\mathcal{U}(\mathbb{Z}/13\mathbb{Z}) \simeq \mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$  que es cíclico.

Ah! y la definición de Orlando de cuerpo es

**Definición 44** (Cuerpo). Diremos que un anillo con unidad es un cuerpo si  $\mathcal{U}(A) = A \setminus \{\mathbf{0}\}$

## 8.2. Subanillos

**Definición 45** (Subanillo). [DH96] Sea  $(A, +, \cdot)$  un anillo,  $B \subset A$ . Decimos que  $B$  es un subanillo si  $(B, +)$  es subgrupo de  $(A, +)$  y el producto restringido a  $B$  es cerrado.

La definición que ha dado Orlando es algo diferente. Es equivalente a la anterior y la plasmamos como una proposición.

**Proposición 116.**  $B \subset A$  es un subanillo si ambas operaciones son cerradas y  $(B, +, \cdot)$  es un anillo (tiene la estructura de anillo).

**Ejemplo 91.**  $(\mathbb{Z}, +, \cdot)$  es un subanillo de  $(\mathbb{Q}, +, \cdot)$ .

**Definición 46** (Subcuerpo). Un subcuerpo es un subanillo que es un cuerpo.

### 8.3. Producto directo

Como ocurría con los cuerpos, una manera de obtener nuevos cuerpos es con el producto directo.

**Definición 47** (Producto directo en anillos). Sean  $(A, +_A, \cdot_A), (B, +_B, \cdot_B)$  dos anillos con unidad. Definimos el producto directo  $A \times B$  como el anillo  $(A \times B, \#, \bullet)$  donde las operaciones se definen:

$$\begin{aligned} \# : (A \times B) \times (A \times B) &\rightarrow A \times B & (a_1, b_1) \# (a_2, b_2) &= (a_1 +_A a_2, b_1 +_B b_2) \\ \bullet : (A \times B) \times (A \times B) &\rightarrow A \times B & (a_1, b_1) \bullet (a_2, b_2) &= (a_1 \cdot_A a_2, b_1 \cdot_B b_2) \end{aligned}$$

**Proposición 117.**  $(A \times B, \#, \bullet)$  en efecto es un anillo.

**Observación 11.** En el nuevo anillo  $(A \times B, \#, \bullet)$  el elemento neutro aditivo es  $\mathbf{0}_{A \times B} = (\mathbf{0}_A, \mathbf{0}_B)$  y el elemento neutro multiplicativo es  $(\mathbf{1}_A, \mathbf{1}_B)$ .

**Observación 12.** Nos preguntamos ahora: ¿Si  $A, B$  son cuerpos, es  $A \times B$  un cuerpo? La respuesta es que NO. Contraejemplo:

$$\underbrace{(\mathbf{1}_A, \mathbf{0}_B)}_{\neq (\mathbf{0}_A, \mathbf{0}_B)} \bullet (a, b) = (\mathbf{1}_A, \mathbf{1}_B) \iff \begin{cases} \mathbf{1}_A \cdot_A a = \mathbf{1}_A \\ \mathbf{0}_B \cdot_B b = \mathbf{1}_B \end{cases} \longrightarrow \text{sin solución}$$

(Aquí lo que falla es que no es cerrado por el producto porque  $(\mathbf{1}_A, \mathbf{0}_B)$  no tiene inverso (y no es el neutro aditivo que es el único que se libra de ese requisito).

Veamos esto con un ejemplo:

**Ejemplo 92.** Consideramos el producto directo de los cuerpos  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . No es un cuerpo porque  $(1, 0) \bullet (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$ , es decir que el producto no es cerrado ya que tenemos dos elementos en  $A \setminus \{\mathbf{0}\}$  que operados nos han dado un elemento fuera. Alternativamente, hemos encontrado divisores de  $\mathbf{0}$ .

#### 8.3.1. Unidades en el producto directo de anillos

**Proposición 118.**  $(a, b) \in \mathcal{U}(A \times B) \iff a \in \mathcal{U}(A) \wedge b \in \mathcal{U}(B)$ . Es decir, que  $\mathcal{U}(A \times B) \simeq \mathcal{U}(A) \times \mathcal{U}(B)$ .

*Demostración.*  $(a, b) \in \mathcal{U}(A \times B) \iff \exists (a', b') \in A \times B \mid (a, b) \bullet (a', b') = (\mathbf{1}_A, \mathbf{1}_B) \iff a \cdot_A a' = \mathbf{1}_A \wedge b \cdot_B b' = \mathbf{1}_B \iff a \in \mathcal{U}(A) \wedge b \in \mathcal{U}(B)$  ♣

**Ejemplo 93.** Las unidades de  $\mathbb{Z} \times \mathbb{Z}$  son

$$\mathcal{U}(\mathbb{Z} \times \mathbb{Z}) = (\{(1, 1), (1, -1), (-1, 1), (-1, -1)\}, \bullet)$$

### 8.4. Divisores de 0. Dominios de integridad.

**Definición 48** (Divisor de 0). Sea  $(A, +, \cdot)$  un anillo conmutativo<sup>a</sup>. Diremos que  $a \in A$  es divisor de  $\mathbf{0} \iff a \neq \mathbf{0} \wedge \exists b \neq \mathbf{0} \in A \mid a \cdot b = \mathbf{0}$

<sup>a</sup>Si aquí no decimos conmutativo entonces especificaremos si se trata de un divisor de  $\mathbf{0}$  por la derecha o por la izquierda. Ver la nota al principio de la sección sobre ideales.

**Ejemplo 94.** En  $\mathbb{Z}/8\mathbb{Z}$  el elemento  $\bar{2}$  es un divisor de  $\mathbf{0}$ :

$$\bar{2} \cdot \bar{4} = \bar{8} = \mathbf{0}$$

Sin embargo,  $\bar{3}$  no lo es ya que

$$\bar{3}\bar{a} = \mathbf{0} \implies \bar{3}^{-1}\bar{3}\bar{a} = \bar{3}^{-1}\mathbf{0} \implies \mathbf{1}\bar{a} = \mathbf{0} \implies \bar{a} = \mathbf{0}$$

Otra manera de ver esto es plantear la ecuación  $a \cdot b = \mathbf{0}$ . El  $\mathbf{0}$  siempre es una solución, pero podemos decir que  $a$  es un divisor de  $\mathbf{0}$  si la ecuación tiene soluciones no triviales.

**Ejemplo 95.**

- En  $\mathbb{Z}$  la ec.  $2x = \mathbf{0}$  solo tiene la solución trivial  $\implies 2$  no es un divisor de  $\mathbf{0}$ .
- En  $\mathbb{Z}/6\mathbb{Z}$  la ec.  $\bar{2}\bar{x} = \mathbf{0}$  tiene la solución  $\bar{x} = \bar{3}$  luego  $\bar{2}$  sí que es un divisor de  $\mathbf{0}$ .

**Proposición 119.** Si  $a \in \mathcal{U}(A)$  entonces  $a$  no es un divisor de  $\mathbf{0}$ . Equivalentemente, si  $a$  es un divisor de  $\mathbf{0}$  entonces  $a \notin \mathcal{U}(A)$ .

*Demostración.* Si  $a \in \mathcal{U}(A)$  sabemos que existe  $a^{-1} \mid a^{-1}a = \mathbf{1} \implies ax = \mathbf{0} \iff a^{-1}ax = a^{-1}\mathbf{0} \iff \mathbf{1}x = \mathbf{0} \iff x = \mathbf{0}$  luego la ecuación solo tiene la solución trivial. ♣

**Proposición 120.** Sea  $A$  un anillo.  $\forall a \in A$  no divisor de  $\mathbf{0} \implies$  se cumple la propiedad cancelativa.

*Demostración.*  $ab = ac \implies b = c \iff ab + (-ac) = a(b - c) = \mathbf{0}$  ♣

**Definición 49** (Dominio de integridad). Un anillo que no tiene elementos divisores de  $\mathbf{0}$  se llama dominio de integridad o DI.

**Ejemplo 96.**

- $\mathbb{Z}$  es un dominio de integridad ya que todo  $a \in \mathbb{Z}, a \neq \mathbf{0}$  tiene un inverso multiplicativo  $a^{-1}$ .
- $\mathbb{Z}/p\mathbb{Z}$  con  $p$  primo es un dominio de integridad.
- $\mathbb{Z}/n\mathbb{Z}$  con  $n$  no primo no es un dominio de integridad ya que si  $\bar{n} = ab$  con  $a \neq n \wedge b \neq n$  se tiene  $\bar{a} \cdot \bar{b} = \bar{n} = \mathbf{0}$  con  $\bar{a} \neq \mathbf{0} \wedge \bar{b} \neq \mathbf{0}$ .

A veces utilizamos como definición de dominio de integridad la siguiente proposición:

**Proposición 121.**  $A$  es un DI  $\iff$  el producto de elementos no nulos es no nulo.

*Demostración.* ( $\iff$ ) Sean  $a, b \in A, a, b \neq \mathbf{0} \implies ab \neq \mathbf{0} \implies A$  dominio de integridad.

( $\implies$ ) Sea  $a \in A, a \neq \mathbf{0}$ .  $A$  DI  $\implies \nexists b \in A \mid a \cdot b = \mathbf{0} \iff$  el producto de no nulos es no nulo. ♣

**Proposición 122.** Sea  $A$  un DI y  $C \subset A$  un subanillo. Entonces  $C$  es un DI.

*Demostración.* Sean  $\mathbf{0} \neq c_1, c_2 \in C$ . Como  $C \subset A$  y  $c_1c_2 \neq \mathbf{0}$  en  $A$  tenemos en particular que  $c_1c_2 \neq \mathbf{0}$  en  $C \implies C$  es un DI. ♣

**Proposición 123.** Si  $A$  es un cuerpo entonces  $A$  es un DI.

Por lo general el recíproco es falso.

## 8.5. Ideales

Los ideales son el homólogo de los subgrupos normales en anillos. Se utilizan por ejemplo para definir el anillo cociente.

En otros sitios, un ideal es en realidad una clase lateral (recordar la ??) y se definen ideales a derecha y a izquierda. El equivalente a un subgrupo normal en anillos sería aquel en el que coinciden las clases laterales a derecha y a izquierda — lo que otros ([MW]) llaman un ideal bilateral (*two-sided ideal*).

Aquí vamos a dar y a utilizar directamente la definición de ideal bilateral y por tanto un ideal para nosotros ya sería un equivalente de un subgrupo normal.

La definición de ideal se puede dar de dos maneras. Así la ha dado Orlando:

**Definición 50** (Ideal). Un subconjunto  $I \subset A$  es un ideal  $\iff$

1.  $\mathbf{0} \in I$
2.  $s, t \in I \implies s + t \in I$
3.  $s \in I \wedge a \in A \implies a \cdot s \in I \wedge s \cdot a \in I$


Esta es otra definición alternativa:

**Definición 51** (Ideal (alternativa)). [DH96, p. 197] Sea  $I$  un subanillo de  $A$ . Decimos que  $I$  es un ideal  $\iff \forall i \in I, \forall a \in A, ai \in I \wedge ia \in I$ .

**Proposición 124.** Si  $I$  es un ideal en  $A$  entonces  $(I, +) < (A, +)$  (es decir,  $I$  es un subgrupo aditivo de  $A$ ).

**Proposición 125.** Sea  $I \subset A$  un ideal. Entonces  $\mathbf{1} \in I \iff I = A$ .

*Demostración.* Por la tercera propiedad de los ideales tenemos que  $\mathbf{1} \in I \implies \forall a \in A, \mathbf{1} \cdot a \in I \implies A \subseteq I \implies A = I$ .

El otro sentido es trivial. 

**Ejemplo 97.** En cualquier anillo  $A$  son ideales tanto el subgrupo  $\{0\}$  como el mismo anillo  $A$  ( $A$  es ideal en sí mismo).

**Ejemplo 98.**  $0\mathbb{Z}, 1\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}$  son todos ideales de  $\mathbb{Z}$  (y subgrupos de  $(\mathbb{Z}, +)$ ).

**Ejemplo 99.** Sabemos que en  $\mathbb{Z}$  todo  $n\mathbb{Z}$  es un ideal. ¿Ocurre lo mismo para  $\{(n, n) \mid n \in \mathbb{Z}\} \subset \mathbb{Z} \times \mathbb{Z}$ ? La respuesta es que NO. Contraejemplo:  $(1, 0) \bullet (3, 3) = (3, 0) \notin \{(n, n) \mid n \in \mathbb{Z}\}$  (al no ser cerrado por el producto no es un subanillo y por tanto tampoco es un ideal).

**Proposición 126.** Sea  $\{I_j\}_{j \in J}$  una familia de ideales en  $A$  ( $I_j \subset A$  es un ideal para cada  $j \in J$ ). Entonces  $\bigcap_{j \in J} I_j$  es un ideal en  $A$ .

**Ejemplo 100.** En el anillo  $\mathbb{Z}$  están los ideales  $6\mathbb{Z}$  y  $8\mathbb{Z}$ . Por la proposición anterior  $6\mathbb{Z} \cap 8\mathbb{Z}$  es un ideal (es  $\text{mcd}(6, 8)\mathbb{Z} = 2\mathbb{Z}$ ).

**Proposición 127.** Sean  $I, J \subset A$  ideales. Entonces  $I + J = \{i + j \mid i \in I \wedge j \in J\}$  es un ideal<sup>1</sup> de  $A$  que contiene a  $I$ , a  $J$ , y además es el menor ideal con esta propiedad.

### 8.5.1. Ideales generados. Ideales principales. Dominios de ideales principales.

A continuación definimos el análogo al subgrupo generado pero para anillos:

**Definición 52** (Ideal generado por un subconjunto). De [DH96]. Sea  $(A, +, \cdot)$  un anillo conmutativo,  $S \subset A$ . Definimos el ideal generado por  $S$  y lo denotamos con  $\langle S \rangle$  como el conjunto de todas las palabras de longitud  $n$  en los elementos de  $S$ , para  $n \in \mathbb{N}$ . Esto es:

$$\langle S \rangle = \{s_1 \cdot a_1 + \cdots + s_n a_n \mid a_i \in A, s_i \in S, n \in \mathbb{N}\} = \left\{ \sum_{i=1}^n a_i s_i \mid a_i \in A, s_i \in S, n \in \mathbb{N} \right\}$$

Ojo al abuso de notación en la definición anterior. El sumatorio y el producto implícito hacen referencia a las operaciones definidas en el anillo  $(A, +, \cdot)$ .


Como cabe esperar, cumple las mismas propiedades que cumplían los subgrupos generados.

**Proposición 128.** Sea  $S = \{S_1, \dots, S_r\} \subset A$  y sea  $\langle S \rangle = \{\sum_{i=1}^r a_i s_i \mid a_i \in A\}$ . Entonces

1.  $\langle S \rangle$  es un ideal<sup>2</sup> en  $A$
2.  $S \subseteq \langle S \rangle$
3. Si  $T$  es un ideal, entonces  $S \subset T \iff \langle S \rangle \subset T$ , esto es,  $\langle S \rangle$  es el menor ideal que contiene a  $S$ .

