Álgebra II

Foto: José Juan Castro

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra II

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán

Granada, 2025

Índice general

En Álgebra I el objeto principal de estudio fueron los anillos conmutativos, conjuntos en los que teníamos definidas dos operaciones, una usualmente denotada con notación aditiva y otra con notación multiplicativa.

Posteriormente, el estudio se centró en los dominios de integridad (DI), anillos conmutativos donde teníamos más propiedades con las que manejar nuestros elementos (como la tan característica propiedad cancelativa). Después, el objeto de estudio fueron los dominios euclídeos (DE), donde ya podíamos realizar un estudio sobre la divisibilidad de los elementos del conjunto.

Finalmente, nos centramos en los dominios de factorización única (DFU), donde realizamos una breve introducción a la irreducibilidad de los polinomios.

En esta asignatura el principal objeto de estudio serán los grupos, conjuntos en los que hay definida una sola operación que entendemos por "buena[1]". Por tanto, los grupos serán estructuras menos restrictivas que los anillos conmutativos, aunque su estudio no será menos interesante.

Los dos primeros temas nos ofrecen una introducción a los grupos, dando muchos ejemplos de grupos y varias propiedades útiles sobre estos. El tercer tema nos proporciona los teoremas de isomorfía, teoremas importantes en la teoría de grupos que nos permitirán empezar a realizar un estudio interesante de los grupos; Aprenderemos en dicho tema a manejar especialmente los grupos cocientes. El cuarto tema nos introduce los grupos resolubles, una propiedad que puede cumplir o no un grupo, que nos servirá en el futuro del estudio de las ecuaciones con radicales. Podemos decir que el quinto tema es el último dedicado al estudio genérico de los grupos, que nos proporciona dos herramientas para el estudio de los grupos, los $G-$conjuntos y los $p-$grupos. En particular, estaremos interesados en el estudio de los $p-$subgrupos de Sylow de un grupo dado, ya que nos permitirán conocer muy bien la estructura de ciertos grupos a partir de poca información sobre ellos.

Finalmente, los dos últimos temas están dedicados a la clasificación de grupos finitos: dado un grupo de cierto orden, ¿cuántos grupos de dicho orden existen? Seremos capaces de responder a esta pregunta siempre en el caso de que el grupo sea abeliano y realizaremos un estudio de lo que les sucede a los grupos no abelianos de orden menor o igual que 15, con lo que al final de la asignatura sabremos clasificar todos los grupos de orden menor o igual que 15.

Debido a la brevedad de este curso y a la gran utilidad del concepto que ahora comentaremos, no se mencionará nada sobre **grupos libres**, un concepto que nos permite definir lo que es la presentación de un grupo. Pese a no usar grupos libres, sí que usaremos presentaciones de grupo, ya que su utilidad nos permite desarrollar un trabajo más cómodo en la teoría que introduciremos. Animamos al lector a consultar la parte de la teoría de grupos que estudia los grupos libres, así como a, tras la superación de esta asignatura, leer sobre Clasificación de Grupos y profundizar más en la Teoría de Grupos. La Teoría de Grupos tiene amplias aplicaciones, tanto dentro como fuera de las matemáticas (criptografía, física, química, ...), por lo que el tiempo dedicado a su estudio no debe ser menospreciado.

[1] La operación cumplirá ciertas propiedades deseables.

1. Grupos: definición, generalidades y ejemplos

Comenzamos realizando la primera definición necesaria para entender el concepto de grupo, que es entender qué es una operación dentro de un conjunto.

Definición 1.1 (Operación binaria)**.** Sea G un conjunto, una operación binaria en G es una aplicación

$$\begin{array}{rccc} * : & G \times G & \longrightarrow & G \\ & (a,b) & \longmapsto & a * b \end{array}$$

Ejemplo. Ejemplos de operaciones binarias sobre conjuntos que ya conocemos son:

1. La suma y el producto de números en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}, \mathbb{C}$.
2. Dado un conjunto X, los operadores $\cap$ y $\cup$ son operaciones binarias sobre el conjunto $\mathcal{P}(X)$.

Antes de dar la definición de grupo, daremos la de monoide, que es menos restrictiva que la de grupo.

Definición 1.2 (Monoide)**.** Un monoide es una tripleta $(G, *, e)$ donde G es un conjunto no vacío, $*$ es una operación binaria en G y e es un elemento destacado de G de forma que se verifica:

i) La propiedad asociativa de $*$:

$$(x * y) * z = x * (y * z) \qquad \forall x, y, z \in G$$

ii) La existencia de un elemento neutro (el elemento destacado de G):

$$\exists e \in G \mid e * x = x * e = x \qquad \forall x \in G$$

Proposición 1.1. *En un monoide, el elemento neutro es único.*

Demostración. Sea $(G, *, e)$ un monoide y sea $f \in G$ tal que $f * x = x * f = x$ $\forall x \in G$:

$$f = f * e = e$$

$\square$

Ejemplo. Ejemplos de monoides ya conocidos son:

1. $(\mathbb{N}, +, 0)$, $(\mathbb{N}, \cdot, 1)$

2. Dado un conjunto X: $(\mathcal{P}(X), \cap, X)$, $(\mathcal{P}(X), \cup, \emptyset)$

Definición 1.3 (Grupo)**.** Un grupo es una tripleta $(G, *, e)$ donde G es un conjunto no vacío, $*$ es una operación binaria en G y e es un elemento destacado de G de forma que se verifica:

i) La propiedad asociativa de $*$:

$$(x * y) * z = x * (y * z) \qquad \forall x, y, z \in G$$

ii) La existencia de un elemento neutro por la izquierda (el elemento destacado de G):

$$\exists e \in G \mid e * x = x \qquad \forall x \in G$$

iii) La existencia de un elemento simétrico por la izquierda para cada elemento de G:

$$\forall x \in G \quad \exists x' \in G \mid x' * x = e$$

Si además se cumple:

iv) La propiedad conmutativa de $*$:

$$x * y = y * x \qquad \forall x, y \in G$$

Entonces, diremos que $(G, *, e)$ es un grupo conmutativo o abeliano.

Notación. Para una mayor comodidad a la hora de manejar grupos, introducimos las siguientes notaciones:

1. Cuando dado un conjunto no vacío G sepamos por el contexto a qué grupo $(G, *, e)$ nos estamos refiriendo, indicaremos simplemente G (o en algunos casos $(G, *)$, para hacer énfasis en la operación binaria) para referirnos al grupo $(G, *, e)$.

2. En algunos casos, usaremos (por comodidad) la notación multiplicativa de los grupos. De esta forma, dado un grupo $(G, \cdot, 1)$, en ciertos casos notaremos la operación binaria $\cdot$ simplemente por yuxtaposición:

$$x \cdot y = xy \qquad \forall x, y \in G$$

   Además, nos referiremos al elemento neutro como "uno" y al simétrico de cada elemento como "inverso", sustituyendo la notación de x' por la de x^{-1}.

3. Otra notación que también usaremos (aunque de forma menos frecuente que la multiplicativa) será la aditiva. Dado un grupo $(G, +, 0)$, nos referiremos al elemento neutro como "cero" y al simétrico de cada elemento como "opuesto", sustituyendo la notación de x' por la de $-x$.

Ejemplo. Ejemplos de grupos que se usarán con frecuencia en la asignatura son:

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con su respectiva suma son grupos abelianos.

2. $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ con su respectivo producto son grupos abelianos.

   Notemos la importancia de eliminar el 0 de cada conjunto para que todo elemento tenga inverso, así como que $\mathbb{Z}^*$ no es un grupo, ya que el inverso de cada elemento (para el producto al que estamos acostumbrados) no está dentro de $\mathbb{Z}^*$.

3. $\{1, -1, i, -i\} \subseteq \mathbb{C}$ con el producto heredado[1] de $\mathbb{C}$ también es un grupo abeliano.

4. $(\mathcal{M}_2(\mathbb{R}), +)$ es un grupo abeliano.

5. Dado un cuerpo $\mathbb{K}$, el grupo lineal de orden 2 con coeficientes en dicho cuerpo:
$$\mathrm{GL}_2(\mathbb{K}) = \{M \in \mathcal{M}_2(\mathbb{K}) : \det(M) \neq 0\}$$
   con el producto heredado de $\mathcal{M}_2(\mathbb{K})$ es un grupo que no es conmutativo.