**Proposición 129.** Consideramos ahora  $\langle s \rangle$  para un elemento  $s \in S$  (esto no es más que  $\langle \{s\} \rangle$ ). Afirmamos que  $s \in \mathcal{U}(A) \iff \langle s \rangle = A$

*Demostración.* Primero, si  $s \in \mathcal{U}(A) \implies \exists a \in A \mid sa = as = \mathbf{1} \implies \mathbf{1} \in \langle s \rangle \implies \forall b \in A, b\mathbf{1} = b \in \langle s \rangle \implies A \subseteq \langle s \rangle$ . Es claro que  $\langle s \rangle \subseteq A$  luego  $A = \langle s \rangle$ .

Recíprocamente,  $A = \langle s \rangle \implies \exists a \mid sa = \mathbf{1} \implies s \in \mathcal{U}(A)$ . 

<sup>1</sup>Ojo: aquí  $I + J$  no tiene nada que ver con la suma directa (el caso particular del producto directo) que había en grupos. De hecho se parece más al producto libre, que recordemos que en caso de que  $I, J$  fueran subgrupos normales daba un subgrupo normal. El equivalente aquí es que si  $I, J$  son ideales entonces su "producto libre" también es un ideal.

<sup>2</sup>Es para asegurarnos de que la construcción que hemos dado produce un ideal.

**Definición 53** (Ideal principal). Diremos que un ideal es principal si está generado por un único elemento.

**Ejemplo 101.** En  $\mathbb{Z}$  consideramos el subconjunto  $S = \{6\} \subset \mathbb{Z}$ . El conjunto  $\langle S \rangle = \{a6 \mid a \in \mathbb{Z}\} = 6\mathbb{Z}$  es un ideal y como está generado por un único elemento, es un ideal principal.

**Definición 54** (Dominio de ideales principales (DIP)). Sea  $(A, +, \cdot)$  un anillo que además es un DI. Si todo ideal  $I \subset A$  es principal decimos que  $A$  es un dominio de ideales principales o DIP.

**Observación 13.** En  $\mathbb{Z}$  todo ideal es principal.

**Ejemplo 102.** Aunque en  $\mathbb{Z}$  todo ideal es principal, también podemos dar ideales de  $\mathbb{Z}$  con varios generadores (aunque para todos ellos siempre podremos encontrar un único elemento que los genere). Por ejemplo  $2\mathbb{Z} = \{6a + 10b \mid a, b \in \mathbb{Z}\} = \langle 6, 10 \rangle$ .

### 8.5.2. Ideales primos

**Definición 55** (Ideal primo). Diremos que  $P \subset A$  es un ideal primo  $\iff$

1.  $P \subsetneq A$
2.  $a_1 \notin P \wedge a_2 \notin P \implies a_1 a_2 \notin P$

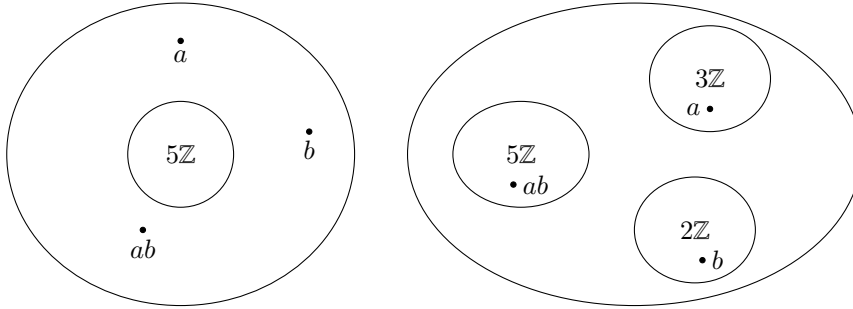


Figura 8.1: Ejemplo de un ideal primo ( $5\mathbb{Z}$ ) y otro no primo ( $6\mathbb{Z}$ ).

**Ejemplo 103.** En  $\mathbb{Z}$  el  $\{0\}$  es un ideal primo. También lo es  $5\mathbb{Z}$ . Por el contrario  $6\mathbb{Z}$  no lo es.<sup>3</sup>

**Proposición 130.** Un anillo  $A$  es un DI  $\iff \{0\}$  es un ideal primo.

Orlando dio la implicación hacia la derecha de este teorema pero [DH96] da la otra.

**Proposición 131.** Sea  $P \subsetneq A$  un ideal propio. Entonces  $A/P$  DI  $\iff P$  ideal primo.

*Demostración.* Ver [DH96, p. 201].



### 8.5.3. Ideales maximales

**Definición 56** (Ideal maximal). Sea  $I \subsetneq A$  un ideal propio. Diremos que  $I$  es un ideal maximal  $\iff \forall J$

$$J \text{ ideal} \wedge I \subseteq J \subset A \implies J = I \vee J = A$$

**Proposición 132.** En el anillo  $(\mathbb{Z}, +, \cdot)$  son ideales maximales  $p\mathbb{Z}$  con  $p$  primo.

**Proposición 133.** Sea  $M \subsetneq A$  un ideal maximal de  $A$ . Entonces  $A/M$  es un cuerpo.

**Proposición 134.** Todo ideal maximal es un ideal primo.

*Demostración.*  $M \subsetneq$  un ideal maximal de  $A \implies A/M$  cuerpo  $\implies A/M$  DI  $\implies M$  ideal primo.



<sup>3</sup>Vaya que chorprecha que los  $p\mathbb{Z}$  con  $p$  primo sean ideales primos.

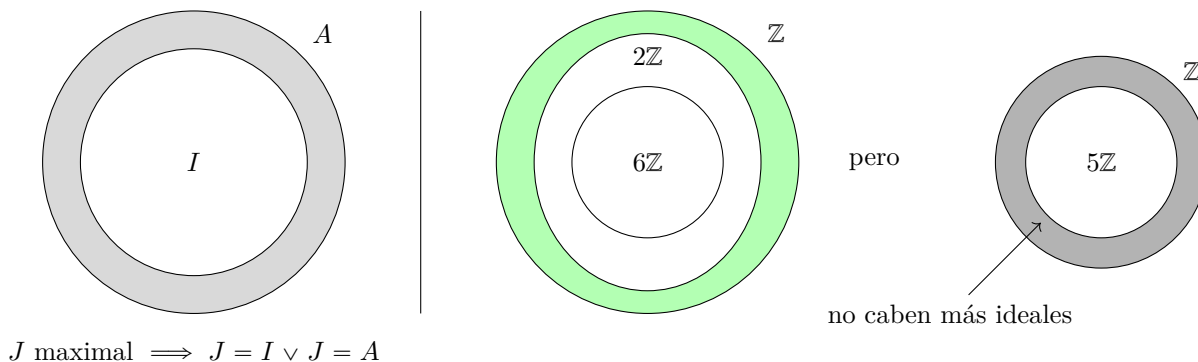


Figura 8.2: Diferencia entre un ideal maximal y uno no maximal. Aquí  $6\mathbb{Z}$  no es maximal pero  $5\mathbb{Z}$  sí que lo es.

El recíproco no es verdad en general. Por ejemplo en  $\mathbb{Z}$  el  $\{0\}$  es un ideal primo pero no es maximal porque  $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$  no es un cuerpo (contrarrecíproco de la proposición 133).

#### 8.5.4. Ideales y el producto directo

**Proposición 135.** Sean  $A, B$  anillos conmutativos con unidad. Sean  $I \subset A, J \subset B$  ideales de  $A$  y  $B$  respectivamente. Entonces  $I \times J \subset A \times B$  es un ideal en el producto directo.

*Demostración.* Comprobamos las propiedades de los ideales:

1.  $\mathbf{0} = (0, 0) \in I \times J$  porque  $\mathbf{0} \in I \wedge \mathbf{0} \in J$
2.  $\forall s = (s_1, s_2), t = (t_1, t_2) \in I \times J$  tenemos que  $s + t = (s_1 + t_1, s_2 + t_2) \in I \times J$  pues  $s_1, t_1 \in I \implies s_1 + t_1 \in I$  y pasa lo mismo con  $s_2$  y  $t_2$ .
3.  $\forall s = (s_1, s_2) \in I \times J, a = (a_1, a_2) \in A \times B$  se tiene que  $sa = (s_1a_1, s_2a_2) \in I \times J$  pues  $s_1a_1 \in I \wedge s_2a_2 \in J$ . Se tiene lo mismo para el producto por la derecha ya que  $A$  y  $B$  son conmutativos.





## Capítulo 9

# Homomorfismos de anillos

### 9.1. Extensión desde los homomorfismos de grupos.

Solo necesitamos definir qué tiene que pasar con la segunda operación. Si lo hacemos bien, todas las propiedades se mantienen.

**Definición 57** (Homomorfismo de anillos). Sean  $(A, +, \cdot), (B, \oplus, \odot)$  anillos y sea  $\varphi : A \rightarrow B$ . Decimos que  $\varphi$  es un homomorfismo de anillos si

1.  $\varphi(a_1 + a_2) = \varphi(a_1) \oplus \varphi(a_2)$
2.  $\varphi(a_1 \cdot a_2) = \varphi(a_1) \odot \varphi(a_2)$
3.  $\varphi(1_A) = 1_B$

**Observación 14.** Dado  $\varphi : A \rightarrow B$  homomorfismo de anillos,  $\text{Im } \varphi \subset B$  siempre es un subanillo de  $B$ .

**Proposición 136** (Inyectividad/sobreyectividad en homomorfismos de anillos). Sea  $\varphi : A \rightarrow B$  un homomorfismo de anillos.

- $\varphi$  inyectivo  $\iff \ker \varphi = \{0\}$
- $\varphi$  sobre  $\iff \text{Im } \varphi = B$

**Proposición 137.** El homomorfismo de anillos  $\varphi : A \rightarrow B$  es una biyección de conjuntos  $\iff \ker \varphi = \{0\} \wedge \text{Im } \varphi = B$ .

**Observación 15.** Si  $\varphi : A \rightarrow B$  homomorfismo de anillos es una biyección de conjuntos entonces  $\varphi^{-1} : B \rightarrow A$  también es un homomorfismo de anillos.

**Definición 58** (Isomorfismo de anillos). Diremos que un homomorfismo de anillos  $\varphi : A \rightarrow B$  es un isomorfismo de anillos  $\iff \exists \varphi^{-1} : B \rightarrow A$  tal que

$$\varphi \circ \varphi^{-1} = Id_B \wedge \varphi^{-1} \circ \varphi = Id_A$$

**Proposición 138.** Sea  $\varphi : A \rightarrow B$  un homomorfismo de anillos. Entonces  $\varphi$  es un isomorfismo de anillos  $\iff \ker \varphi = \{0\} \wedge \text{Im } \varphi = B$ .

### 9.2. Homomorfismos de anillos y divisores de 0

**Ejemplo 104.** Sea  $s \in A, s \neq 0$ . Fijado  $s$ , definimos  $\alpha_s : A \rightarrow A, a \mapsto a \cdot s$ . Observemos:

1.  $\alpha_s$  es un homomorfismo de grupos
2.  $\alpha_s$  es inyectivo  $\iff \ker \alpha_s = \{0\}$ 
  - $\ker \alpha_s = \{0\} \iff s$  no es divisor de 0
  - $\ker \alpha_s \neq \{0\} \iff s$  es divisor de 0
3.  $\text{Im } \alpha_s = \langle \{s\} \rangle$ 
  - $s \in \mathcal{U}(A) \iff \langle s \rangle$  (ver proposición 8.5.1), por tanto  $\alpha_s$  es sobre  $\iff \text{Im } \alpha_s = A \iff \langle s \rangle = A \iff s \in \mathcal{U}(A)$ .

Este ejemplo nos permite dar el siguiente teorema:

**Teorema 139.** Sea  $(A, +, \cdot)$  un anillo finito y sea  $a \in A \setminus \{0\}$ . Entonces, o bien  $a \in \mathcal{U}(A)$ , o bien  $a$  es un divisor de 0. Por tanto escribimos

$$A \setminus \{0\} = \mathcal{U}(A) \cup \bigcup_{\text{disjunta}} \{a \in A \mid a \text{ divisor de } 0\}$$

*Demostración.* Fijo  $s \in A \setminus \{0\}$ . Como  $A$  es finito  $\alpha_s$  inyectiva  $\iff \alpha_s$  sobreyectiva  $\iff \alpha_s$  biyectiva. Entonces, fijándonos en el ejemplo anterior, tenemos

- Si  $s \in \mathcal{U}(A)$  entonces  $\alpha_s$  inyectiva<sup>1</sup>  $\implies \ker \alpha_s = \{0\} \implies s$  no es un divisor de 0.
- Si  $s \notin \mathcal{U}(A)$  entonces  $\alpha_s$  no es sobre  $\implies \alpha_s$  no inyectiva  $\implies \ker \alpha_s \neq \{0\} \implies s$  es un divisor de 0.

♣

**Ejemplo 105.** Sea  $A = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ . ¿Cuántos divisores de 0 tiene  $A$ ?

*Demostración.* Sabemos que  $|A| = 80 \implies A \setminus \{0\}$  tiene 79 elementos. Además, por la proposición 118, sabemos que  $\mathcal{U}(A) = \mathcal{U}(\mathbb{Z}/8\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/10\mathbb{Z}) \implies |\mathcal{U}(A)| = 4 \times 4 = 16$ . Luego hay  $79 - 16 = 63$  divisores de 0 en  $A$ . ♣

### 9.3. Homomorfismos de anillos e ideales

#### 9.3.1. Relación de equivalencia inducida por los ideales

**Definición 59** (Relación de equivalencia por ideales). Sea  $I \subset A$  un ideal. Definimos la relación de equivalencia  $a_1 Ra_2 \iff a_1 - a_2 \in I$ .

**Proposición 140.**  $R$  es efectivamente una relación de equivalencia

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

1. Reflexiva:  $\forall a_1 \in A, a_1 - a_1 = 0 \in I \implies a_1 Ra_1$
2. Simétrica:  $\forall a_1, a_2 \in A$  con  $a_1 Ra_2$  tenemos que  $a_2 - a_1 = -(a_1 - a_2) \in I \implies a_2 Ra_1$
3. Transitiva:  $a_1 Ra_2 \wedge a_2 Ra_3 \implies (a_1 - a_2) \in I \wedge (a_2 - a_3) \in I \implies ((a_1 - a_2) - (a_2 - a_3)) \in I \implies (a_1 - a_3) \in I \implies a_1 Ra_3$

♣

¿Cómo son las clases de equivalencia que viven en el conjunto cociente  $A/I$ ? Pues son de la forma  $\bar{a} = a + I = \{a + i_i \mid i_i \in I\}$ . Podemos dotar de estructura de anillo a este conjunto cociente. Las operaciones que definimos son las naturales:

**Definición 60** (Estructura de anillo del cociente). Sea  $(A, +, \cdot)$  un anillo,  $I \subset A$  un ideal. La relación de equivalencia  $a_1 Ra_2 \iff a_1 - a_2 \in I$  define una partición en clases de equivalencia  $\bar{a} \in A/I$ . Definimos las operaciones  $\#$  y  $\bullet$

$$\bar{a} \# \bar{b} = a + i_i + b + i_j = a + b + \underbrace{i_i + i_j}_{\in I} = \overline{a + b} \quad (9.1)$$

$$\bar{a} \bullet \bar{b} = (a + i_i)(b + i_j) = ab + \underbrace{ai_i + bi_j + i_i i_j}_{\in I} = \overline{a \cdot b} \quad (9.2)$$

De este modo  $(A/I, \#, \bullet)$  es un anillo y  $\pi : A \rightarrow A/I$  definido con  $a \mapsto \pi(a) = \bar{a}$  es un homomorfismo de anillos.

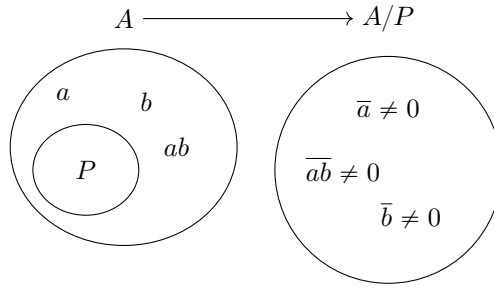
Hemos esperado a dar esto hasta ahora para poder dar la definición correcta del homomorfismo de anillos  $\pi$  que aparece al crear el cociente.

**Proposición 141.** Lo que dice la definición es verdad:  $(A/I, \#, \bullet)$  es un anillo y  $\pi$  un homomorfismo de anillos.

<sup>1</sup>Esto es porque  $\forall a, b \in A, \alpha_s(a) = \alpha_s(b) \iff sa = sb \iff s^{-1}sa = s^{-1}sb \iff a = b \implies \alpha_s$  inyectiva. Ver ejercicio para más detalles en la demostración de este teorema.

**Proposición 142.** La función  $\pi : A \rightarrow A/I$  que da las clases de equivalencia es un epimorfismo de grupos (es sobreyectivo) y además  $\ker \pi = I$ .

**Proposición 143.**  $P \subset A$  ideal primo  $\iff A/P$  es un dominio de integridad



*Demostración.* Sabemos que

$$\begin{aligned} a \notin P &\iff \bar{a} \neq \bar{0} \text{ en } A/P \\ b \notin P &\iff \bar{b} \neq \bar{0} \text{ en } A/P \\ a \cdot b \notin P &\iff \overline{a \cdot b} = \bar{a} \cdot \bar{b} \neq \bar{0} \text{ en } A/P \end{aligned}$$

Luego es claro que  $P$  ideal primo  $\iff$  el producto de elementos no nulos es no nulo en  $A/P \iff A/P$  es un DI (dominio de integridad). ♣

### 9.3.2. Retículo de ideales

**Definición 61** (Retículo de ideales). Estaría bien tener una definición de esto.

**Ejemplo 106.** En  $(\mathbb{Z}/8\mathbb{Z}, +, \cdot)$  el retículo de ideales coincide con los subgrupos de  $(\mathbb{Z}/8\mathbb{Z}, +)$ :

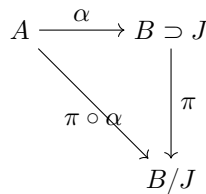
$$\{\bar{0}\} \subset \langle \bar{4} \rangle = \{\bar{0}, \bar{4}\} \subset \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\} \subset \mathbb{Z}/8\mathbb{Z}$$

### 9.3.3. Correspondencia entre ideales por un epimorfismo de anillos

Ahora damos un teorema análogo al de correspondencia que dimos para subgrupos (teorema 37).

**Teorema 144** (de correspondencia entre ideales). Sean  $A$  y  $B$  anillos y sea  $\alpha : A \rightarrow B$  un homomorfismo de anillos.

1. Si  $J \subset B$  es un ideal entonces  $\alpha^{-1}(J)$  es un ideal en  $A$ .
2. Si  $I \subset A$  es un ideal y además  $\alpha$  es sobreyectivo entonces la imagen  $\alpha(I)$  es un ideal en  $B$ .



*Demostración de 1.* Observar que  $\alpha^{-1}(J) = \ker(\pi \circ \alpha)$  y por tanto es un ideal. ♣

*Demostración de 2.* Probamos las 3 propiedades de los ideales (definición de Orlando, definición 50).

1.  $0 \in I \wedge \alpha$  h. de anillos  $\implies \alpha(0) = 0 \in \alpha(I)$
2. Sean  $\alpha(b_1), \alpha(b_2) \in \alpha(I)$ . Entonces  $\exists a_1, a_2 \in I \mid b_1 = \alpha(a_1) \wedge b_2 = \alpha(a_2)$ . Por tanto  $b_1 + b_2 = \alpha(a_1 + a_2) = \alpha(a_1) + \alpha(a_2) \in \alpha(I) \implies b_1 + b_2 \in \alpha(I)$ .
3. Sea  $b \in B$ . Como  $\alpha$  es sobre,  $\exists a \in A \mid \alpha(a) = b$ . Sea  $b' \in \alpha(I) \implies \exists a' \in I \mid b' = \alpha(a')$ . Entonces  $bb' = \alpha(a)\alpha(a') = \alpha(aa') \in \alpha(I)$  porque  $aa' \in I$ .



**Proposición 145.** Sea  $(A, +, \cdot)$  un anillo,  $I \subsetneq A$  un ideal propio de  $A$ . Sea  $\pi : A \rightarrow A/I$  la función sobreyectiva que da las clases de equivalencia para cada elemento  $a \in A \mapsto \bar{a}$  que tiene  $\ker \pi = I$ . Se tiene

1. Si  $\bar{J}$  es un ideal en  $A/I$  entonces  $\pi^{-1}(\bar{J})$  es un ideal en  $A$  que contiene a  $I$
2. Si  $J$  es un ideal en  $A$  entonces  $\pi(J)$  es un ideal en  $A/I$  y  $J \subset \pi^{-1}(\pi(J))$ .
  - Si además  $I \subset J$  entonces hay igualdad  $J = \pi^{-1}(\pi(J))$ .

*Demostración.* Si  $\bar{J}$  es un ideal en  $A/I$ .

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/I \supset \bar{J} \\ & & \downarrow \pi' \\ & & \frac{A/I}{\bar{J}} \end{array}$$

La composición  $\pi' \circ \pi$  es un homomorfismo de anillos y además  $\ker(\pi' \circ \pi) = \pi^{-1}(\bar{J})$



**Observación 16.** El ideal  $\{\bar{0}\}$  de  $A/I$  tiene contraimagen  $\pi^{-1}(\{\bar{0}\}) = I$ .

**Ejemplo 107.** Buscamos el retículo de ideales del grupo  $\mathbb{Z}/8\mathbb{Z}$ . Por la proposición 145 tenemos que los ideales  $\bar{J}$  de  $\mathbb{Z}/8\mathbb{Z}$  están en correspondencia con los ideales  $J$  en  $a$  que contengan a  $8\mathbb{Z}$  (Aquí  $A = \mathbb{Z}$ ,  $I = 8\mathbb{Z}$ ).

$$\begin{array}{ccc} \mathbb{Z} = \langle 1 \rangle & \longrightarrow & \langle \bar{1} \rangle = \mathbb{Z}/8\mathbb{Z} \\ | & & | \\ 2\mathbb{Z} = \langle 2 \rangle & \longrightarrow & \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\} \\ | & & | \\ 4\mathbb{Z} = \langle 4 \rangle & \longrightarrow & \langle \bar{4} \rangle = \{\bar{0}, \bar{4}\} \\ | & & | \\ 8\mathbb{Z} = \langle 8 \rangle & \longrightarrow & \langle \bar{8} \rangle = \{\bar{0}\} \end{array}$$

Figura 9.1: Retículo de ideales del anillo  $\mathbb{Z}/12\mathbb{Z}$  en correspondencia con los ideales de  $\mathbb{Z}$  que contienen a  $12\mathbb{Z}$ .

Obtenemos cada ideal de  $\mathbb{Z}/12\mathbb{Z}$  aplicando  $\pi$  a cada ideal de  $\mathbb{Z}$  que contiene a  $12\mathbb{Z}$ , esto es, cogiendo cada uno de sus elementos y tomando su clase. Para simplificar el dibujo, hemos puesto los ideales con generadores pero se puede hacer a mano. También se puede hacer directamente tomando la imagen del generador de un ideal de  $\mathbb{Z}$  que contiene a  $12\mathbb{Z}$ .

**Ejemplo 108.** Buscamos el retículo de ideales de  $\mathbb{Z}/12\mathbb{Z}$ . Aplicando la proposición 145 tomando  $A = \mathbb{Z}$ ,  $I = 12\mathbb{Z}$ , sabemos que los ideales del retículo de  $\mathbb{Z}/12\mathbb{Z}$  están en correspondencia con los del retículo de  $\mathbb{Z}$  que contienen al  $12\mathbb{Z}$ .

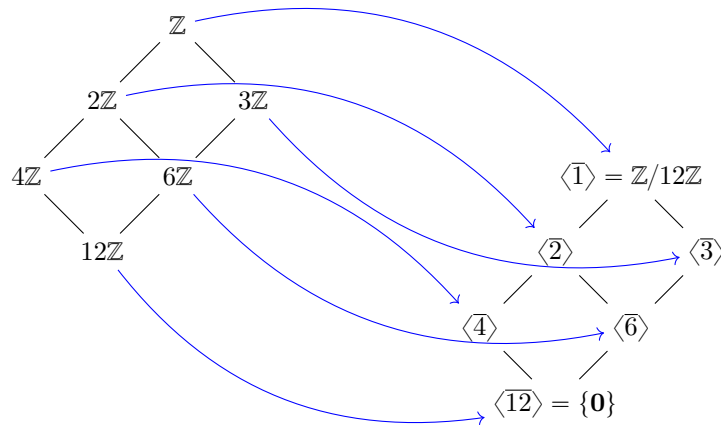


Figura 9.2: Los ideales de  $\mathbb{Z}/12\mathbb{Z}$  en correspondencia con los ideales de  $\mathbb{Z}$  que contienen a  $12\mathbb{Z}$ .

Como cabría esperar...

**Proposición 146.** En  $\mathbb{Z}/n\mathbb{Z}$  hay un ideal por cada divisor positivo de  $n$ . Además dos ideales  $\pi(n\mathbb{Z})$  y  $\pi(m\mathbb{Z})$  cumplen

$$(n\mathbb{Z} \subset m\mathbb{Z} \iff m \text{ divide a } n) \implies (\pi(n\mathbb{Z}) \subset \pi(m\mathbb{Z}) \iff m \text{ divide a } n)$$

**Ejemplo 109** (Retículo de ideales de  $(\mathbb{Z}, +, \cdot)$ ). Sabemos que los ideales de  $\mathbb{Z}$  son de la forma  $n\mathbb{Z} = 0\mathbb{Z}, 1\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, \dots$  para  $n = 0, 1, 2, 3, \dots$ . Observemos que podemos construir el retículo sabiendo que  $n\mathbb{Z} \subset m\mathbb{Z} \iff n \in m\mathbb{Z} \iff m \mid n$ . Así nos va quedando el retículo:

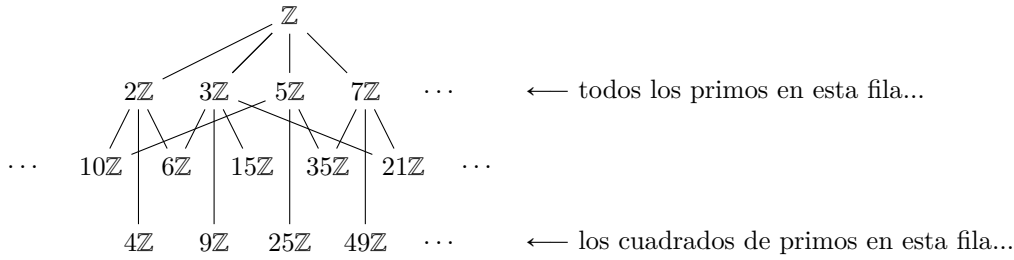


Figura 9.3: Retículo de ideales de  $(\mathbb{Z}, +, \cdot)$ .

**Observación 17.** Ya hemos visto que los ideales maximales de  $\mathbb{Z}$  son los de la forma  $p\mathbb{Z}$  con  $p$  primo. Es natural entonces que  $\mathbb{Z}/n\mathbb{Z}$  tenga tantos ideales maximales como divisores primos tenga  $n$ . Observemos que no importa la multiplicidad ya que los ideales que se corresponden con  $p^r$ ,  $r > 1$  no están en la primera fila, sino que están incluidos en ideales que sí están en la primera fila.

Mira tu por donde...

**Proposición 147.** Sea  $(A, +, \cdot)$  un anillo. Son equivalentes:

1.  $A$  es un cuerpo.
2. El retículo de ideales es el trivial, es decir, que solo tiene como ideales a  $\{0\}$  y a sí mismo.

## 9.4. Primer teorema de isomorfía para anillos

**Teorema 148** (Primer teorema de la isomorfía para anillos). Sea  $\alpha : A \rightarrow B$  homomorfismo de anillos sobreyectivo. Entonces  $B$  es isomorfo a  $A/\ker \alpha$ .

El resultado que acabamos de dar a veces se llama Teorema Fundamental de Isomorfismos de Anillos [DH96]. Lo hemos llamado Primer Teorema de la Isomorfía para anillos porque es lo mismo cambiando grupo por anillo y subgrupo normal por ideal.

$$\begin{array}{ccc}
 A & \xrightarrow{\alpha} & B \\
 \pi \downarrow & \nearrow \exists! \bar{\alpha} & \\
 A/\ker \alpha & & 
 \end{array}$$

Para probarlo nos ayudamos del siguiente Lema:

**Lema 149.** Sea  $\varphi : A \rightarrow B$  homomorfismo de anillos. Sea  $I$  un ideal en  $A$  tal que  $I \subset \ker \varphi$ . Entonces:

$$\begin{array}{ccc}
 A & \xrightarrow{\varphi} & B \\
 \pi \downarrow & \nearrow \exists! \bar{\varphi} & \\
 A/I & & 
 \end{array}$$

1.  $\exists! \bar{\varphi} : A/\ker \varphi \rightarrow B$  tal que  $\varphi = \bar{\varphi} \circ \pi$

$$2. \ker \bar{\varphi} = \frac{\ker \varphi}{I}$$

*Demostración de 1.* Recordemos que  $\pi : A \rightarrow A/I$  (la proyección que lleva cada elemento a su clase) es sobre. Tenemos que demostrar que  $\varphi = \bar{\varphi} \circ \pi$ , es decir que  $\forall a \in A, \varphi(a) = \bar{\varphi}(\pi(a)) = \bar{\varphi}(\bar{a})$  está bien definida. Recordemos que  $\bar{a} = \bar{a'} \iff a - a' \in I$ . Como  $I \subset \ker \varphi \implies \varphi(a - a') = 0 \iff \varphi(a) = \varphi(a')$ . ♣

*Demostración de 2.* Sea  $\bar{a} \in A/I$

$$\bar{a} \in \ker \bar{\varphi} \iff \bar{\varphi}(\bar{a}) = \mathbf{0}_B \iff \varphi(a) = 0 \iff a \in \ker \varphi$$

♣

*Demostración del primer teorema de la isomorfía para anillos.* Por el lema tenemos que  $\bar{\alpha}$  es un homomorfismo de anillos. Además, como  $\alpha$  es sobre por hipótesis y  $\pi$  también lo es tenemos que  $\bar{\alpha}$  es sobre. Aplicando la segunda parte del lema tenemos que  $\ker \bar{\alpha} = \frac{\ker \alpha}{\ker \alpha} = \{\bar{0}\}$  luego  $\bar{\alpha}$  es inyectiva.