6. $\mathbb{Z}_n$ con su suma es un grupo abeliano, $\forall n \in \mathbb{N}$.

7. $\mathcal{U}(\mathbb{Z}_n) = \{[a] \in \mathbb{Z}_n \mid \mathrm{mcd}(a, n) = 1\}$ con el producto es un grupo abeliano, $\forall n \in \mathbb{N}$. También lo notaremos por $\mathbb{Z}_n^\times$.

8. Dado $n \geqslant 1$, consideramos:
$$\begin{aligned}\mu_n = \{\text{raíces complejas de } x^n - 1\} &= \left\{\xi_k = \cos\frac{2k\pi}{n} + i \operatorname{sen}\frac{2k\pi}{n} : k \in \{0, \ldots, n-1\}\right\} \\ &= \left\{1, \xi, \xi^2, \ldots, \xi^{n-1} : \xi = \cos\frac{2\pi}{n} + i \operatorname{sen}\frac{2\pi}{n}\right\}\end{aligned}$$
   Este conjunto es un grupo abeliano con el producto heredado de $\mathbb{C}$.

9. Dado un cuerpo $\mathbb{K}$, el grupo lineal especial de orden 2 sobre dicho cuerpo:
$$\mathrm{SL}_2(\mathbb{K}) = \{M \in \mathcal{M}_2(\mathbb{K}) : \det(M) = 1\}$$
   con el producto heredado de $\mathcal{M}_2(\mathbb{K})$ es un grupo que no es conmutativo.

10. Sean $(G, \square, e), (H, \triangle, f)$ dos grupos, si consideramos sobre $G \times H$ la operación binaria $* : (G \times H) \times (G \times H) \to G \times H$ dada por:
$$(x, u) * (y, v) = (x \square y, u \triangle v) \qquad \forall (x, u), (y, v) \in G \times H$$
    Entonces, $G \times H$ es un grupo, al que llamaremos grupo directo de G y H. Este será abeliano si y solo si G y H lo son.

11. Si X es un conjunto no vacío y consideramos
$$S(X) = \{f : X \to X \mid f \text{ biyectiva}\} = \mathrm{Perm}(X)$$
    es un grupo no abeliano con la operación de composición de funciones $\circ$.

    En el caso en el que X sea finito y tenga n elementos: $X = \{x_1, x_2, \ldots, x_n\}$, notaremos:
$$S_n = S(X)$$

[1] Será común hablar de "operación heredada" cuando consideramos un subconjunto de un conjunto en el que ya hay definida una operación interna, haciendo referencia a la restricción en dominio y recorrido de dicha operación interna al subconjunto considerado.

12. Sea $(G, *, e)$ un grupo y X un conjunto, consideramos el conjunto:

$$\text{Apl}(X, G) = G^X = \{f : X \to G \mid f \text{ aplicación}\}$$

junto con la operación binaria $* : G^X \times G^X \to G^X$ dada por:

$$(f * g)(x) = f(x) * g(x) \qquad \forall x \in X, \quad \forall f, g \in G^X$$

Entonces, $(G^X, *, g)$ es un grupo, con elemento neutro:

$$g(x) = e \qquad \forall x \in X$$

de esta forma, dada $f \in G^X$, la aplicación simétrica de f será:

$$f'(x) = (f(x))' \qquad \forall x \in X$$

Casos a destacar son:

a) Si $X = \emptyset$, entonces $G^X = \{\emptyset\}$.

b) Si $X = \{1, 2\}$, entonces G^X se identifica con $G \times G$.

13. El grupo más pequeño que se puede considerar es el único grupo válido sobre un conjunto unitario $X = \{e\}$. Es decir, el grupo $(X, *, e)$ con $X = \{e\}$ y $* : X \times X \to X$ dada por:

$$e * e = e \qquad e \in X$$

A este grupo (independientemente de cual sea el conjunto X, ya que todos tendrán la misma[2] estructura) lo llamaremos grupo trivial.

Ejemplo. Consideramos en $\mathbb{Z}$ la operación binaria $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dada por:

$$a * b = a + b + 1 \qquad \forall a, b \in \mathbb{Z}$$

Donde usamos $+$ para denotar la suma de $\mathbb{Z}$. Se pide demostrar que $(\mathbb{Z}, *)$ es un grupo abeliano.

Demostración. Demostramos cada una de las propiedades de la definición de grupo abeliano:

- La propiedad asociativa de $*$ es consecuencia de las propiedades asociativa y conmutativa de $+$:

$$\begin{gathered}(a * b) * c = (a + b + 1) * c = a + b + 1 + c + 1 = a + b + c + 2 \\ a * (b * c) = a * (b + c + 1) = a + b + c + 1 + 1 = a + b + c + 2 \\ \forall a, b, c \in \mathbb{Z}\end{gathered}$$

[2]Concepto que luego formalizaremos.

- Buscamos $x \in \mathbb{Z}$ de forma que $x * a = a$ para todo $a \in \mathbb{Z}$, por lo que queremos resolver la ecuación:

$$X * a = a \Longleftrightarrow X + a + 1 = a \Longrightarrow X = -1$$

  Por lo que $-1 \in \mathbb{Z}$ es el elemento neutro para $*$:

$$-1 * a = -1 + a + 1 = a \qquad \forall a \in \mathbb{Z}$$

- Fijado $x \in \mathbb{Z}$, tratamos de buscar un elemento simétrico para x, por lo que buscamos resolver la ecuación:

$$X * x = -1 \Longleftrightarrow X + x + 1 = -1 \Longleftrightarrow X = -x - 2$$

  Por lo que dado $x \in \mathbb{Z}$, su elemento simétrico es $-x - 2 \in \mathbb{Z}$:

$$(-x - 2) * x = -x - 2 + x + 1 = -1 \qquad \forall x \in \mathbb{Z}$$

- La propiedad conmutativa de $*$ es consecuencia de la propiedad conmutativa de $+$:

$$a * b = a + b + 1 = b + a + 1 = b * a \qquad \forall a, b \in \mathbb{Z}$$

□

Propiedades

Aunque estas propiedades parezcan ya conocidas y familiares (por ejemplo para el caso $(\mathbb{Z}, +, 0)$), es una buena observación darnos cuenta de que son válidas para **cualquier grupo** que consideremos, por raros y difíciles que sean sus elementos y operación interna.

Proposición 1.2. *Sea $(G, *, e)$ un grupo, destacamos sus primeras propiedades:*

i) $x * x' = e \ \forall x \in G$.

ii) $x * e = x \ \forall x \in G$.

iii) *El elemento neutro de $*$ es único. Simbólicamente:*

$$\exists_1 e \in G \mid e * x = x \qquad \forall x \in G$$

iv) *Fijado $x \in G$, el simétrico de x es único. Simbólicamente:*

$$\forall x \in G \quad \exists_1 x' \in G \mid x' * x = e$$

Demostración. Demostramos cada una a partir de la anterior:

i) En primer lugar, observemos que:

$$x' * (x * x') = (x' * x) * x' = e * x' = x' \tag{1.1}$$

Ahora:

$$x * x' = e * (x * x') = \big((x')' * x'\big) * (x * x') = (x')' * (x' * (x * x')) \overset{(*)}{=} (x')' * x' = e$$

Donde en $(*)$ hemos usado (1.1).

ii) Usando *i*) en $(*)$:

$$x * e = x * (x' * x) = (x * x') * x \overset{(*)}{=} e * x = x$$

iii) Sea $f \in G$ de forma que $f * x = x\ \forall x \in G$, entonces:

$$f = f * e \overset{(*)}{=} e$$

Donde en $(*)$ hemos usado *ii*).

De otra forma, podríamos haber argumentado que gracias a *ii*), todo grupo es un monoide, por lo que podemos aplicar la Proposición 1.1 y ya habríamos terminado.

iv) Dado $x \in G$, sea $x'' \in G$ de forma que $x'' * x = e$, entonces:

$$x'' = x'' * e \overset{(*)}{=} x'' * (x * x') = (x'' * x) * x' = e * x' = x'$$

Donde en $(*)$ hemos usado *i*).

□

Notación. A partir de ahora, dado un grupo $(G, *, e)$, comenzaremos a usar (por comodidad) la notacion multiplicativa de los grupos:

$$xy = x * y \qquad \forall x, y \in G$$

Y denotando a x' (el elemento simétrico de x) por x^{-1}.

Proposición 1.3. *En un grupo G se verifica la propiedad cancelativa (tanto a la izquierda como a la derecha):*

$$\forall x, y, z \in G : \begin{cases} xy = xz \Longrightarrow y = z \\ xy = zy \Longrightarrow x = z \end{cases}$$

Demostración. Para la primera, supongamos que $xy = xz$:

$$y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = ez = z$$

Ahora, para la segunda, supongamos que $xy = zy$ y la demostración es la misma que la anterior pero en el otro sentido y tomando $e = yy^{-1}$.

$$x = xe = x(yy^{-1}) = (xy)y^{-1} = (zy)y^{-1} = z(yy^{-1}) = z$$

□

Proposición 1.4. *Sea G un grupo, entones:*

1. $e^{-1} = e$.
2. $(x^{-1})^{-1} = x$, $\forall x \in G$.
3. $(xy)^{-1} = y^{-1}x^{-1}$, $\forall x, y \in G$.

Demostración. Cada caso se demuestra observando sencillamante que:

1. $ee = e$.
2. $xx^{-1} = e$.
3. $(y^{-1}x^{-1})(xy) = y^{-1}x^{-1}xy = y^{-1}ey = e$.

$\square$

Proposición 1.5. *Sea G un conjunto no vacío con una operación binaria $*$ asociativa, son equivalentes:*

i) *G es un grupo.*

ii) *Para cada par de elementos $a, b \in G$, las ecuaciones[3]:*

$$aX = b \qquad Xa = b$$

Tienen solución en G, es decir: $\exists c, d \in G \mid ac = b \wedge da = b$.

Demostración. Demostramos las dos implicaciones:

i) $\Rightarrow$ *ii)* Tomando $c = a^{-1}b, d = ba^{-1} \in G$ se tiene.

ii) $\Rightarrow$ *i)* Basta demostrar que $\exists e \in G$ con $ex = x$ $\forall x \in G$ y que fijado $x \in G$, entonces $\exists x' \in G$ con $x'x = e$:

1. Dado $a \in G$, sabemos que la ecuación $Xa = a$ tiene solución, por lo que existe $e \in G$ de forma que $ea = a$.

   Veamos que no depende de la elección de a; es decir, que es un elemento neutro para cualquier elemento de G. Para ello, dado cualquier $b \in G$, sabemos que la ecuación $aX = b$ tiene solución, por lo que existirá un $x_b \in G$ de forma que $ax_b = b$. Finalmente:

   $$eb = e(ax_b) = (ea)x_b = ax_b = b \qquad \forall b \in G$$

2. Fijado $x \in G$, sabemos que la ecuación $Xx = e$ tiene solución, por lo que existe $x' \in G$ de forma que $x'x = e$, para cualquier $x \in G$.

$\square$

Proposición 1.6 (Ley asociativa general)**.** *Sea G un grupo, dados $n, m \in \mathbb{N}$ con $n > m > 0$, se tiene que:*

$$\left(\prod_{i=1}^{m} x_i\right)\left(\prod_{i=m+1}^{n} x_i\right) = \prod_{i=1}^{n} x_i \qquad \forall x_i \in G, \quad i \in \{1, \dots, n\}$$

Demostración. Por inducción sobre $n \in \mathbb{N}$:

- Para $n = 0, n = 1$: No hay nada que probar: $\nexists m \in \mathbb{N}$ con $0 < m < n$.

[3] Donde hemos usado X para denotar la incógnita y que no se confunda con un elemento de G.

- Para $n = 2$: Dado $m \in \mathbb{N}$ con $0 < m < n$ (entonces $m = 1$):

$$\left(\prod_{i=1}^{m} x_i\right)\left(\prod_{i=m+1}^{n} x_i\right) = x_1 x_2 = \prod_{i=1}^{n} x_i \qquad \forall x_1, x_2 \in G$$

- Supuesto para n, veámoslo para $n+1$: Dado $m \in \mathbb{N}$ con $0 < m < n+1$:

$$\begin{aligned}\left(\prod_{i=1}^{m} x_i\right)\left(\prod_{i=m+1}^{n+1} x_i\right) &= \left[x_1\left(\prod_{i=2}^{m} x_i\right)\right]\left[\left(\prod_{i=m+1}^{n} x_i\right)x_{n+1}\right] \\ &= x_1\left(\prod_{i=2}^{m} x_i \prod_{i=m+1}^{n} x_i\right)x_{n+1} \overset{(*)}{=} x_1\left(\prod_{i=2}^{n} x_i\right)x_{n+1} = \prod_{i=1}^{n+1} x_i \\ &\forall x_i \in G, \quad i \in \{1, \ldots, n+1\}\end{aligned}$$

  Donde en $(*)$ hemos usado la hipótesis de inducción, ya que $0 < m-1 < n$.

□

Definición 1.4 (Potencia)**.** Sea $(G, \cdot, e)$ un grupo, dado $x \in G$ y $n \in \mathbb{Z}$, podemos definir:

$$x^n = \begin{cases} \prod\limits_{i=1}^{n} x & \text{si } n > 0 \\ e & \text{si } n = 0 \\ (x^{-1})^{-n} & \text{si } n < 0 \end{cases}$$

Notación. En grupos aditivos $(G, +, 0)$, en lugar de x^n escribiremos $n \cdot x$, que se define de igual forma pero en el caso $n > 0$, en lugar de escribir $\prod$, escribiremos $\sum$.

Proposición 1.7. *Sea G un grupo, se verifica que:*

$$x^{n+m} = x^n \cdot x^m \qquad \forall x \in G, \quad n, m \in \mathbb{Z}$$

Demostración. Aunque la demostración es sencilla, hemos de distinguir bastantes casos, pues hemos de asegurarnos de que el límite superior de cada producto sea siempre un número positivo. Fijado $x \in G$, distinguimos en función de los valores de $n, m \in \mathbb{Z}$:

1. $n > 0$:

   a) $m > 0$:

   $$x^{n+m} = \prod_{i=1}^{n+m} x = \left(\prod_{i=1}^{n} x\right)\cdot\left(\prod_{i=n+1}^{n+m} x\right) = \left(\prod_{i=1}^{n} x\right)\cdot\left(\prod_{i=1}^{m} x\right) = x^n \cdot x^m$$

   b) $m = 0$:

   $$x^{n+0} = x^n = x^n \cdot e = x^n \cdot x^0$$

   c) $m < 0$:

   En este caso, no sabemos el signo de $n+m$. Por tanto, hemos de distinguir casos:

1) $\underline{n+m>0}$: Entonces, $n > -m$. Tenemos:

$$x^n \cdot x^m = \left(\prod_{i=1}^{n} x\right) \cdot \left(x^{-1}\right)^{-m} = \left(\prod_{i=1}^{n} x\right) \cdot \left(\prod_{i=1}^{-m} x^{-1}\right) = \prod_{i=1}^{n-(-m)} x = \prod_{i=1}^{n+m} x = x^{n+m}$$

2) $\underline{n+m=0}$: Entonces, $n = -m$. Tenemos:

$$x^{n+m} = x^0 = e = \left(\prod_{i=1}^{n} x\right) \cdot \left(\prod_{i=1}^{n} x^{-1}\right) = x^n \cdot \left(\prod_{i=1}^{-m} x^{-1}\right) = x^n \cdot \left(x^{-1}\right)^{-m} = x^n \cdot x^m$$

3) $\underline{n+m<0}$: Entonces, $n < -m$. Tenemos:

$$x^n \cdot x^m = \left(\prod_{i=1}^{n} x\right) \cdot \left(x^{-1}\right)^{-m} = \left(\prod_{i=1}^{n} x\right) \cdot \left(\prod_{i=1}^{-m} x^{-1}\right) = \prod_{i=1}^{-m-n} x^{-1} =$$
$$= \prod_{i=1}^{-(n+m)} x^{-1} = (x^{-1})^{-(n+m)} = x^{n+m}$$