Como  $\bar{\alpha}$  es un homomorfismo de anillos, es inyectivo y es sobre, tenemos que es un isomorfismo de anillos y por tanto  $B \simeq A/\ker \alpha$  ♣

**Corolario 14.** Sea  $\alpha : A \rightarrow B$  homomorfismo de anillos (no necesariamente sobre). Entonces  $\text{Im } \alpha \simeq A/\ker \alpha$ .

**Observación 18.** Sea  $\varphi : A \rightarrow B$  un homomorfismo de anillos y  $B$  un DI. Si restringimos  $\varphi$  a su imagen lo convertimos en sobreyectivo. Por el primer teorema de la isomorfía tenemos que  $A/\ker \varphi \simeq \text{Im } \varphi$  que es un dominio luego  $\ker \varphi$  es un ideal primo en  $A$ .

**Ejemplo 110.** Sea  $\alpha : \mathbb{Z}[X] \rightarrow \mathbb{Z}$  un homomorfismo de anillos sobreyectivo definido por

$$\begin{aligned} \sum_{j=0}^n a_j X^j &\mapsto \sum_{j=0}^n a_j 3^j \\ a_0 &\mapsto a_0 \end{aligned}$$

Entonces  $\ker \alpha = \langle x - 3 \rangle$  y además  $\mathbb{Z} \simeq \mathbb{Z}[X]/\ker \alpha$ . Aquí  $\ker \alpha$  es un ideal primo porque el cociente es un dominio.

**Observación 19.** Hay veces que no existe un homomorfismo de anillos entre dos anillos cualesquiera. No ocurre como con grupos que siempre teníamos el trivial.

**Ejemplo 111.** No existe homomorfismo de anillos  $f : \mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$  porque nos vemos forzados a definir  $f(1) = 1$  pero entonces  $f(1 + 1 + 1) = f(0) = 0 \neq \bar{3} = f(1) + f(1) + f(1)$ .

**Proposición 150.** Sea  $A$  un anillo cualquiera y sea  $\alpha : \mathbb{Z} \rightarrow A$  definida por  $f(1) = 1_A$  que automáticamente nos define  $f(-1) = -1_A$ ,  $f(2 = 1 + 1) = 1_A + 1_A, \dots, f(n) = n1_A$ ,  $f(-n) = n(-1_A)$ . Entonces si  $\alpha$  es un homomorfismo de anillos es el único homomorfismo de anillos entre  $\mathbb{Z}$  y  $A$ .

**Proposición 151.** Si  $A$  es un anillo y  $\alpha : \mathbb{Z} \rightarrow A$  es el homomorfismo de anillos, entonces  $\text{Im } \alpha \subset A$  es un DI.

**Definición 62** (Característica de un dominio). Diremos que  $A$  es un DI de característica 0 si  $\ker \alpha = \{0\}$ . Diremos que  $A$  es un DI de característica  $p$  si  $\ker \alpha = p\mathbb{Z}$ .

**Ejemplo 112.** Consideramos  $\alpha : \mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}[X]$ . Existe un único homomorfismo de anillos  $\alpha$  y además  $\ker \alpha = 3\mathbb{Z} \implies \mathbb{Z}/3\mathbb{Z}[X]$  es un DI de característica 3.

## 9.5. Cuerpo de fracciones de un anillo

Sean  $a, b \in A$  elementos de un anillo  $A$  cualquiera. En general  $ax = b$  no tiene solución dentro del anillo pero muchas veces las soluciones de esta ecuación son de interés. Por ejemplo, para resolver dichas ecuaciones cuando  $A = (\mathbb{Z}, +, \cdot)$  extendemos  $\mathbb{Z}$  al cuerpo  $(\mathbb{Q}, +, \cdot)$ . En esta sección veremos como esta extensión en realidad se puede hacer para cualquier DI conmutativo y con unidad.

**Definición 63** (Cuerpo de fracciones de un anillo). Sea  $(A, +, \cdot)$  un anillo conmutativo y con unidad y además sea  $A$  un DI. Definimos en  $A \times A \setminus \{0\}$  la relación de equivalencia

$$(a, b) \sim (c, d) \iff ad = bc \quad (9.3)$$

Definimos además el **cuerpo de fracciones**  $C = (A \times A \setminus \{0\}) / \sim = \{[(a, b)] \mid (a, b) \in A \times A \setminus \{0\}\}$  y dos operaciones sobre las clases de equivalencia

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)] \quad (9.4)$$

$$[(a, b)] \cdot [(c, d)] = [(ac, bd)] \quad (9.5)$$

Este conjunto  $C$  es el conjunto de los pares  $[(a, b)]$  tales que  $a, b \in A \wedge b \neq 0$  y lo interpretamos como los números  $\frac{a}{b}$  (está siempre bien definido porque  $b \neq 0$ ).

**Proposición 152.** La relación  $\sim$  es efectivamente una relación de equivalencia.

**Teorema 153.**  $(C, +, \cdot)$  es un cuerpo y además contiene un subanillo isomorfo a  $A$ .

*Demostración.* Para ver que  $(C, +, \cdot)$  es un cuerpo hay probar que  $(C, +, \cdot)$  es un anillo conmutativo con unidad y que no hay divisores de  $0$ . Es decir que las operaciones están bien definidas, que  $(C, +)$  es un grupo abeliano, que el producto es asociativo y conmutativo (es decir que  $(C \setminus \{0\}, \cdot)$  es un grupo abeliano), y que se cumplen las propiedades distributivas. Ver [DH96, p.209].

Además afirmamos que  $C$  contiene un subanillo isomorfo a  $A$ . Este subanillo es

$$\mathcal{A} = \{[(a, 1)] \mid a \in A\}$$

Se comprueba que en efecto es un subanillo (es cerrado por las operaciones y tiene estructura de anillo) y se define  $f : A \rightarrow \mathcal{A}$  con  $f(a) = [(a, 1)]$ . Se comprueba que  $f$  es en efecto un isomorfismo de anillos. ♣

En lo que sigue diremos que  $A$  es un subanillo de  $C$  aunque esto no es del todo cierto pero abusamos del lenguaje ya que son isomorfos.

**Ejemplo 113.** Veamos ejemplos de cuerpos de fracciones de los anillos más importantes:

- El cuerpo de fracciones de  $\mathbb{Z}$  es  $\mathbb{Q}$ . Bueno, en realidad es isomorfo a  $\mathbb{Q}$  con el isomorfismo  $f([(p, q)]) = \frac{p}{q}$ .
- El cuerpo de fracciones de  $\mathbb{Z}[i]$  es  $\mathbb{Q}[i]$ . En esta ocasión el isomorfismo es

$$f([(p + qi, u + vi)]) = \frac{(p + qi)}{(u + vi)} = \frac{(p + qi)(u - vi)}{u^2 + v^2} = \frac{pu + vq}{u^2 + v^2} + i \frac{qu - pv}{u^2 + v^2}$$

- El cuerpo de fracciones de  $\mathbb{Z}[\sqrt{m}]$  es  $\mathbb{Q}[\sqrt{m}]$
- Todo cuerpo coincide con su cuerpo de fracciones porque son isomorfos mediante  $f(a) = [(a, 1)]$ .

En ocasiones nos podemos pasar extendiendo un anillo para posibilitar que las ecuaciones  $ax = b$  tengan solución. Por ejemplo  $ax = b$  para  $a, b \in \mathbb{Z}$  tiene solución en  $\mathbb{Q}$  pero también en  $\mathbb{R}$  y  $\mathbb{C}$ . Por eso es interesante dar el siguiente resultado:

**Proposición 154.** Sea  $A$  un DI conmutativo y con unidad. Entonces su cuerpo de fracciones  $C$  es el menor cuerpo que contiene a  $A$ . Es decir que si cualquier otro cuerpo  $\tilde{C}$  contiene a  $A$  entonces existe un subcuerpo  $C' \subset \tilde{C}$  tal que  $C$  es isomorfo a  $C'$ .

*Demostración.* Ver [DH96, p.210]. ♣





## Capítulo 10

# Anillos de polinomios

### 10.1. Definiciones básicas y primeros resultados

**Definición 64** (Anillo de polinomios). Sea  $(A, +, \cdot)$  un anillo conmutativo y con unidad. Definimos el anillo de polinomios con coeficientes en  $A$  e incógnita  $X$

$$A[X] = \left\{ \sum_{i=0}^m a_i X^i \mid a_i \in A \wedge m \in \mathbb{N} \right\}$$

Para dos elementos cualesquiera  $p = \sum_{i=0}^n a_i X^i$ ,  $q = \sum_{i=0}^m a_i X^i \in A[X]$  se definen las operaciones suma y producto

$$\begin{aligned} p + q &= \sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i \\ p \cdot q &= \sum_{i=0}^{\max(n,m)} s_i X^i, \quad s_i = \sum_{j=0}^i p_j q_{i-j} \end{aligned}$$

Estas operaciones son las operaciones término a término de toda la vida.

**Proposición 155.** Sea  $(A, +, \cdot)$  un anillo conmutativo y con unidad. Entonces el anillo de polinomios  $(A[X], +, \cdot)$  es un anillo conmutativo y con unidad.

En este anillo el elemento neutro aditivo  $\mathbf{0}$  es el polinomio que tiene todos sus coeficientes  $a_j = 0$ .

**Definición 65** (Polinomio mónico). Sea  $A[X]$  un anillo de polinomios y  $p \in A[X]$ . Diremos que  $p$  es mónico  $\iff a_m = \max\{a_k \mid a_k \neq 0\} = 1$ .

**Definición 66** (Grado de un polinomio). Sea  $p \in A[X]$ . Definimos el grado del polinomio  $p = \sum_{j=0}^n a_j X^j$

$$\text{gr } p = \max\{j \mid a_j \neq 0\} \tag{10.1}$$

**Proposición 156.** Si  $A$  es un DI entonces  $A[X]$  también lo es.

*Demostración.* Sean  $p, q \in A[X]$  no nulos. Entonces

$$\begin{aligned} p \cdot q = \mathbf{0} &\iff \sum_{i=0}^{\max(n,m)} s_i X^i \\ &\iff s_i = \sum_{j=0}^i p_j q_{i-j} = 0 \\ &\iff p_j q_{i-j} = 0, \quad \forall 0 \leq j \leq i \\ &\iff p_j = \mathbf{0} \vee q_{i-j} = \mathbf{0} \text{ en } A \end{aligned}$$

ya que  $A$  es un DI. ♣

**Corolario 15.** Si  $A[X]$  es un DI conmutativo y con unidad y  $p, q \in A[X]$  con  $p, q \neq \mathbf{0}$  entonces

$$\text{gr } pq = \text{gr } p + \text{gr } q \quad (10.2)$$

**Proposición 157.** Si  $A[X]$  es un DI conmutativo y con unidad entonces  $\mathcal{U}(A[X]) = \mathcal{U}(A)$ .

Ahora hacemos lo mismo para cuerpos:

**Proposición 158.** Si  $K$  es un cuerpo entonces  $K[X]$  es un DI.

*Demostración.* Si  $K$  es un cuerpo entonces  $\mathcal{U}(K[X]) = \mathcal{U}(K) = K \setminus \{0\}$ . ♣

*Demostración.* Si  $K$  es un cuerpo en particular es un DI y nos reducimos a hace dos proposiciones. ♣

**Teorema 159** (Algoritmo de la división). Sea  $K$  un cuerpo y sean  $p, q \in K[X]$  con  $q \neq \mathbf{0}$ . Entonces existen  $c, r \in K[X]$  tales que  $p = qc + r$  y además  $\text{gr } r = 0 \vee \text{gr } r < \text{gr } q$ .

Aquí  $c$  es el cociente y  $r$  es el resto.

**Definición 67** (Divisibilidad). Sean  $p, q \in K[X]$ . Decimos que  $p$  divide a  $q$  en  $K[X]$  y lo denotamos con  $p \mid q \iff q = cp$  con  $c \in K[X]$  (es decir, si el resto es 0).

**Proposición 160.** Sea  $K$  un cuerpo entonces  $K[X]$  es un DIP.

*Demostración.* Como en  $K[X]$  tenemos un algoritmo de la división entonces todo ideal es principal. ♣

**Corolario 16.** Si  $K$  es un cuerpo entonces en  $K[X]$  identificamos los ideales en  $K[X]$  con los polinomios mónicos en  $K[X]$ . Es decir

$$\begin{aligned} p \in K[X] \text{ mónico} &\iff I = \langle p \rangle \text{ ideal en } K[X] \\ \langle p \rangle \subset \langle q \rangle &\iff p \in \langle q \rangle \iff q \mid p \text{ en } K[X] \end{aligned}$$

## 10.2. Factorizacion e irreducibilidad en anillos de números

**Definición 68** (Divisibilidad). Sea  $A$  un DI conmutativo y con unidad y sean  $r, s \in A$ . Decimos que  $r$  divide a  $s$  y lo denotamos por  $r \mid s \iff \exists t \in A \mid s = rt$ . Escribimos  $s/r$  para denotar a  $t$ .

**Definición 69** (Primo). Sea  $A$  un anillo conmutativo. Decimos que  $p \in A$  es primo  $\iff p \neq \mathbf{0} \wedge p \notin \mathcal{U}(A) \wedge \forall a, b \in A$

$$p \mid ab \implies p \mid a \vee p \mid b$$

**Proposición 161.** Sea  $A$  un anillo conmutativo. Sea  $p \in A, p \neq \mathbf{0}, p \notin \mathcal{U}(A)$ .

$$p \text{ primo} \iff \langle p \rangle \text{ es un ideal primo}$$

**Ejemplo 114.** En  $\mathbb{Z}$  (que tiene  $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$ ) todo subanillo  $p\mathbb{Z}$  con  $p$  primo (en el sentido tradicional de la palabra) es un ideal primo.

La definición de primo generaliza para futuras estructuras a la definición de elemento irreducible.

**Definición 70** (Elemento irreducible). Sea  $A$  un DI conmutativo y con unidad y sea  $r \in A$  tal que  $a \neq \mathbf{0} \wedge a \in \mathcal{U}(A)$  (que sea no nulo e invertible). Decimos que  $r$  es irreducible si no puede escribirse como producto de otros dos elementos ninguno de los cuales es invertible:

$$r \in A \text{ irreducible} \iff \forall s, t \in A, r = st \implies s \in \mathcal{U}(A) \vee t \in \mathcal{U}(A) \quad (10.3)$$

Observemos que no puede ocurrir que  $p \in \mathcal{U}(A) \wedge q \in \mathcal{U}(A)$  y que además  $pq = a \notin \mathcal{U}(A)$  (las unidades son un grupo  $\implies$  clausura).

**Proposición 162.** Sea  $p \in A$ .

$$p \text{ primo} \implies p \text{ irreducible}$$

**Definición 71** (Elementos asociados). Sea  $A$  un DI conmutativo y con unidad. Dos elementos  $r, s \in A$  se dicen asociados  $\iff \exists u \in \mathcal{U}(A) \mid r = us$ .

**Proposición 163.** Sea  $A$  un DI. Sean  $a, a' \in A$ . Entonces  $a$  y  $a'$  son asociados  $\iff \langle a \rangle = \langle a' \rangle$ .

**Definición 72** (Dominio de factorización única (DFU)). Sea  $D$  un DI. Diremos que  $D$  es un dominio de factorización única (DFU) si se cumplen las siguientes condiciones  $\forall a \in D$ :

- $a \neq 0 \wedge a \notin \mathcal{U}(D) \implies a = p_1 p_2 \dots p_r$  donde  $p_i$  es irreducible en  $D$
- $a = p_1 p_2 \dots p_r$ ,  $p_i$  irreducible y  $a = q_1 q_2 \dots q_s$ ,  $q_i$  irreducible  $\implies r = s$  y además  $r_i$  y  $q_i$  son asociados para  $i = 1, \dots, r$  (la igualdad es un caso particular de el ser asociados).

Ahora vemos la relación de los DFU con los DIP.

**Proposición 164.** Si  $A$  es un DFU entonces  $A[X]$  es un DFU.

**Teorema 165.** Sea  $A$  un DIP entonces  $a \in A$  es irreducible  $\iff \langle a \rangle$  es maximal.

*Demostración.* Ver [DH96, p. 247]



**Definición 73** (Propiedad de cadena creciente). Diremos que un anillo  $A$  tiene la propiedad de cadena creciente  $\iff$  toda cadena creciente  $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_n \subseteq \dots$  es finita. Es decir, que  $\exists n \mid I_n = I_{n+1} = I_{n+2} = \dots$ .

**Proposición 166.** Si  $D$  es un DIP entonces  $D$  tiene la propiedad de cadena creciente.

La demostración es tan ingenua como uno quiera.

*Demostración.* Sea  $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_n \subseteq \dots$  una cadena de ideales. Sabemos que en cualquier anillo  $\bigcup I_i$  es un ideal. Sea  $J = \langle d \rangle$  para algún  $d \in D$ . Como  $D$  es un DIP ocurre que  $d \in \bigcup I_i \implies d \in I_{n_0} \implies \langle d \rangle \subset I_{n_0} \implies I_{n_0} = I_{n_0+1} = \dots$  ♣

**Teorema 167.** Sea  $A$  un DIP. Entonces  $A$  es un DFU.

*Demostración.* Parece ser que la prueba consiste en ver que si un DI tiene la propiedad de la cadena creciente entonces es un DFU. Utiliza que todos los DIP tienen esta propiedad para probar este teorema. Ver [DH96, p. 248] ♣

**Definición 74** (Dominio euclideo). Sea  $D$  un DI y  $d : D \setminus \{0\} \rightarrow \mathbb{Z} \geq 0$  una aplicación que cumple

1.  $a, b \in D$ ,  $a, b \neq 0 \implies d(a) \leq d(ab)$
2. Si  $b \neq 0$  entonces  $\forall a \in D$ ,  $\exists c, r \in D \mid a = cb + r$  (con posibilidad de que  $r = 0$ ).

Entonces decimos que  $D$  es un dominio euclídeo y lo abreviamos con DE.

**Ejemplo 115.** El anillo  $(\mathbb{Z}, +, \cdot)$  con  $d(a) = |a|$  es un DE.

*Demostración.* Es bien sabido que  $\mathbb{Z}$  es un DI. Comprobamos que  $d$  cumple las propiedades pedidas:

1.  $a, b \in \mathbb{Z}$ ,  $a, b \neq 0 \implies |a| \leq |ab| = |a||b| \geq 1$
2. La segunda propiedad se cumple porque en  $\mathbb{Z}$  tenemos algoritmo de la división<sup>1</sup>



**Ejemplo 116.** Sea  $K$  un cuerpo. El anillo de polinomios  $K[X]$  con la función  $d = \text{gr}$  (el grado) es un DE.

<sup>1</sup>El algoritmo de la división se debe a Euclides, de ahí que esto se llame dominio euclídeo.

*Demostración.*

$$p, q \in K[X], p, q \neq 0 \implies \text{gr } p \leq \text{gr } pq = \text{gr } p + \text{gr } q$$

Tenemos algoritmo de la división:  $\exists g \neq 0, p = qg + r$  con  $\text{gr } r < \text{gr } q$ . ♣

**Teorema 168.** Sea  $D$  un DE. Entonces  $D$  es un DIP. Así, nos queda:

$$\text{DE} \implies \text{DIP} \implies \text{DFU}$$

### 10.3. Factorización e irreducibilidad en anillos de polinomios

**Teorema 169.** [DH96, p. 232] Sea  $K$  un cuerpo y  $p \in K[X]$  un polinomio irreducible. Entonces el ideal generado por  $p$  es maximal en  $K[X]$ .

En particular, si  $p$  es mónico entonces se cumple el recíproco.

**Proposición 170.** Sea  $K$  un cuerpo y  $p \in K[X]$  un polinomio mónico. Entonces  $p$  es irreducible  $\iff \langle p \rangle$  (el ideal generado por  $p$ ) es maximal.

**Proposición 171.** Sea  $p(x) \in K[X]$ . Entonces  $a_0 \in K$  es un 0 de  $p(x)$ , es decir  $p(a_0) = 0 \iff p(x) = (x - a_0)q(x)$  con  $q(x) \in K[X]$ .

**Observación 20.** Si  $p(x)$  es un polinomio de grado  $n$  entonces no puede tener más de  $n$  ceros en  $K$ .

#### 10.3.1. Criterios de irreducibilidad

**Teorema 172.** [DH96, p.222] Sea  $K$  un cuerpo y sea  $f(x) \in K[X]$  un polinomio de grado 2 o 3. Entonces  $f(x)$  es reducible  $\iff f(x)$  tiene una<sup>a</sup> raíz en  $K$ .

<sup>a</sup>Aquí no sé si tiene que ser una o valen varias. Orlando lo da diciendo que  $f(x)$  es irreducible  $\iff f(x)$  no tiene raíces en  $K$ .

**Proposición 173** (Criterio para las raíces de polinomios con coeficientes en  $\mathbb{Z}$ ). Sea  $f(x) = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ . Entonces  $\frac{a}{b} \in \mathbb{Q}$  con  $\text{mcd}(a, b) = 1$  es una raíz de  $f(x)$   $\iff a \mid a_0 \wedge b \mid a_n$ .

**Teorema 174** (Criterio de Eisenstein). Sea  $f(x) = \sum_{j=0}^n a_j X^j \in \mathbb{Z}[X]$  un polinomio. Si existe  $p$  primo tal que  $p \mid a_j, \forall j = 1, \dots, n-1$  y además  $p \nmid a_n \wedge p^2 \nmid a_0$  entonces  $f(x)$  es irreducible en  $\mathbb{Q}[X]$ .

**Proposición 175.** Si  $K[X]$  es un cuerpo entonces todo polinomio mónico de grado 1 es irreducible.

**Observación 21.** En  $K[X] = \mathbb{C}[X]$  todo polinomio mónico irreducible tiene grado 1.

**Observación 22.** En  $K[X] = \mathbb{R}[X]$  todo polinomio mónico irreducible tiene grado 1 o 2.

Esto es, si un primo  $p$  divide a todos los coeficientes menos el primero y el último y además no divide al primero ni su cuadrado divide al último entonces el polinomio es irreducible en  $\mathbb{Q}[X]$ .

#### 10.3.2. Construcción de anillos de polinomios finitos

**Proposición 176.** Sea  $K$  un cuerpo y sea  $f(x) \in K[X]$  un polinomio mónico. Entonces  $K[X]/\langle f(x) \rangle$  es un cuerpo  $\iff \langle f(x) \rangle$  es irreducible.

*Demostración.* Viene de la proposición proposición 168 que vale para polinomios mónicos. ♣

**Teorema 177.** Sea  $K$  un cuerpo y sea  $f(x) = \sum_{j=0}^n a_j X^j \in K[X]$  un polinomio mónico irreducible. Entonces  $K[X]/\langle f(x) \rangle$  es un  $K$ -espacio vectorial con base  $\{1, X, X^2, \dots, X^n\}$  y por tanto de dimensión  $n$ .

Por analogía a cómo se mueven los números en la página 202 de Santorum obtenemos:

**Proposición 178.** Sea  $K$  cuerpo de dimensión  $k$ ,  $f(x)$  un polinomio mónico irreducible de grado  $n$  en  $K[X]$ . Entonces  $|K[X]/\langle f(x) \rangle| = k^n$ .



# Capítulo 11

## Por clasificar

### 11.1. Clase de equivalencia por el grupo de biyecciones

**Definición 75** (Clase de equivalencia por el grupo de biyecciones). Sea  $(G, *)$  un grupo,  $X$  un conjunto,  $Biy(X) = \{f \mid f : X \longrightarrow X \text{ biyección}\}$ , y  $\alpha : G \longrightarrow Biy(X)$  es un homomorfismo de grupos. Definimos la siguiente relación de equivalencia:

$$a \mathcal{R} b \text{ si } \exists g \mid \alpha(g)a = b$$

Por esta relación, definimos la **clase** de equivalencia de un elemento  $a \in X$  como:

$$cl(a) = \{\alpha(g)(a) \mid g \in G\} \ni a$$

Para poder definirlo mejor nos gustaría saber cuantos elementos existen en  $cl(a)$ . Para ello nos ayudaremos del *centralizador de  $a$*  (definición 23). En nuestro caso particular, el centralizador es:

$$C_G(a) = \{g \in G \mid \alpha(g)(a) = a\}$$

Es fácil ver que si  $g \in C_G(a)$  y  $g' \in C_G(a)$  entonces  $g * g' = C_G(a)$ .

**Teorema 179** (Orden de la clase de equivalencia de un elemento). Sea  $(G, *)$  un grupo,  $C(a)$  el centralizador de  $a$  y  $cl(a)$  la clase de equivalencia de  $a$ :

$$|cl(a)| = [G : C(a)]$$

- 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 117** (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:

$$S_4 = cl((1234)) \cap cl((1223)) \cap cl((12)(34)) \cap cl((12)) \cap cl(Id)$$

$$|S_4| = |cl((1234))| \cap |cl((1223))| \cap |cl((12)(34))| \cap |cl((12))| \cap |cl(Id)|$$

- 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  $C((123)) = \langle(123)\rangle$ .

- 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 3.3.1). 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>1</sup>.

$$(1324)(12)(34)(1324)^{-1}$$

$$(34)(21)$$

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>2</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:

$$\langle(1324)\rangle = \{(1324), (12)(23), (4321), Id\}$$

$$\langle(12)\rangle = \{(12), Id\}$$

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

<sup>1</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>2</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.



- 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 considerabamos  $G_1 \times G_2$  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).

Observación:

$$\gamma : G \xrightarrow{\text{Int}} \text{Aut}(G)$$

$\gamma$  es un homomorfismo de grupos que lleva cada elemento  $g \in G$  al automorfismo conjugación  $\gamma_g(x) = gxg^{-1}$ . Observamos que si  $N \triangleleft G$ ,  $\forall g \in G, \gamma_g(N) = gNg^{-1} = N$ .

**Proposición 180.**  $N$  es normal en  $G$  ( $N \triangleleft G$ ) sí y solo sí al restringir  $\phi_g$  a  $N$  la imagen es  $N$ :

$$\begin{array}{c} G \xrightarrow{\gamma_g} G \\ N \xrightarrow{\gamma_g|_N} N \end{array}$$

Es decir, que si  $N$  es normal,  $\gamma_g|_N$  induce un isomorfismo  $\gamma_g|_N : N \rightarrow N$ .

*Demostración.* Cristalina de la definición de subgrupo normal.



En general, al restringir  $\gamma_g$  a un subgrupo de  $G$  no tenemos esta propiedad.

Además, si  $N \triangleleft G$  tiene sentido restringir  $\gamma : G \xrightarrow{\text{Int}} \text{Aut}(G)$  a  $\text{Aut}(N)$  y la restricción da un homomorfismo.

## 11.2. Por revisar

**Teorema 181.** Dado el anillo  $A$  y un ideal propio  $I$

$$\pi : A \rightarrow A/I, \quad I \subset \pi^{-1}(\bar{J}) \subset A, \quad \bar{0} \in \bar{J} \subset A/I$$

existe una identificación entre el retículo de ideales  $A/I$  con el subretículo de ideales de  $A$  que contienen a  $I$ .  
Es decir, si  $J$  es un ideal en  $A/I$  entonces  $\pi^{-1}(\bar{J})$  es un ideal en  $A$  que contiene al ideal  $I$ .

El ideal cero de  $A/I$  tiene contraimagen  $\pi^{-1}(\{0\}) = I$ . Si  $\bar{J}$  es un ideal en  $A/I$

$$\pi : A \rightarrow A/I \rightarrow (A/I)/\bar{J}$$

es un homomorfismo de anillos (la composición de homomorfismos de anillos es un homomorfismo de anillos).  $\pi^{-1}(\bar{J}) = \ker$  de la composición.

**Teorema 182.** Sea  $\alpha : A \rightarrow B$  un homomorfismo de anillos.

- $\ker \alpha$  es un ideal
- $\text{Im } \alpha$  es un subanillo
- $\alpha$  es sobreyectivo  $\iff \text{Im } \alpha = B$
- $\alpha$  es inyectivo  $\iff \ker \alpha = \{0\}$

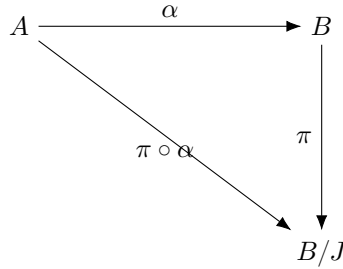
**Definición 76** (Isomorfismo de anillos). Un homomorfismo de anillos  $\alpha : A \rightarrow B$  es un isomorfismo cuando es una biyección. En este caso decimos que  $A$  y  $B$  son isomorfos y lo notamos con  $A \simeq B$ .