2. $\underline{n=0}$:

$$x^{0+m} = x^m = e \cdot x^m = x^0 \cdot x^m$$

3. $\underline{n<0}$:

a) $\underline{m>0}$:

$$x^{n+m} = x^{m+n} = x^m \cdot x^n = \prod_{i=1}^{m} x \cdot \prod_{i=1}^{-n} x^{-1} = x^n \cdot x^m$$

donde en la primera igualdad hemos usado la propiedad conmutativa de la suma en $\mathbb{Z}$, en la segunda hemos empleado el caso anteriormente demostrado, y en la última igualdad hemos empleado que $xx^{-1} = e = x^{-1}x$.

b) $\underline{m=0}$:

$$x^{n+0} = x^n = x^n \cdot e = x^n \cdot x^0$$

c) $\underline{m<0}$:

$$x^n \cdot x^m = \left(x^{-1}\right)^{-n} \cdot \left(x^{-1}\right)^{-m} = \left(\prod_{i=1}^{-n} x^{-1}\right) \cdot \left(\prod_{i=-1}^{-m} x^{-1}\right) =$$
$$= \prod_{i=1}^{-n-m} x^{-1} = \left(x^{-1}\right)^{-(n+m)} = x^{n+m}$$

□

Definición 1.5 (Grupos finitos e infinitos)**.** Sea G un grupo, si G como conjunto tiene[4] $n \in \mathbb{N} \setminus \{0\}$ elementos, diremos que es un grupo finito. En dicho caso, diremos que n es el "orden del grupo", notado por: $|G| = n$.
Si G no fuera finito, decimos que es un grupo infinito.

[4]Excluimos $n = 0$ ya que en la definición de grupo exigimos que $G \neq \emptyset$.

Definición 1.6 (Tabla de Cayley)**.** En un grupo finito $G = \{x_1, x_2, \dots, x_n\}$, se llama tabla de Cayley (o de multiplicar[5]) a la matriz $n \times n$ de forma que su entrada (i, j) es $x_i x_j$.

Ejemplo. A continuación, mostramos ejemplos de posibles tablas de Cayley para ciertas operaciones sobre determinados grupos. Como podemos ver, la finalidad de la tabla es mostrar en cada caso cómo se comporta la operación binaria cuando se aplica a distintos elementos del grupo.

1. Si $G = \{0, 1\}$, podemos considerar sobre G las operaciones $*_1$ y $*_2$, cuya definición puede obtenerse a partir de sus tablas de Cayley:

$*_1$	0	1
0	0	1
1	1	0

$*_2$	0	1
0	1	0
1	0	1

2. Si $G = \{0, 1, 2\}$, podemos considerar sobre G la siguiente operación binaria:

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

3. Si $G = \{0, 1, 2, 3\}$, podemos considerar sobre G las siguientes operaciones binarias:

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

A partir de la definición de la tabla de Cayley para la operación binaria de un grupo pueden deducirse ciertas propiedades que estas tienen, las cuales no demostraremos, entendiendo que pueden deducirse de forma fácil a partir de la definición de grupo:

- Si consideramos un grupo abeliano, su tabla de Cayley será una matriz simétrica.
- Todos los elementos del grupo aparecen en todas las filas o columnas de la tabla de Cayley, ya que en la Proposición 1.5 vimos que las ecuaciones $aX = b$ y $Xa = b$ tenían que tener solución $\forall a, b \in G$, para que G fuese un grupo.
- Como para que G sea un grupo tiene que haber un elemento que actúe de neutro, esto se refleja en la tabla con un elemento que mantiene igual los encabezados en una fila y en una columna.

Definición 1.7 (Orden de un elemento)**.** Sea $(G, \cdot, 1)$ un grupo, el orden de un elemento $x \in G$ es el menor $n \in \mathbb{N} \setminus \{0\}$ (en caso de existir) que verifica: $x^n = 1$. En cuyo caso, notaremos[6]: $O(x) = \text{ord}(x) = n$.
Si para un elemento $x \in G$ dicho n no existe, se dice que su orden es infinito: $O(x) = +\infty$.

[5]Entendiendo que en este caso hacemos uso de la notación multiplicativa.
[6]Podremos encontrarnos cualquiera de las dos notaciones.

Notación. Si consideramos un grupo con notación aditiva, $(G, +, 0)$, interpretando la anterior definición con esta notación diremos que $x \in G$ tendrá orden $n \in \mathbb{N} \setminus \{0\}$ si n es el menor natural no nulo de forma que verifica $n \cdot x = \sum_{i=1}^{n} x = 0$.

Proposición 1.8. *Sea G un grupo, $x \in G$ con $O(x) = n$ y sea $m \in \mathbb{N} \setminus \{0\}$:*

$$x^m = 1 \Longleftrightarrow n \mid m$$

Demostración. Demostramos las dos implicaciones:

$\Longrightarrow$) Si $O(x) = n$, entonces no puede ser $m < n$, ya que si no el orden de x no sería n sino m, por lo que $m \geqslant n$. En cuyo caso, $\exists q, r \in \mathbb{N}$ de forma que:

$$m = nq + r \qquad \text{con } 0 \leqslant r < n$$

Pero entonces:

$$1 = x^m = x^{nq+r} = x^{nq}x^r = x^r \overset{(*)}{\Longrightarrow} r = 0$$

Donde en $(*)$ hemos usado que $r < n$, ya que si r no fuese 0, tendríamos que $O(x) = r$.

$\Longleftarrow$) Si $n \mid m$, entonces $\exists q \in \mathbb{N}$ de forma que $m = qn$, luego:

$$x^m = x^{qn} = (x^n)^q = 1^q = 1$$

□

Proposición 1.9. *Sea G un grupo, se verifica que:*

1. $O(x) = 1 \Longleftrightarrow x = 1$.
2. $O(x) = O(x^{-1})\ \forall x \in G$.
3. *Si $O(x) = +\infty$ para cierto $x \in G$, entonces todas las potencias de x son elementos distintos de G.*
4. *Si G es finito, entonces $O(x) \neq +\infty$ para todo $x \in G$.*
5. *Si $O(x) = n \in \mathbb{N} \setminus \{0\}$ para cierto $x \in G$, entonces x tiene n potencias distintas. Más aún, sean $p, q \in \mathbb{N}$ de forma que $x^p = x^q$ con $q > p$, entonces:*

$$x^{q-p} = 1 \Longleftrightarrow n \mid (q - p)$$

Demostración. Demostramos todas las propiedades:

1. Por doble implicación:

   $\Longleftarrow$) Trivial.

   $\Longrightarrow$) Si aplicamos la definición de $O(x)$ y de x^1:

$$1 = x^1 = \prod_{i=1}^{1} x = x$$

2. Distinguimos dos casos:

   - Fijado $x \in G$ con $O(x) = n$, entonces $x^n = 1$, por lo que:

     $$x^{-1} = x^{n-1}$$

     Veamos en primer lugar que $O(x^{-1}) \leqslant n$. Para ello, vemos que $\left(x^{-1}\right)^n = 1$:

     $$\left(x^{-1}\right)^n = \left(x^{n-1}\right)^n = x^{n(n-1)} = (x^n)^{n-1} = 1$$

     Veamos ahora que $O(x^{-1}) \geqslant n$. Supongamos ahora que $O(x^{-1}) = k$, entonces:

     $$(x^{-1})^k = 1 \Longrightarrow x^{(n-1)k} = 1 \Longrightarrow n \mid (n-1)k$$

     Por tanto, como $n \nmid (n-1)$ y $\operatorname{mcd}(n, n-1) = 1$, entonces $n \mid k$, por lo que $n \leqslant k = O(x^{-1})$. Por tanto, tenemos que:

     $$n \leqslant O(x^{-1}) \leqslant n \Longrightarrow O(x^{-1}) = n$$

   - Si tenemos que $O(x) = +\infty$, por reducción al absurdo, supongamos que $\exists n \in \mathbb{N} \setminus \{0\}$ de forma que $O(x^{-1}) = n$.
     Que $O(x) = +\infty$ significa que $\nexists m \in \mathbb{N} \setminus \{0\}$ de forma que $x^m = 1$.
     Como $O(x^{-1}) = n$, tenemos que:

     $$\left(x^{-1}\right)^n = 1 \Longrightarrow x = \left(x^{-1}\right)^{-1} = \left(x^{-1}\right)^{n-1}$$

     De donde llegamos a que:

     $$x^n = \left(\left(x^{-1}\right)^{n-1}\right)^n = \left(\left(x^{-1}\right)^n\right)^{n-1} = 1^{n-1} = 1$$

     Contradicción, puesto que $O(x) = +\infty$. Deducimos que si $O(x) = +\infty$, entonces ha de ser $O(x^{-1}) = +\infty$.