**Proposición 183.** Si  $\alpha : A \rightarrow B$  es un homomorfismo de anillos y una biyección de conjuntos entonces  $\alpha^{-1} : B \rightarrow A$  es nuevamente un homomorfismo de anillos.

## Homomorfismos de anillos e ideales

**Teorema 184.** Sea  $\alpha : A \rightarrow B$  un homomorfismo de anillos. Entonces

1. Si  $J \subset B$  es un ideal en  $B$  entonces  $\alpha^{-1}(J)$  es un ideal en  $A$ .
2. Si  $\alpha$  es sobreyectiva entonces la imagen  $\alpha(I)$  de un ideal  $I \subset A$  es un ideal en  $B$



*Demostración.* 1.  $\alpha^{-1}(J) = \ker(\pi \circ \alpha)$  y por tanto es un ideal.

2. Probamos las propiedades de los ideales:

- a)  $\alpha(0) = 0 \in \alpha(I)$
- b) Sean  $b_1, b_2 \in \alpha(I)$  tenemos que ver que  $b_1 + b_2 \in \alpha(I)$ . Sean  $a_1, a_2 \in I$  tales que  $b_1 = \alpha(a_1)$  y  $b_2 = \alpha(a_2)$ . Por ser  $\alpha$  h. de anillos tenemos que  $b_1 + b_2 = \alpha(a_1 + a_2) = \alpha(a_1) + \alpha(a_2)$ .
- c) Sean  $b \in B$ ,  $b' \in \alpha(I)$ . Tenemos que probar que  $bb' \in \alpha(I)$ . Sabemos que  $b' \in \alpha(I) \iff b' = \alpha(a)$ ,  $a \in I$ . Como  $b \in B$  y  $\alpha$  es sobre tiene que existir  $d \in I$  tal que  $\alpha(d) = b$ . Por tanto  $\alpha(d \cdot a) = b \cdot b' \implies bb' \in \alpha(I)$ .

♣

Fijado  $I \subset A$  consideramos  $\pi : A \rightarrow A/I$  que es un homomorfismo de anillos sobreyectivo.

1. Si  $\bar{J} \subset A/I$  es un ideal en  $A/I$  entonces  $\pi^{-1}(\bar{J})$  es un ideal en  $A$  que contiene a  $I$ .
  2. Si  $J$  es un ideal en  $A$  entonces  $\pi(J)$  es un ideal en  $A/I$  y  $J \subseteq \pi^{-1}(\pi(J))$  (es claro porque si  $j \in J$  entonces  $\pi(j) \in \pi(J)$ ).
- a) Además, si  $I \subseteq J$  entonces  $J = \pi^{-1}(\pi(J))$ .

*Demostración.* Si  $\delta \in \pi^{-1}(\pi(J)) \implies \delta \in J$ . Además,  $\delta \in \pi^{-1}(\pi(J)) \iff \pi(\delta) \in \pi(J) \iff \pi(\delta) = \pi(d_1)$ ,  $d_1 \in J \iff \delta - d_1 \in \ker \pi = I$ . Tomamos

$$\delta = \underbrace{(\delta - d_1)}_{\in I} + \underbrace{d_1}_{\in J} \in J$$

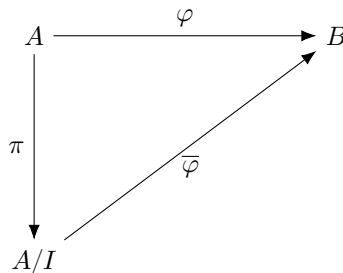
porque  $I \subset J$ .

♣

La siguiente proposición nos llevará al primer teorema de la isomorfía.

**Proposición 185.** Sea  $\varphi : A \rightarrow B$  un homomorfismo de anillos con  $\ker \varphi$  ideal en  $A$ . Sea  $I$  un ideal en  $A$  con  $I \subset \ker \varphi$ .

- Existe un único homomorfismo de anillos  $\bar{\varphi} : A/I \rightarrow B$  tal que  $\varphi = \bar{\varphi} \circ \pi$ .



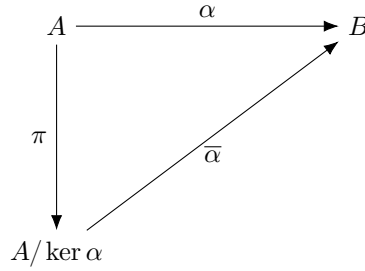
*Demostración.* Definimos  $\bar{\varphi}(\bar{a}) = \varphi(a)$ . Aunque choque (porque el  $\bar{a}$  puede venir de muchos  $a$ ) aseguramos que  $\bar{\varphi}$  está bien definida. Veamos por qué. Sabemos que  $a'$  y  $a$  definen el mismo elemento en  $A/I \iff a' - a \in I$ . Spongamos que  $I \subset \ker \varphi$ . Entonces  $\varphi(a - a') = 0 \iff \varphi(a) - \varphi(a') = 0 \implies \bar{\varphi}$  está bien definida como función.

Veamos ahora que en efecto se cumple que  $\bar{\varphi}$  es un homomorfismo de anillos, es decir que  $\bar{\varphi}(\bar{a} + \bar{b}) = \bar{\varphi}(\bar{a}) + \bar{\varphi}(\bar{b})$ . Recordando la definición que hemos dado de  $\varphi$  y la propiedad  $\bar{a} + \bar{b} = \overline{a + b}$  es claro que  $\bar{\varphi}(\bar{a} + \bar{b}) = \bar{\varphi}(\overline{a + b}) = \varphi(a + b) = \varphi(a) + \varphi(b) = \bar{\varphi}(\bar{a}) + \bar{\varphi}(\bar{b})$ . Es análogo para el producto ya que  $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ . ♣

■  $\ker \bar{\varphi} = \ker \varphi / I$

*Demostración.* Sea  $\bar{a} \in A/I$ . Entonces  $\bar{a} \in \ker \bar{\varphi} \iff \bar{\varphi}(\bar{a}) = 0 \iff \varphi(a) = 0 \iff a \in \ker \varphi$ . ♣

**Teorema 186** (Primer teorema de la isomorfía (anillos)). Si  $\alpha : A \rightarrow B$  es un homomorfismo de anillos sobreyectivo entonces  $B \simeq A / \ker \alpha$ .



*Demostración.* Nos apoyamos en la proposición anterior tomando  $I = \ker \alpha$ . Como  $\alpha$  y  $\pi$  son sobreyectivas tenemos que  $\bar{\alpha}$  es sobreyectiva. Aplicando el segundo resultado de la proposición anterior tenemos que  $\ker \bar{\alpha} = \ker \alpha / \ker \alpha = \{0\} \implies \bar{\alpha}$  es inyectiva. Concluimos que  $\bar{\alpha}$  es un isomorfismo de anillos y por tanto  $B \simeq A / \ker \alpha$ . ♣



# Parte III

## Apéndices



# Apéndice A

## Ejercicios

### A.1. Hoja 1

**Ejercicio (H1.2).** Sean  $a, b, c \in G = (-1, 1)$ . Probamos las propiedades de los grupos.

■ **Asociatividad:**

$$(a * b) * c = \left( \frac{a+b}{1+ab} \right) * c = \frac{\left( \frac{a+b}{1+ab} \right) + c}{1 + \left( \frac{a+b}{1+ab} \right) c} = \frac{\frac{a+b+c+abc}{1+ab}}{\frac{1+ab+ac+bc}{1+ab}} = \frac{a+b+c+abc}{1+ab+ac+bc}$$
$$a * (b * c) = a * \left( \frac{b+c}{1+bc} \right) = \frac{a + \left( \frac{b+c}{1+bc} \right)}{1 + a \left( \frac{b+c}{1+bc} \right)} = \frac{\frac{a+b+c+abc}{1+bc}}{\frac{1+ab+ac+bc}{1+bc}} = \frac{a+b+c+abc}{1+ab+ac+bc}$$

- **Elemento neutro:** es el 0 ya que  $x * 0 = \frac{x+0}{1+x \cdot 0} = \frac{x}{1} = x$  y además  $0 * x = \frac{0+x}{1+0 \cdot x} = \frac{x}{1} = x$
- **Elemento inverso:** la ecuación

$$x * x^{-1} = 0 \iff \frac{x + x^{-1}}{1 + x x^{-1}} = 0 \iff x^{-1} = -x$$

siempre tiene solución y ocurre lo mismo para la ecuación  $x^{-1} * x = 0 \iff x^{-1} = -x$

- **Clausura:** tenemos que probar que si  $x, y \in (-1, 1)$  entonces  $x * y \in (-1, 1)$ . Consideramos  $f(x, y) = x * y = \frac{x+y}{1+xy}$ . Derivando tenemos que  $\nabla f(x, y) = \left( \frac{1}{(1+xy)^2}, \frac{1}{(1+xy)^2} \right) \neq 0, \forall x, y \in [-1, 1] \times [-1, 1]$ . Si el máximo no se alcanza en ningún sitio de dentro del cuadrado  $(-1, 1) \times (-1, 1)$  se tendrá que alcanzar en el borde.
  - Fijado  $x = 1$  tenemos que  $f(1, y) = \frac{1+y}{1+y} = 1 \implies f(1, -1 < y < 1) < 1$  porque si  $f(1, -1 < y < 1)$  tomara un valor mayor que 1 habría un máximo en  $(-1, 1) \times (-1, 1)$  y esto no puede ser pues  $\nabla f$  no se anula en el cuadrado.
  - Fijado  $x = -1$  tenemos que  $f(-1, y) = \frac{y-1}{1-y} = -1 \implies f(-1, -1 < y < 1) > -1$  por la misma razón que antes.
  - Hacemos lo mismo fijando la  $y$  y variando la  $x$ .

En el borde (que no está incluido) se alcanzan máximo y mínimo que acotan a  $f$  en el cuadrado:

$$-1 < f(x, y) = x * y < 1, \quad \forall x, y \in G$$

**Ejercicio (H1.3).** Hallar los inversos de los siguientes elementos, cada uno en su grupo correspondiente:

1.  $o(\overline{11})$  en  $\mathcal{U}(\mathbb{Z}^*/23\mathbb{Z})$
2.  $o(\overline{5})$  en  $\mathcal{U}(\mathbb{Z}^*/31\mathbb{Z})$

*Demostración.* Por el pequeño teorema de Fermat ([oM]) tenemos que  $a^{p-1} \equiv 1 \pmod{p}$  para  $p$  primo. Entonces

$$11^2 2 \equiv 1 \pmod{23} \implies o(\overline{11}) = 22 \implies \overline{11}^{-1} = \overline{11}^{21}$$
$$5^2 0 \equiv 1 \pmod{31} \implies o(\overline{5}) = 30 \implies \overline{5}^{-1} = \overline{5}^{29}$$



**Ejercicio (H1.33).** 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  $gag^{-1} = a \implies ga = ag \implies a \in Z(G)$ . ♣

**Ejercicio (H1.31).** Sea  $G$  un grupo de orden 8. Probad que o bien  $G$  es cíclico o  $a^4 = 1$ , para cada  $a \in G$ .

*Demostración.* Tenemos que probar que  $G$  cíclico XOR  $\forall a \in G, a^4 = 1$ . Probamos dos implicaciones:

- $G$  cíclico  $\implies \exists a \in G \mid a^4 \neq 1$ . Si  $G$  es cíclico entonces  $\exists g \in G \mid o(g) = 8 \implies o(g^4) = \frac{o(g)}{\gcd(o(g), 4)} = \frac{8}{\gcd(8, 4)} = 2$ .
- Si para todo  $a \in G, a^4 = 1$  entonces no hay ningún  $g \in G \mid o(g) = 8$  luego  $G$  no puede estar generado por ningún elemento y por tanto no es cíclico. ♣

**Ejercicio (H1.33).** Sea  $H$  un grupo. Suponed que existe un único  $a \in G$  de orden 2. Demostrad que  $a \in Z(G)$ .

*Demostración.* Sabemos que  $Z(G) = \{a \in G \mid ag = ga, \forall g \in G\}$  y además  $ag = ga \iff a = gag^{-1}$ . Definimos  $\varphi_g(a) = gag^{-1}$  (el isomorfismo conjugación) que es un isomorfismo  $\forall g \in G \implies o(\varphi_g(a)) = o(a), \forall g \in G$ . Si  $a$  es el único elemento de orden 2 entonces necesariamente  $\varphi_g(a) = a, \forall g \in G \implies a = gag^{-1} \implies ag = ga \implies a \in Z(G)$ . ♣

## A.2. Hoja 2

**Ejercicio (H2.1).** Se considera el tercer grupo diédrico  $D_3$ . Se pide hallar lo siguiente:

1. Las clases de conjugación de cada uno de sus elementos.

*Demostración.* Las clases dan una partición del grupo. Si un elemento pertenece a una clase, entonces la clase de ese elemento también es la clase a la que pertenece.

- $cl(e) = \{e\}$
- $cl(B)$ ? Sabemos que  $|cl(B)| = [G : C(B)]$ . Sabemos que  $\langle B \rangle = \{1, B, B^2\} \subset C(B)$  luego  $|C(B)| \geq 3$ . Si hubiera más elementos en  $C(B)$  tendríamos que  $|C(B)| = 6$  pues  $C(B) < D_3$ . Esto no ocurre porque sabemos que  $B$  no conmuta con todos los demás elementos. Por ejemplo  $BA \neq AB$ . Por tanto  $|C(B)| = 3 \implies |cl(B)| = [D_3 : C(B)] = 6/3 = 2$ . Es claro que  $B \in cl(B)$ . Además, como  $cl(B)$  contiene elementos transformados por el isomorfismo conjugación sabemos que el otro elemento que hay tiene orden 3. El único elemento que queda de orden 3 es  $B^2 \implies cl(B) = \{B, B^2\}$ .
- $cl(A)$ ? Sabemos que  $A$  no conmuta con todos ( $A \notin Z(D_3)$ ) luego  $|C(A)| < 6$ . Sabemos que  $\langle A \rangle = \{1, A\} < C(A)$ . Además, como  $C(A)$  es un (sub)grupo sabemos que no puede haber más elementos porque si los hubiera,  $|\langle A \rangle| \mid |C(A)| \implies C(A) \geq 6$  pero ya hemos visto que no puede ser. Es decir que  $|cl(A)| = [D_3 : C(A)] = 6/2 = 3$ . Por tanto  $cl(A)$  incluye los 3 elementos que nos quedan:  $cl(A) = \{A, AB, AB^2\}$ . ♣

2. Los elementos de  $\text{Int}(D_3)$ .
3. Los centralizadores  $C_{D_3}(x)$  para cada  $x \in D_3$
4. Los normalizadores  $N(H)$  para cada  $H < D_3$ .