3. Por reducción al absurdo, supongamos que existen $p, q \in \mathbb{N}$ con $p < q$ de forma que $x^p = x^q$, luego:

   $$x^{q-p} = 1$$

   De donde deducimos que $O(x) < +\infty$, contradicción, luego $x^p \neq x^q$ para todo $p, q \in \mathbb{N}$ con $p \neq q$.

4. Por reducción al absurdo, supongamos que $\exists x \in G$ con $O(x) = +\infty$. En este caso, podemos construir una aplicación $\phi : \mathbb{N} \to G$ dada por $\phi(n) = x^n$ $\forall n \in \mathbb{N}$. Esta aplicación es inyectiva gracias al punto 3, lo que contradice que G sea un grupo finito. Concluimos que $O(x) \in \mathbb{N} \setminus \{0\}$ para todo $x \in G$.

5. Si $O(x) = n$, consideramos la sucesión:

   $$x, x^2, x^3, \ldots, x^{n-1}, x^n = 1$$

   Si seguimos calculando potencias, está claro que se repetirá este patrón, por lo que tratamos de ver que todos los elementos de la sucesión son distintos entre sí. Por reducción al absurdo, supuesto que existen $p, q \in \mathbb{N}$ de forma que $p < q \leqslant n$ con $x^p = x^q$, entonces $x^{q-p} = 1$ con $q - p \leqslant n$, lo que contradice que $O(x) = n$.

Para ver que si $p, q \in \mathbb{N}$ con $x^p = x^q$, entonces:

$$x^{q-p} = 1 \Longleftrightarrow n \mid (q - p)$$

Basta aplicar la Proposición 1.8 con $m = q - p$.

$\square$

Ejemplo. Mostramos ahora ejemplos de órdenes de ciertos elementos en distintos grupos, entendiendo que cuando consideramos conjuntos susceptibles de ser anillos (conjuntos con suma y multiplicación), si dejamos el 0 en el conjunto consideramos el grupo con su suma ($e = 0$) y que cuando quitamos el 0 del conjunto consideramos el grupo con su multiplicación ($e = 1$).

1. Si cogemos $x \neq 1$ en $\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*$ con la multiplicación: $O(x) = +\infty$.
2. Si consideramos $\mathbb{C}^*$ con su multiplicación: $O(i) = 4$, ya que $i^4 = 1$.
3. En $\mathbb{Z}_9$, $O\left(\overline{6}\right) = 3$:
$$\begin{gathered} \overline{6} \neq \overline{0} \\ \overline{6+6} = \overline{12} = \overline{3} \neq \overline{0} \\ \overline{6+6+6} = \overline{18} = \overline{0} \end{gathered}$$
4. En $\mathbb{Z}_7^* = \mathcal{U}(\mathbb{Z}_7)$:
   - $O\left(\overline{2}\right) = 3$:
   $$\begin{gathered} \overline{2} \neq \overline{1} \\ \overline{2 \cdot 2} = \overline{4} \neq \overline{1} \\ \overline{2 \cdot 2 \cdot 2} = \overline{8} = \overline{1} \end{gathered}$$
   - $O\left(\overline{3}\right) = 6$.
   $$\begin{gathered} \overline{3} \neq \overline{1} \\ \overline{3 \cdot 3} = \overline{9} = \overline{2} \neq \overline{1} \\ \overline{3 \cdot 3 \cdot 3} = \overline{27} = \overline{6} \neq \overline{1} \\ \overline{3 \cdot 3 \cdot 3 \cdot 3} = \overline{81} = \overline{3} \neq \overline{1} \\ \overline{3 \cdot 3 \cdot 3 \cdot 3 \cdot 3} = \overline{243} = \overline{5} \neq \overline{1} \\ \overline{3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3} = \overline{729} = \overline{1} \end{gathered}$$

1.1. Grupos diédricos D_n

A continuación, estaremos interesados en el estudio de una familia[7] de grupos conocida como los "grupos diédricos", cuyo estudio se desarrollará a lo largo de la asignatura.

[7] Donde con "familia" hacemos referencia a un conjunto de grupos que guardan cierta similitud entre ellos.

1.1.1. Motivación

Para entender estos grupos, conviene destacar la forma en la que surgieron ciertos objetos geométricos que luego fueron interesantes desde el punto de vista algebraico, por formar un grupo.

Ejemplo. Si pensamos en un triángulo equilátero (el menor polígono regular) sobre el plano centrado en el origen como el de la Figura 1.1, donde hemos numerado los vértices del mismo, es interesante preguntarnos sobre las isometrías del plano en el plano que dejan invariante al mismo.

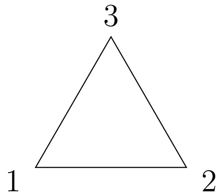


Figura 1.1: Triángulo equilátero con centro en el origen de coordenadas.

En Geometría II se vio que las únicas isometrías que podemos considerar en el plano son los giros y las simetrías axiales o centrales, por lo que procedemos a distinguir casos:

Giros. Como vemos en la Figura 1.2, de forma intuitiva vemos que giros (pensando que todos son en sentido antihorario) que dejan el triángulo invariante solo hay 3:

- El giro de ángulo $\frac{2\pi}{3}$.
- El giro de ángulo $\frac{4\pi}{3}$.
- El giro de ángulo 2π.

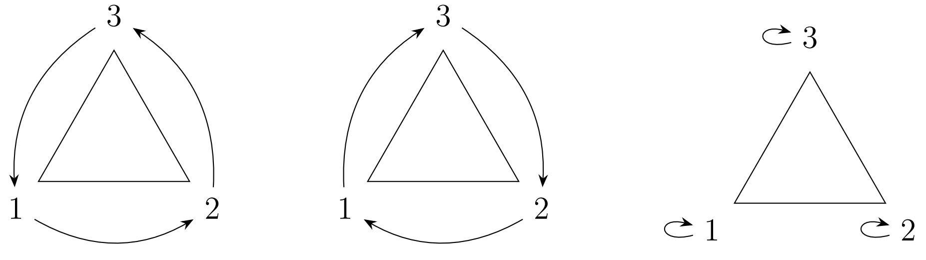


Figura 1.2: Todos los giros que dejan invariánte al triángulo.

Simetrías. Como vemos en la Figura 1.3, de forma intuitiva vemos que hay 3 simetrías axiales que dejan invariante al triángulo y que no hay ninguna simetría central que lo deje invariante:

- La simetría respecto a la mediatriz del segmento 2, 3.
- La simetría respecto a la mediatriz del segmento 3, 1.

- La simetría respecto a la mediatriz del segmento 1, 2.

Notemos la forma en la que hemos nombrado las rectas respecto a las cuales se hace la simetría: la recta l_i contiene al vértice i-ésimo.

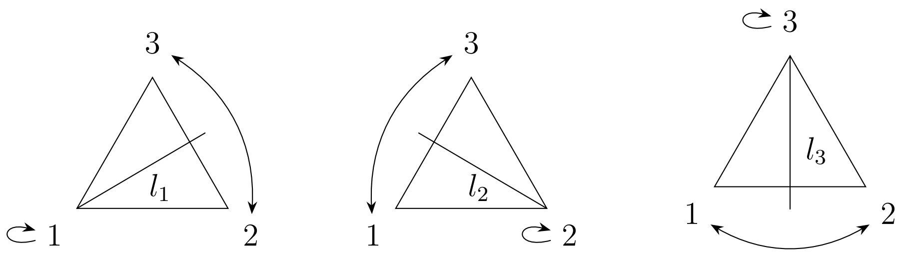


Figura 1.3: Todas las reflexiones que dejan invariante al triángulo.

Con el fin de estudiar las isometrías que mantienen polígonos regulares en el plano, conviene introducir las siguientes definiciones y notaciones:

Definición 1.8 (Permutación)**.** Sea X un conjunto, una permutación del mismo es cualquier aplicación biyectiva $f : X \to X$.