**Ejercicio (H2.2).** *Demostración.* Obtenidas las clases en el ejercicio H2.1 se verifica que  $|D_3| = |cl(e)| + |cl(B)| + |cl(A)| = 1 + 2 + 3 = 6$ . ♣

**Ejercicio (H2.6).** Sea  $G$  un grupo. ¿Verdadero o falso?

1.  $H < G$  y  $H$  conmutativo implica  $H \triangleleft G$ .
2.  $H < G$  y  $|H| = 2$  implica  $H \triangleleft G$ .
3. Si  $\varphi : G \rightarrow G_1$  es un homomorfismo de grupos, entonces  $\text{Im } \varphi \triangleleft G$
4. Si  $H \triangleleft K$  y  $K \triangleleft G$  entonces  $H \triangleleft G$
5. Si  $H \triangleleft G$  y  $|H| = m$  entonces  $H$  es el único subgrupo de  $G$  de orden  $m$ .
6. Si  $H \triangleleft G$  entonces  $H < Z(G)$ .

*FALSO.* Contraejemplo: En  $G = D_4$  tomamos  $H = \langle B^2 \rangle = \{1, B, B^2, B^3\} \not\subset Z(D_4) = \{1, B^2\}$ . ♣



**Ejercicio (H2.10).** *Demostración.* Fijado  $n$  y definida  $\alpha_n : G \rightarrow G$ ,  $x \mapsto x^n$  tenemos que  $\alpha_n$  es un homomorfismo de grupos. Además podemos expresar  $H_2 = \ker \alpha_n \implies H_2 \triangleleft G$ . Además también tenemos que  $H_1 = \text{Im } \alpha_n < G$ . Veamos que  $H_1 \triangleleft G$ . Es decir, que  $gH_1g^{-1} = H_1$ ,  $\forall g \in G$ . Para ello tomamos  $x_1^n \in H_1$  y lo conjugamos  $gx_1^n g^{-1} = (gx_1 g^{-1})^n$  por ser  $\alpha$  homomorfismo de grupos. En particular  $(gx_1 g^{-1})^n \in \text{Im } \alpha \implies (gx_1 g^{-1})^n \in H_1 \implies (gx_1 g^{-1})^n = x_2^n$  para algún  $x_2 \in H_1 \implies H_1 \triangleleft G$ . ♣

**Ejercicio (H2.13).** Si  $A$  es un grupo abeliano con  $n$  elementos y  $k$  es un entero primo con  $n$ , demostrad que la aplicación  $\varphi : A \rightarrow A$  definida por  $\varphi(a) = a^k$  es un isomorfismo.

- $\varphi$  homomorfismo de grupos.

*Demostración.*

$$\varphi(a)\varphi(b) = a^k b^k = (ab)^k = \varphi(ab)$$

♣

- $\varphi$  biyectiva  $\iff \varphi$  inyectiva ya que dominio y codominio coinciden

*Demostración.*  $\ker \varphi = \{a \in A \mid \varphi(a) = a^k = 1\}$ . Probaremos que  $a^k = 1 \iff a = 1$  y por tanto que  $\ker \varphi = \{1\} \implies \varphi$  inyectiva. Sabemos que  $a^k = 1 \iff o(a^k) = 1$ . Sea  $t = o(a) \mid n$ . Distinguiamos dos casos

- Si  $t = 1$  entonces  $a = 1$  y ya está
- Si  $t > 1$  entonces  $o(a^k) = \frac{t}{\text{mcd}(k,t)} = \frac{t}{1} > 1$  contradicción. Luego necesariamente  $t = o(a) = 1$ .

♣

**Ejercicio (H2.22).** Demostrad que si  $G$  es un grupo no conmutativo y tiene orden  $p^3$  ( $p$  un número primo) entonces  $Z(G)$  tiene orden  $p$ .

*Demostración.* Sabemos que  $Z(G) < G \implies |Z(G)| \mid |G| \implies |Z(G)| \in \{1, p, p^2, p^3\}$

- $|Z(G)| \neq p^3$  porque en tal caso  $G$  sería conmutativo
- $|Z(G)| \neq 1$  porque  $G$  es un  $p$ -grupo y por tanto su centro no es el trivial.
- Si  $|Z(G)| = p^2$  entonces  $|G/Z(G)| = p \implies G/Z(G)$  es cíclico lo que no es posible si  $G$  no es abeliano.

Por descarte concluimos que  $|Z(G)| = p$ .

♣

**Ejercicio (H2.25).** Sabemos que  $\text{Aut}(\mathbb{Z}/12\mathbb{Z}) \simeq \mathcal{U}(\mathbb{Z}^*/12\mathbb{Z})$  donde  $\mathbb{Z}^*/12\mathbb{Z}$  es el grupo multiplicativo  $(\{\bar{1}, \bar{2}, \bar{3}, \dots, \bar{11}\}, \cdot)$ . Queda  $\mathcal{U}(\mathbb{Z}^*/12\mathbb{Z}) = (\{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}, \cdot)$  y además da la casualidad que  $\forall x \in \mathcal{U}(\mathbb{Z}^*/12\mathbb{Z})$ ,  $o(x) = 2$  (todos los elementos son su propio inverso) por lo que no tenemos restricciones al definir  $f : \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/12\mathbb{Z})$ :

$$\begin{aligned} f : \mathbb{Z}/2\mathbb{Z} &\rightarrow \text{Aut}(\mathbb{Z}/12\mathbb{Z}) \simeq \mathcal{U}(\mathbb{Z}^*/12\mathbb{Z}) \\ e = \bar{0} &\mapsto 1 \\ \bar{1} &\mapsto \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\} \end{aligned}$$

**Ejercicio (H2.26).** Sea  $|G_1| = m$ ,  $|G_2| = n$ ,  $\text{mcd}(m, n) = 1$ . Si  $f : G_1 \rightarrow G_2$  es h. de g. sabemos que  $o(f(a)) \mid o(a)$ ,  $\forall a \in G_1$ . Además  $o(a) \mid m \wedge o(f(a)) \mid n$  por el teorema de Lagrange (23).

$$\begin{cases} o(a) \mid m \wedge o(f(a)) \mid n \\ \text{mcd}(m, n) = 1 \\ o(f(a)) \mid o(a) \end{cases} \implies o(a) = o(f(a)) = 1, \forall a \in G_1$$

Por lo que solo puede haber un homomorfismo entre ellos y además es el trivial  $f(a) = e_{G_2}$ .

**Ejercicio (H2.19).** Definimos una función  $f : [0, 2\pi] \subset \mathbb{R} \rightarrow \mathbb{S}^1$ ,  $\alpha \mapsto \cos \alpha + i \sin \alpha$ . Esta función tiene la propiedad de que  $f(\alpha) \cdot f(\alpha') = \cos(\alpha + \alpha') + i \sin(\alpha + \alpha') = f(\alpha + \alpha')$  y por tanto es un h. de g.<sup>1</sup> entre  $\mathbb{R}$  y  $\mathbb{S}^1$ .

Un elemento de  $\cos \alpha + i \sin \alpha \in \mathbb{S}^1$  es de torsión  $\iff \exists n \mid (\cos \alpha + i \sin \alpha)^n = 1$ . Ahora bien  $(\cos \alpha + i \sin \alpha)^n = \cos n\alpha + i \sin n\alpha = 1 \iff n\alpha = k2\pi$ .

<sup>1</sup>A la izquierda (en  $\mathbb{R}$ ) sumamos pero a la derecha (en  $\mathbb{S}^1$ ) multiplicamos.

### A.3. Hoja 4

**Ejercicio** (H4.11). Hallar los subgrupos de Sylow de  $S_5$ . Sabemos que  $|S_5| = 5! = 2^3 \cdot 3 \cdot 5$  y por Primero de Sylow tenemos lo siguiente:

- $\exists P_2, |P_2| = 2^3 = 8$ .
- $\exists P_3, |P_3| = 3$ . Además en  $S_5$  hay  $\binom{5}{3}2! = 20$  3-ciclos y en cada  $gP_3g^{-1} = \{1, a, a^2 \mid o(a) = 3\}$  hay 2 elementos de orden 3 distintos. Además,  $g_1P_3g_1^{-1} \cap g_2P_3g_2^{-1} = \{e\}$  porque si su intersección fuera más grande entonces serían el mismo subgrupo (porque son cíclicos). Es por esto que tenemos que repartir 40 elementos dando 2 a cada 3-grupo con lo que obtenemos  $n_3 = 20/2 = 10$  3-subgrupos de Sylow en  $S_5$ .
- $\exists P_5, |P_5| = 5$ . Además en  $S_5$  hay  $4! = 24$  5-ciclos (elementos de orden 5) y en cada  $gP_5g^{-1} = \{1, a, a^2, a^3, a^4 \mid o(a) = 5\}$  tenemos 4 elementos de orden 5 distintos. Además,  $g_1P_5g_1^{-1} \cap g_2P_5g_2^{-1} = \{e\}$  porque si su intersección fuera más grande entonces serían el mismo. Así, tenemos 24 5-ciclos a repartir entre los diferentes  $gP_5g^{-1}$  dando 4 5-ciclos a cada 1. Por tanto tenemos  $n_5 = 24/4 = 6$  5-subgrupos de Sylow en  $S_5$ .

**Ejercicio** (H4.18). Demostrar que todo grupo de orden  $|G| = 5^3 \cdot 7^3$  tiene un subgrupo normal de orden 125.

*Demostración.* Primero de Sylow  $\implies \exists P_5 < G, |P_5| = 125$ . Tercero de Sylow  $\implies n_5 \mid 7^3 \wedge n_5 \equiv 1 \pmod{5}$  es decir  $n_5 \in \{1, 7, 49, 343\} \wedge n_5 \in \{1, 6, 11, \dots\}$ . Como ni 49 ni 343 son congruentes con 1 módulo 5 tenemos que  $n_5 = 1 \implies P_5 \triangleleft G$ . ♣

**Ejercicio** (H4.20). Hallad todos los grupos abelianos de órdenes 36, 64, 96 y 100.

1.  $|G| = 36 = 2^2 \cdot 3^2$

*Demostración.* Primero de Sylow  $\implies \exists P_2, |P_2| = 4 \wedge \exists P_3, |P_3| = 9$ . Además  $G$  abeliano  $\implies P_2, P_3 \triangleleft G \implies G \simeq P_2 \times P_3$ . Estudiamos los grupos de orden 4 y de orden 9

- $|P_2| = 4$  entonces  $P_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \vee P_2 \simeq \mathbb{Z}/4\mathbb{Z}$
- $|P_3| = 9$  entonces  $P_3 \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \vee P_3 \simeq \mathbb{Z}/9\mathbb{Z}$

Como  $G \simeq P_2 \times P_3$  tenemos 4 posibles grupos abelianos de orden 36. ♣

**Ejercicio** (H4.22). Hallar todos los grupos abelianos de orden 175.

*Demostración.*  $|G| = 5^2 \cdot 7$ . Por el Primero de Sylow tenemos que  $\exists P_5, P_7 < G$  con  $|P_5| = 25, |P_7| = 7$  y además por ser  $G$  abeliano tenemos que  $P_5, P_7 \triangleleft G \implies G \simeq P_5 \times P_7$ . Estudiamos los grupos de orden 25 y de orden 7:

- $|P_5| = 25 \wedge P_5$  abeliano  $\implies P_5 \simeq \mathbb{Z}/25\mathbb{Z} \vee P_5 \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ . En ambos casos  $P_5$  es producto directo de cíclicos pues  $\mathbb{Z}/n\mathbb{Z}$  es cíclico.
- $|P_7| = 7 \wedge P_7$  abeliano  $\implies P_7 \simeq \mathbb{Z}/7\mathbb{Z}$ . Ocurre lo mismo que con  $P_5$ .

Concluimos que  $G \simeq \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \vee G \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ . Los dos casos son abelianos por ser producto directo de grupos cíclicos. ♣

**Ejercicio** (H4.23). ¿Cuántos elementos de orden 3 puede tener un grupo abeliano de orden 36?

*Demostración.*  $|G| = 36 = 2^2 3^2$ . Primero de Sylow  $\implies \exists P_2, P_3 < G, |P_2| = 4, |P_3| = 9$ . Estudiamos los grupos de órdenes 4 y 9:

- $|P_3| = 9 \implies P_3 \simeq \mathbb{Z}/9\mathbb{Z} \vee P_3 \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

♣

### A.4. Hoja 5

**Ejercicio** (H5.1). Demuestra que el conjunto  $(\mathcal{C}([0, 1]), +, \cdot)$ , donde  $\mathcal{C}([0, 1]) := \{f : [0, 1] \rightarrow R \text{ continua}\}$  con las operaciones

$$(f + g)(x) = f(x) + g(x) \qquad (f \cdot g)(x) = f(x) \cdot g(x)$$

es un anillo y di qué tipo de anillo es.

*Solución.* Es claro que la suma es asociativa y conmutativa porque se reduce al caso numérico. Además el elemento neutro aditivo es  $\mathbf{0} := f(x) = 0$ . El producto también es asociativo y conmutativo porque se reduce al caso numérico (para poder hacer estas reducciones es necesario que  $f$  sea continua). ♣

**Ejercicio (H5.2).** Halla las unidades en los siguientes anillos  $\mathbb{Z}[\sqrt{-2}]$ ,  $\mathbb{Z}[\sqrt{-5}]$ ,  $M_2(\mathbb{Q})$ ,  $M_2(\mathbb{Z})$ .

*Demostración.* ■  $\mathcal{U}(M_2(\mathbb{Q})) = \{A \in M_2(\mathbb{Q}) \mid \det A \neq 0\}$ .

- $\mathcal{U}(M_2(\mathbb{Z})) = \{A \in M_2(\mathbb{Z}) \mid \det A = \pm 1\}$ . Esto es porque  $AA^{-1} = \mathbf{1} \implies \det(AA^{-1}) = 1 \implies \det A = \frac{1}{\det A^{-1}}$  pero necesariamente  $\det A \in \mathbb{Z} \implies \det A = \pm 1$ .



**En lo que sigue consideramos anillos conmutativos con unidad, y supondremos que  $1 \neq 0$ .**

**Ejercicio (H5.3).** Demuestra que un cuerpo no tiene divisores de cero.

*Demostración.* Supongamos  $C$  cuerpo y  $a \in C$  divisor de  $0$ . Entonces  $\exists b \in C \mid ab = 0$ . Ahora bien,  $ab \in C \implies \exists(ab)^{-1} \in C \mid (ab)(ab)^{-1} = 1$  pero entonces  $0 \cdot (ab)^{-1} = 1 \implies 0 = 1$  contradicción. ♣

**Ejercicio (H5.4).** Demuestra que en un anillo finito, todo elemento no nulo es una unidad o bien un divisor de cero. Observa, en particular, que un anillo finito es un dominio si y solo si es un cuerpo.

**Ejercicio (H5.6).** Demuestra que si  $A$  es un dominio conmutativo, entonces  $A[X]$  es un dominio conmutativo.

*Demostración.* Supongamos  $A[X]$  no es un dominio conmutativo, es decir, que hay divisores de  $0$ . Entonces  $\exists p, q \in A[X] \mid pq = 0 \implies$  al multiplicar los coeficientes dan  $0$  con lo que nos reducimos al caso de  $A$  que ya es un dominio. ♣

**Ejercicio (H5.7).** Demuestra que el producto  $R_1 \times R_2$  de anillos es un anillo (con las operaciones componente a componente). Indica cuáles son las unidades. Decide si el producto de dos cuerpos es un cuerpo.