Si X es el conjunto $\{1, 2, \ldots, n\}$, es usual notar:

$$S_n = \text{Perm}(X) = \{f : X \to X \mid f \text{ es una permutación}\}$$

Definición 1.9 (Ciclo)**.** Sea $\{a_1, a_2, \ldots, a_m\} \subseteq \{1, 2, \ldots, n\}$, un ciclo de longitud $m \leqslant n$ es una permutación $\sigma \in S_n$ de forma que:

1. $\sigma(a_i) = a_{i+1}$ para todo $i \in \{1, \ldots, m-1\}$.
2. $\sigma(a_m) = a_1$.
3. $\sigma(a_j) = a_j$ para todo $a_j \notin \{a_1, a_2, \ldots, a_m\}$.

En dicho caso, representaremos a σ por:

$$\sigma = (a_1 \ a_2 \ \ldots \ a_m)$$

Observación. Notemos que podemos notar a un ciclo de longitud m, σ, de m formas distintas:

$$\sigma = (a_1 \ a_2 \ \ldots \ a_m) = (a_2 \ \ldots \ a_m \ a_1) = \ldots = (a_m \ a_1 \ a_2 \ \ldots \ a_{m-1})$$

De esta forma, el número de ciclos de longitud m son todas las posibles combinaciones de los m elementos entre n, pero como cada vez aparecen m:

$$\frac{V_m^n}{m}$$

A los $2-$ciclos los llamaremos transposiciones.

Ejemplo. Para familiarizarnos con los ciclos, observamos que:

- En S_3, los ciclos de longitud 2 que podemos considerar son: (1 2), (1 3) y (2 3). Estos se interpretan respectivamente como:
  - Mantener el 3 fijo e intercambiar el 1 con el 2.
  - Mantener el 2 fijo e intercambiar el 1 con el 3.
  - Mantener el 1 fijo e intercambiar el 2 con el 3.
- En S_3, los únicos ciclos de longitud 3 que podemos considerar son: (1 2 3) y (3 2 1), cuya definición debe estar clara.

Notación. Es claro que no toda permutación es un ciclo. Sin embargo, hay ciertas permutaciones como por ejemplo la aplicación $\sigma : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ dada por:

$$\begin{aligned} \sigma(1) &= 2 \\ \sigma(2) &= 1 \\ \sigma(3) &= 4 \\ \sigma(4) &= 3 \end{aligned}$$

Que restringida a $\{1, 2\}$ da el ciclo (1 2) y que restringida al $\{3, 4\}$ da el ciclo (3 4). Será usual denotar permutaciones como esta por[8]:

$$\sigma = (1\ 2)(3\ 4)$$

Aprovechando la notación para los ciclos previamente definida, si por ejemplo extendemos σ a $\{1, 2, 3, 4, 5\}$ definiendo:

$$\sigma(5) = 5$$

Entonces, la notación para σ será la misma: (1 2)(3 4), ya que el 5 "no se mueve".

Ejemplo. Volviendo al ejemplo anterior del triángulo y de las isometrías que lo dejan invariante, si notamos por:

- r al giro de ángulo $\frac{2\pi}{3}$.
- s a la simetría axial cuya recta pasa por el vértice 1.

Puede comprobarse de forma geométrica que a partir de composiciones de r y de s obtenemos los otros 4 movimientos restantes (notaremos la composición de aplicaciones por yuxtaposición, ya que estamos buscando un grupo con estas aplicaciones):

- El giro de ángulo $\frac{4\pi}{3}$ es $r^2 = rr$.
- El giro de ángulo 2π es r^3.
- La simetría respecto a la recta l_2 es sr^2.
- La simetría respecto a la recta l_3 es sr.

[8]Más adelante formalizaremos bien esta notación, aunque por ahora empecemos a usarla desde un punto de vista más intuitivo.

Notemos que el giro de ángulo 2π es la identidad, que es el elemento neutro para la composición, por lo que el elemento neutro del futuro grupo que definamos será r^3, que podemos denotar por 1. Además, la composición de aplicaciones es una operación asociativa y se deja como ejercicio demostrar que cada elemento del conjunto:

$$D_3 = \{1, r, r^2, s, sr, sr^2\}$$

Tiene un elemento simétrico respecto de la composición. Podemos ver que $(D_3, \circ, 1)$ es un grupo.

Ejemplo. Continuando con la motivación para los grupos diédricos, nos preguntamos ahora qué pasa si en vez de considerar las isometrías que mantienen invariante a un triángulo equilátero, consideramos las isometrías del plano que mantienen invariantes los vértices de un cuadrado sobre el plano; un cuadrado como el de la Figura 1.4.

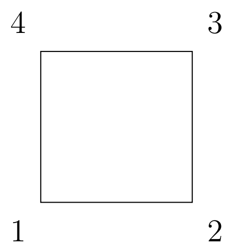


Figura 1.4: Cuadrado con centro en el origen de coordenadas.

Es fácil ver que las únicas isometrías que dejan invariante al cuadrado son (Véase la Figura 1.5):

- Los giros de ángulos $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ y 2π.
- Las simetrías axiales respecto a las rectas:
  - La recta que une los vértices 1 y 3.
  - La recta que une los vértices 2 y 4.
  - La recta que es mediatriz del segmento 1, 2.
  - La recta que es mediatriz del segmento 2, 3.

Todos estos movimientos pueden verse como aplicaciones lineales $f : \mathbb{R}^2 \to \mathbb{R}^2$ tal y como se hace en geometría o aprovecharnos de que todas ellas mantienen el cuadrado invariante, por lo que podemos pensar en ellas como si fueran permutaciones del conjunto $\{1, 2, 3, 4\}$. Aprovechando esta dualidad, vemos que:

- El giro de ángulo $\frac{\pi}{2}$ es $(1\ 2\ 3\ 4)$.
- El giro de ángulo π es $(1\ 3)(2\ 4)$.
- El giro de ángulo $\frac{3\pi}{2}$ es $(1\ 4\ 3\ 2)$.
- El giro de ángulo 2π es la identidad, (1).

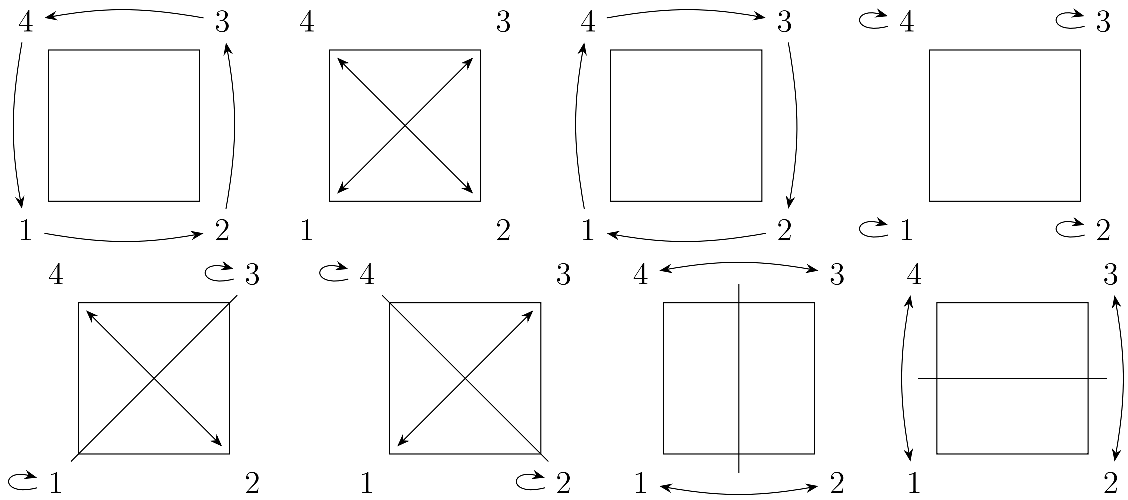


Figura 1.5: Giros y simetrías que dejan invariante al cuadrado

- La simetría respecto a la recta que une 1 y 3 es (2 4).
- La simetría respecto a la recta que une 2 y 4 es (1 3).
- La simetría respecto a la mediatriz de 1 y 2 es (1 2)(3 4).
- La simetría respecto a la mediatriz de 2 y 3 es (1 4)(2 3).

Dejamos como ejercicio hacer esta correspondencia (notar las isometrías como su correspondiente permutación) con los movimientos que teníamos en el triángulo. Si ahora hacemos como hicimos anteriormente con el triángulo y notamos por:

- r al giro de ángulo $\frac{\pi}{2}$.
- s a la reflexión respecto a la recta que pasa por el vértice 1.

Podemos obtener los otros 6 movimientos (o permutaciones desde el punto de vista algebráico) con la composición de r y s:

- r^2 es (1 3)(2 4).
- r^3 es (1 4 3 2).
- r^4 es 1 (la aplicación identidad).
- sr es (1 4)(2 3).
- sr^2 es (1 3).
- sr^3 es (1 2)(3 4).

De esta forma, si consideramos el conjunto:

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

Tenemos que $(D_4, \circ, 1)$ es un grupo. Más aún, podemos completar su tabla de Cayley para observar cómo se comporta $\circ$ dentro de D_4:

$\circ$	1	r	r^2	r^3	s	sr	sr^2	sr^3
1	1	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	1	sr^3	s	sr	sr^2
r^2	r^2	r^3	1	r	sr^2	sr^3	s	sr
r^3	r^3	1	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	1	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	1	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	1	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	1

1.1.2. Definición y primeras propiedades

Una vez comprendida la motivación de los grupos diédricos, estamos preparados para dar su definición. No demostraremos que, dado $n \in \mathbb{N}$, el conjunto de isometrías que dejan invariante al polígono regular de n lados forma un grupo si consideramos sobre dicho conjunto la composición de aplicaciones, ya que no es interesante para esta asignatura.

Sin embargo, aceptaremos la definición como válida (animamos al lector a investigar más sobre los grupos diédricos y su definición) y procedemos a destacar las propiedades algebraicas de estos grupos, que es lo que nos interesa.

Definición 1.10 (Grupos diédricos D_n)**.** Sea D_n el conjunto de isometrías que dejan invariante al polígono regular de n lados. Sabemos que D_n tiene $2n$ elementos:

- n rotaciones de ángulo $\frac{2k\pi}{n}$, con $k \in \{1, \ldots, n\}$.
- n simetrías axiales:
  - Si n es par, tenemos:
    - $n/2$ simetrías respecto a las mediatrices.
    - $n/2$ simetrías respecto a unir vértices opuestos.
  - Si n es impar, tenemos n simetrías respecto a las mediatrices.

Se verifica que $(D_n, \circ, 1)$ es un grupo. Además, destacamos dos elementos suyos:

- r, la rotación de ángulo $\frac{2\pi}{n}$.
- s, la simetría axial respecto a la recta que pasa por el origen de coordenadas y el vértice nombrado 1.

De esta forma, todos los elementos de D_n son:

$$D_n = \left\{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\right\}$$

Proposición 1.10. *Dado $n \in \mathbb{N}$, en D_n se cumple que:*

1. *$1, r, r^2, \ldots, r^{n-1}$ son todos distintos y $r^n = 1$, es decir, $O(r) = n$.*

2. *$s^2 = 1$. En particular, $O(s) = 2$.*

3. *$s \neq r^i$, $\forall\ 0 \leqslant i \leqslant n-1$.*

4. *sr^i con $0 \leqslant i \leqslant n-1$ son simetrías.*

5. *$sr^i \neq sr^j$ para todo $i \neq j$, con $i, j \in \{1, \ldots, n-1\}$.*

6. *$sr = r^{-1}s$.*

7. *$sr^i = r^{-i}s$.*

Demostración. Demostramos cada una de las propiedades:

1. La primera parte es compentencia de Geometría. Para la segunda, basta ver que r^n es componer n veces el giro de ángulo $\frac{2\pi}{n}$, que es lo mismo que considerar el giro de ángulo $n \cdot \frac{2\pi}{n} = 2\pi$, que es la identidad.

2. Es competencia de Geometría.

3. Es competencia de Geometría, que puede probarse de distintas formas:

   - Viendo que s tiene puntos fijos y r^i no.
   - Viendo que s es un movimiento inverso y que r^i es directo.

4. Es competencia de Geometría.

5. Basta aplicar 1.

6, 7. Son competencia de Geometría.

□

Usaremos los resultados de la Proposición 1.10 con frecuencia, como las propiedades básicas de los grupos diédricos. Notemos que a partir de estas puede construirse la tabla de Cayley para cualquier grupo diédrico D_n.

Ejercicio. Construya la tabla de Cayley para D_4 y D_5 usando los resultados de la Proposición 1.10.

1.2. Generadores de un grupo

Definición 1.11 (Conjunto de generadores de un grupo)**.** Sea G un grupo, diremos que $S \subseteq G$ es un conjunto de generadores de G si todo elemento $x \in G$ puede escribirse como producto finito de elementos de S y de sus inversos. En dicho caso, notaremos: $G = \langle S \rangle$.
Si S es un conjunto finito, $S = \{x_1, x_2, \ldots, x_n\} \subseteq G$, podemos escribir:

$$G = \langle x_1, x_2, \ldots, x_n \rangle$$

Y diremos que G es finitamente generado.
Si S está formado solo por un elemento, diremos que G es un grupo cíclico.

Observación. Sea G un grupo y $S \subseteq G$, equivalen:

i) S es un conjunto de generadores de G.

ii) Dado $x \in G$, $\exists x_1, x_2, \dots, x_p \in S$ de forma que:

$$x = x_1^{\gamma_1} x_2^{\gamma_2} \dots x_p^{\gamma_p} \qquad \gamma_i \in \mathbb{Z}, \quad i \in \{1, \dots, p\}$$

Ejemplo. Como ejemplos a destacar, vemos que:

1. $\mathbb{Z} = \langle 1 \rangle$ si pensamos en $(\mathbb{Z}, +, 0)$, ya que dado $x \in \mathbb{Z}$:

   - Si $x > 0$, entonces:
     $$x = \underbrace{1 + 1 + \ldots + 1}_{x \text{ veces}}$$
   - Si $x < 0$, entonces (-1 es el simétrico de 1):
     $$x = \underbrace{-1 - 1 - \ldots - 1}_{x \text{ veces}}$$
   - Si $x = 0$, entonces: $x = 1 - 1$.

2. $D_n = \langle r, s \rangle$, ya que $D_n = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$.

Definición 1.12 (Presentación de un grupo)**.** Sea G un grupo y $S \subseteq G$, si $G = \langle S \rangle$ y existe un conjunto de relaciones $R_1, R_2, \dots, R_m$ (igualdades entre elementos de S, $\{1\}$ y los elementos simétricos de S) tal que cualquier relación entre los elementos de S puede deducirse de estas, entonces, decimos que estos generadores y relaciones constituyen una presentación de G, notado:

$$G = \langle S \mid R_1, R_2, \dots, R_n \rangle$$

Ejemplo. Veamos algunos ejemplos de presentaciones, observando que dar una presentación es equivalente a dar la definición del propio grupo, ya que a partir de la presentación pueden deducirse todos los elementos del grupo y las relaciones que estos guardan entre sí.

1. En el diédrico D_n, tenemos que:
   $$D_n = \langle r, s \mid rs = sr^{-1}, r^n = 1, s^2 = 1 \rangle$$

2. $D_1 := \langle s \mid s^2 = 1 \rangle$.

   En este caso, vemos que $D_1 = \{1, s\}$.

3. $D_2 := \langle r, s \mid r^2 = s^2 = 1, sr = rs \rangle$.

   Ahora, tenemos: $D_2 = \{1, r, s, rs\}$.

4. $C_n = \langle x \mid x^n = 1 \rangle$ es un grupo cíclico de orden n.

   Vemos que: $C_n = \{1, x, x^2, x^3, \dots, x^{n-1}\}$

5. $V^{\text{abs}} = \langle x, y \mid x^2 = 1, y^2 = 1, (xy)^2 = 1\rangle$ es el grupo de Klein abstracto.

   En primer lugar, sabemos que $\{1, x, y\} \subseteq V^{\text{abs}}$. Como x e y son de orden 2, sabemos que $x^{-1} = x$ y que $y^{-1} = y$. Además, vemos que $xy \in V^{\text{abs}}$ y que:

   $$(xy)^2 = 1 \Longleftrightarrow xyxy = 1 \Longleftrightarrow xy = yx$$

   Por lo que xy también está en V^{abs}, con $(xy)^{-1} = yx$. Vemos que no hay más elementos que puedan estar en V^{abs}, con lo que:

   $$V^{\text{abs}} = \{1, x, y, xy\}$$

   Observamos que el grupo nos recuerda a D_2.