Ver proposición 117.

**Ejercicio (H5.9).** Se considera el anillo de los *enteros algebraicos*

$$\mathbb{Z}^{int} = \{\alpha \in \mathbb{C} : p(\alpha) = 0 \text{ para algún } p \in \mathbb{Z}[X] \text{ mónico}\}$$

Demuestra lo siguiente

1.  $\mathbb{Z}^{int} \cap \mathbb{Q} = \mathbb{Z}$

*Demostración.* Veremos que las raíces racionales de  $p$  son en realidad enteras. Sean  $p, q \in \mathbb{Z}$  coprimos con  $q \neq 0$ . Si  $p(\frac{p}{q}) = 0$  se tiene

$$\begin{aligned} p(x) &= x^n + \dots a_1 x + a_0 = 0 \\ p\left(\frac{p}{q}\right) &= \left(\frac{p}{q}\right)^n + \dots + a_1 \left(\frac{p}{q}\right) + a_0 = 0 \\ p^n + \dots + a_n p q^{n-1} + a_0 q^n &= 0 \\ p^n &= q(a_{n-1} + q a_{n-2} + \dots + a_0 q^{n-1}) \\ \implies q &= 1 \implies \frac{p}{q} \in \mathbb{Z} \implies \mathbb{Z}^{int} \cap \mathbb{Q} = \mathbb{Z} \end{aligned}$$



2. el elemento  $2$  de  $\mathbb{Z}^{int}$  no es una unidad ni es irreducible

- Para que  $2$  sea unidad tiene que tener inverso multiplicativo en  $\mathbb{Z}^{int}$ . No es una unidad ya que su inverso es  $\frac{1}{2} \in \mathbb{Q} \implies \frac{1}{2} \notin \mathbb{Z}^{int}$  por el apartado anterior.
- $2$  no es irreducible si encontramos dos  $a, b \in \mathbb{Z}^{int}$  tales que  $ab = 2$  y  $a, b \notin \mathcal{U}(\mathbb{Z}^{int})$ .

**Ejercicio (H5.10).** Demuestra que  $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$  es un subcuerpo de  $\mathbb{C}$ .

**Ejercicio (H5.13).** Demuestra que todo subanillo de un cuerpo es un dominio.

*Demostración.* En un cuerpo no hay divisores de  $0$  por tanto cualquier subconjunto no los tendrá. Por la definición 49 el subanillo es un DI. ♣

**Ejercicio (H5.14).** Sea  $R$  un anillo e  $I$  un ideal de  $R$ . Demuestra que los siguientes subconjuntos de  $R$  son ideales de  $R$ .

1.  $\text{Rad}(I) := \{a \in R : a^n \in I \text{ para algún } n \in \mathbb{N}\}$  (el radical de  $I$ );

*Demostración.* Ver radical de un ideal en Wikipedia. ♣

2.  $\text{Ann}(I) := \{a \in R \mid ax = \mathbf{0}, \text{ para todo } x \in I\}$

*Demostración.*

a)  $\mathbf{0} \in \text{Ann}(I)$ . Sí porque  $\mathbf{0}x = \mathbf{0} \forall x \in I$

b)  $\text{Ann}(I)$  es cerrado por la suma. Sean  $a, b \in \text{Ann}(I)$  entonces  $ax = \mathbf{0}, bx = \mathbf{0} \forall x \in I \implies ax + bx = \mathbf{0} \implies (a + b)x = \mathbf{0} \implies a + b \in \text{Ann}(I)$ . ♣

**Ejercicio (H5.15).** Sea  $R$  un anillo conmutativo con unidad. Demuestra lo siguiente:

1. Si  $I$  es un ideal de  $R$  entonces  $I = R \iff$  existe una unidad de  $R$  en  $I$ .

*Demostración.*  $\exists u \in \mathcal{U}(R), u \in I \implies I = R$ . Por ser  $I$  ideal tenemos que  $\forall a \in R, \forall i \in I, ai \in I$ . Tomando  $a = u$  tenemos que  $au \in I$ . Como esto vale  $\forall a \in R$  tenemos que también valdrá para  $a = u^{-1} \in R$  por ser  $u$  unidad. Por tanto  $uu^{-1} = \mathbf{1} \in I$ . Ahora podemos repetir el proceso para  $i = \mathbf{1}$ . Obtenemos que  $\forall a \in R, a\mathbf{1} \in I \implies I = R$ . ♣

2.  $R$  es un cuerpo  $\iff \{\mathbf{0}\}$  es el único ideal propio de  $R$ .

*Demostración.* Utilizamos el apartado anterior. Si  $R$  es un cuerpo entonces todo elemento excepto el  $\mathbf{0}$  tiene inverso, es decir,  $\forall a \in R, \exists a^{-1} \in R$ . Si  $I$  ideal en  $R$  contiene a cualquier elemento distinto del  $\mathbf{0}$  por el apartado anterior tenemos que  $I = R$ . ♣

**Ejercicio (H5.17).** Encuentra todos los ideales maximales en  $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/10\mathbb{Z}$  y en  $\mathbb{Z}/n\mathbb{Z}$ .

**Ejercicio (H5.21).** Halla el cuerpo de fracciones de los siguientes dominios:

Ver [DH96, p. 208].

**Ejercicio (H5.22).**

Apéndice B

Índices



# Lista de definiciones

1.	Definición (Grupo)	7
2.	Definición (Orden de un elemento)	8
3.	Definición (Orden o cardinalidad de un grupo)	8
4.	Definición (Grupo abeliano)	9
5.	Definición (Subgrupo)	9
6.	Definición (Retículo de subgrupos)	10
7.	Definición (Subgrupo generado varios elementos)	10
8.	Definición (Subgrupo generado por un elemento)	10
9.	Definición (Presentación de un grupo)	11
10.	Definición (Grupo de permutaciones de $n$ elementos)	12
11.	Definición (Grupo cíclico)	14
12.	Definición (Clase lateral)	15
13.	Definición (Índice de un subgrupo en un grupo)	16
14.	Definición (Subgrupo normal)	16
15.	Definición (Conjunto cociente en grupos)	16
16.	Definición (Homomorfismo de grupos)	17
17.	Definición (Núcleo de un homomorfismo)	17
18.	Definición (Imagen de un homomorfismo)	17
19.	Definición (Producto directo de grupos)	23
20.	Definición (Producto libre de grupos)	23
21.	Definición (Conjugados)	29
22.	Definición (Centro de un grupo)	30
23.	Definición (Centralizador de un elemento)	31
24.	Definición (P-grupo)	32
25.	Definición (Normalizador de un subconjunto)	34
26.	Definición (Conjunto de biyecciones)	39
27.	Definición (Ciclo)	40
28.	Definición (Trasposición)	43
29.	Definición (Paridad de una permutación)	44
30.	Definición (Signatura de una permutación)	44
31.	Definición (Tipo de una permutación)	44
32.	Definición (Grupo alternado)	47
33.	Definición (Grupo simple)	47
34.	Definición (P-subgrupo de Sylow)	52
35.	Definición (Suma directa)	59
36.	Definición ( <i>Suma</i> libre de grupos)	59
37.	Definición (Expresión característica)	61
38.	Definición (Anillo)	65
39.	Definición (Anillo con unidad o anillo unitario)	65
40.	Definición (Anillo conmutativo)	65
41.	Definición (Cuerpo (alternativa))	66
42.	Definición (Extensión de anillos)	66
43.	Definición (Unidades en anillos)	67
44.	Definición (Cuerpo)	67
45.	Definición (Subanillo)	67

46.	Definición (Subcuerpo)	67
47.	Definición (Producto directo en anillos)	68
48.	Definición (Divisor de 0)	68
49.	Definición (Dominio de integridad)	69
50.	Definición (Ideal)	69
51.	Definición (Ideal (alternativa))	70
52.	Definición (Ideal generado por un subconjunto)	70
53.	Definición (Ideal principal)	71
54.	Definición (Dominio de ideales principales (DIP))	71
55.	Definición (Ideal primo)	71
56.	Definición (Ideal maximal)	71
57.	Definición (Homomorfismo de anillos)	73
58.	Definición (Isomorfismo de anillos)	73
59.	Definición (Relación de equivalencia por ideales)	74
60.	Definición (Estructura de anillo del cociente)	74
61.	Definición (Retículo de ideales)	75
62.	Definición (Cuerpo de fracciones de un anillo)	78
63.	Definición (Anillo de polinomios)	81
64.	Definición (Polinomio mónico)	81
65.	Definición (Grado de un polinomio)	81
66.	Definición (Divisibilidad)	82
67.	Definición (Divisibilidad)	82
68.	Definición (Primo)	82
69.	Definición (Elemento irreducible)	82
70.	Definición (Elementos asociados)	83
71.	Definición (Dominio de factorización única (DFU))	83
72.	Definición (Propiedad de cadena creciente)	83
73.	Definición (Dominio euclideo)	83
74.	Definición (Clase de equivalencia por el grupo de biyecciones)	87
75.	Definición (Isomorfismo de anillos)	89



# Lista de teoremas

1.	Teorema (Propiedad cancelativa)	8
5.	Teorema (Hoja 1, ejercicio 7)	9
16.	Teorema (Teorema de clasificación de grupos cíclicos)	14
19.	Teorema (Hoja 1, ejercicio 9)	14
23.	Teorema (de Lagrange)	15
36.	Teorema (de correspondencia entre subgrupos mediante homomorfismos)	19
40.	Teorema (Tercer teorema de la isomorfía)	21
43.	Teorema (Cardinalidad del producto libre)	24
46.	Teorema (Grupos notables de distintos órdenes finitos.)	25
60.	Teorema (de Cauchy)	31
87.	Teorema (Igualdad entre subgrupos y grupos alternantes)	48
89.	Teorema (Simplicidad del grupo alternante)	48
90.	Teorema (Grupo producto semidirecto)	49
91.	Teorema (Primero de Sylow)	52
92.	Teorema (Segundo de Sylow)	52
93.	Teorema (Tercero de Sylow)	52
99.	Teorema (de alguien 1)	58
106.	Teorema (de estructura de grupos abelianos finitos)	62
144.	Teorema (de correspondencia entre ideales)	75
148.	Teorema (Primer teorema de la isomorfía para anillos)	77
157.	Teorema (Algoritmo de la división)	82
172.	Teorema (Criterio de Eisenstein)	84
177.	Teorema (Orden de la clase de equivalencia de un elemento)	87
184.	Teorema (Primer teorema de la isomorfía (anillos))	91



# Lista de ejemplos

1.	Ejemplo (Ejemplos de grupos infinitos) . . . . .	7
2.	Ejemplo (Grupo de las clases módulo $n$ ) . . . . .	8
4.	Ejemplo (Retículo de subgrupos $\mathbb{Z}$ ) . . . . .	10
5.	Ejemplo (Grupo de cuaterniones) . . . . .	11
6.	Ejemplo (El famoso grupo $D_4$ ) . . . . .	12
7.	Ejemplo (Grupos diédricos de orden $n$ ) . . . . .	12
10.	Ejemplo (Grupo de biyecciones $S_3$ ) . . . . .	13
12.	Ejemplo (Homomorfismo trivial) . . . . .	18
16.	Ejemplo (Automorfismo conjugación) . . . . .	19
19.	Ejemplo (del primer teorema de la isomorfía) . . . . .	19
20.	Ejemplo (Retículo de subgrupos de $\mathbb{Z}/8\mathbb{Z}$ ) . . . . .	20
25.	Ejemplo (Retículo de subgrupos de $D_4$ ) . . . . .	27
64.	Ejemplo (de aplicación de los teoremas de Sylow) . . . . .	53
83.	Ejemplo (Anillo conmutativo con unidad) . . . . .	66
84.	Ejemplo (Anillo conmutativo sin unidad) . . . . .	66
85.	Ejemplo (Anillo no conmutativo con unidad) . . . . .	66
86.	Ejemplo (Anillo no conmutativo sin unidad) . . . . .	66
109.	Ejemplo (Retículo de ideales de $(\mathbb{Z}, +, \cdot)$ ) . . . . .	77
114.	Ejemplo (Posibles descomposiciones en ciclos de $S_4$ ) . . . . .	87



# Lista de ejercicios

. Ejercicio (H3.8) . . . . .	42
. Ejercicio (H1.2) . . . . .	95
. Ejercicio (H1.3) . . . . .	95
. Ejercicio (H1.33) . . . . .	95
. Ejercicio (H1.31) . . . . .	96
. Ejercicio (H1.33) . . . . .	96
. Ejercicio (H2.1) . . . . .	96
. Ejercicio (H2.2) . . . . .	96
. Ejercicio (H2.6) . . . . .	96
. Ejercicio (H2.10) . . . . .	97
. Ejercicio (H2.13) . . . . .	97
. Ejercicio (H2.22) . . . . .	97
. Ejercicio (H2.25) . . . . .	97
. Ejercicio (H2.26) . . . . .	97
. Ejercicio (H2.19) . . . . .	97
. Ejercicio (H4.11) . . . . .	98
. Ejercicio (H4.18) . . . . .	98
. Ejercicio (H4.20) . . . . .	98
. Ejercicio (H4.22) . . . . .	98
. Ejercicio (H4.23) . . . . .	98
. Ejercicio (H5.1) . . . . .	98
. Ejercicio (H5.2) . . . . .	99
. Ejercicio (H5.3) . . . . .	99
. Ejercicio (H5.4) . . . . .	99
. Ejercicio (H5.6) . . . . .	99
. Ejercicio (H5.7) . . . . .	99
. Ejercicio (H5.9) . . . . .	99
. Ejercicio (H5.10) . . . . .	99
. Ejercicio (H5.13) . . . . .	99
. Ejercicio (H5.14) . . . . .	99
. Ejercicio (H5.15) . . . . .	100
. Ejercicio (H5.17) . . . . .	100
. Ejercicio (H5.21) . . . . .	100
. Ejercicio (H5.22) . . . . .	100



# Glosario

**DE** Dominio euclídeo (ver definición 73). 83

**DFU** Dominio de factorización única (ver definición 71). 83

**DI** Dominio de integridad (ver definición 49). 69, 71, 78, 79, 81–83

**DIP** Dominio de ideales principales (ver definición 54). 71, 82, 83, 102





# Bibliografía

- [DH96] José Dorronsoro and Eugenio Hernandez. *Números, Grupos y Anillos*. Addison-Wesley Iberoamericana, S.A. - Universidad Autónoma de Madrid, 1996.
- [Epp] David Eppstein. Dih4 subgroups.
- [MW] Todd; Moslehian, Mohammad Sal; Rowland and Eric W. Weisstein. Ideal.
- [oM] Encyclopedia of Mathematics. Fermat's little theorem.
- [Wik] Wikipedia. Definición de la presentación de un grupo.