6. $Q_2^{\text{abs}} = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1}\rangle$.

   Inicialmente, $\{1, x, y\} \subseteq Q_2^{\text{abs}}$. De la primera relación vemos que también tenemos $\{x^2, x^3\} \subseteq Q_2^{\text{abs}}$. Reescribimos la última relación, para buscar más elementos de forma cómoda:

   $$yxy^{-1} = x^{-1} \Longleftrightarrow yx = x^{-1}y$$

   Como yx no guarda ninguna relación con x e y, sabemos que también está en el grupo, junto con yx^2 y yx^3. De esta forma:

   $$Q_2^{\text{abs}} = \{1, x, x^2, x^3, y, yx, yx^2, yx^3\}$$

Ejemplo. Las similitudes que hemos encontrado entre distintos grupos como entre V^{abs} y D_2 las formalizaremos con ayuda de un concepto algebraico que luego definiremos, pero merece la pena destacar ahora una similaritud entre Q_2^{abs}, el grupo de los cuaternios $Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$ y unos elementos del grupo $\mathrm{SL}_2(\mathbb{C})$. Para familiarizarnos con los cuaternios, estos cumplen que:

$$\begin{gathered} i^2 = j^2 = k^2 = -1 \\ ij = k \quad jk = i \quad ki = j \\ ji = -k \quad kj = -i \quad ik = -j \end{gathered}$$

Productos que pueden recordarse observando la Figura 1.6

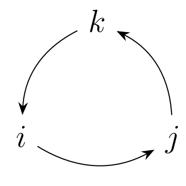


Figura 1.6: Dirección en la que se multiplican los cuaternios de forma positiva.

Se deja como ejercicio ver en qué forma podemos entender que los grupos Q_2, Q_2^{abs} y el subconjunto de matrices de $\mathrm{SL}_2(\mathbb{C})$ con la operación heredada del mismo:

$$C = \left\{ \begin{array}{c} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \end{array} \right\} \subseteq \mathrm{SL}_2(\mathbb{C})$$

Si pensamos en relacionar los elementos de la Tabla 1.1.

Q_2^{abs}	C	Q_2
1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1
x	$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$	i
y	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	j
x^2	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	-1
x^3	$\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$	$-i$
xy	$\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$	k
x^2y	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$-j$
x^3y	$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$	$-k$

Tabla 1.1: Elementos que se relacionan.

1.3. Grupos Simétricos S_n

Recordamos que dado un conjunto X, podemos considerar el conjunto de todas sus permutaciones:

$$S(X) = \{f : X \to X \mid f \text{ biyectiva}\}$$

Definición 1.13 (Grupos Simétricos S_n)**.** Dado $n \in \mathbb{N}$, consideramos $X = \{1, 2, \ldots, n\}$ y definimos $S_n = S(X)$, el conjunto de todas las permutaciones de X. Se verifica que S_n junto con la operación de composición de aplicaciones es un grupo:

- La composición de aplicaciones es asociativa.
- La aplicación $id : X \to X$ es el elemento neutro.
- Como las permutaciones son biyecciones, cada una tiene su elemento simétrico.

Llamaremos a $(S_n, \circ, id)$ el $n-$ésimo grupo simétrico, que recordamos tiene orden:

$$|S_n| = n!$$

Notación. Estaremos interesados en ver cómo se comportan de forma algebraica las permutaciones de conjuntos de n elementos, por lo que tendremos que conocer en cada caso cuáles son las aplicaciones con las que estamos trabajando.

Para abreviar, en muchos casos usaremos la notación matricial de las permutaciones. Sea $\sigma \in S_n$, sabemos que dar σ es equivalente a dar $\sigma(a)$ para cualquier $a \in X$. De esta forma, podemos dar una matriz $2 \times n$ de la forma:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Observemos que, conocida la matriz anterior, conocemos σ.

Ejemplo. En este ejemplo, vemos los grupos simétricos más pequeños:

1. Si consideramos S_0, son todas las permutaciones del $\emptyset$ en el $\emptyset$, que solo hay una: $\sigma : \emptyset \to \emptyset$.

2. Si consideramos S_1, solo hay una permutación: $id : \{1\} \to \{1\}$.

3. En S_2, tenemos $S_2 = \{\sigma_1, \sigma_2\}$, con:

$$\sigma_1 = id = \left(\begin{array}{cc} 1 & 2 \\ 1 & 2 \end{array}\right), \quad \sigma_2 = \left(\begin{array}{cc} 1 & 2 \\ 2 & 1 \end{array}\right)$$

   Hasta ahora, todos estos grupos son abelianos.

4. En S_3, tenemos:

$$S_3 = \left\{ \left(\begin{array}{ccc} 1 & 2 & 3 \\ 1 & 2 & 3 \end{array}\right), \left(\begin{array}{ccc} 1 & 2 & 3 \\ 1 & 3 & 2 \end{array}\right), \left(\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 1 & 3 \end{array}\right), \left(\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array}\right), \left(\begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \end{array}\right), \left(\begin{array}{ccc} 1 & 2 & 3 \\ 3 & 2 & 1 \end{array}\right) \right\}$$

   Que ya es un ejemplo de grupo simétrico no abeliano, ya que si tomamos:

$$\sigma = \left(\begin{array}{ccc} 1 & 2 & 3 \\ 1 & 3 & 2 \end{array}\right), \quad \tau = \left(\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 1 & 3 \end{array}\right)$$

   Vemos que $\sigma\tau \neq \tau\sigma$:

$$\sigma\tau = \left(\begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \end{array}\right) \neq \left(\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array}\right) = \tau\sigma$$

   De esta forma, acabamos de probar que S_n con $n \geqslant 3$ no es abeliano, ya que si estamos en S_n, podemos considerar las extensiones de σ y τ a S_n:

$$\sigma = \left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{array}\right), \quad \tau = \left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{array}\right)$$

   Y tendremos que $\sigma\tau \neq \tau\sigma$.

Ejemplo. Sean $s_1, s_2 \in S_7$ dadas por:

$$s_2 = \left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 2 & 1 & 4 & 3 \end{array}\right), \quad s_1 = \left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 1 & 7 & 6 \end{array}\right)$$

Se pide calcular s_1s_2, s_2s_1 y s_2^2.

$$s_1s_2 = \left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 7 & 2 & 3 & 5 & 4 \end{array}\right)$$
$$s_2s_1 = \left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 2 & 1 & 5 & 3 & 4 \end{array}\right)$$
$$s_2^2 = \left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 7 & 5 & 2 & 6 \end{array}\right)$$

Proposición 1.11. *Se verifica que:*

1. *Dado $\sigma \in S_n$, existe $m \in \mathbb{N}$ de forma que $\sigma^{m+1}(x) = x$, $\forall x \in X = \{1, \ldots, n\}$.*
2. *Todo ciclo es una permutación.*
3. *El orden de un ciclo de longitud m es m.*
4. *Si $\sigma = (x_1\ x_2\ \ldots\ x_{m-1}\ x_m)$, entonces: $\sigma^{-1} = (x_m\ x_{m-1}\ \ldots\ x_2\ x_1)$.*

Demostración. Demostramos cada propiedad:

1. Por la Proposición 1.9, como S_n es un grupo finito, sabemos que $\exists n \in \mathbb{N} \setminus \{0\}$ de forma que $O(\sigma) = n$. Tomando $m = n - 1$, tenemos que:
$$\sigma^{m+1}(x) = \sigma^n(x) = x \qquad \forall x \in X$$
2. Se tiene directamente por la definición de ciclo.
3. Sea $\sigma \in S_n$ un ciclo de longitud m:
$$\sigma = (x_1\ x_2\ \ldots\ x_m) \qquad x_1, x_2, \ldots, x_m \in X$$
Queremos ver que $O(\sigma) = m$. Para ello:
   - En primer lugar, veamos que $\sigma^m = 1$:
     - Si $x \in X$ con $x \neq x_i$ para todo $i \in \{1, \ldots, m\}$, entonces $\sigma(x) = x$, luego:
$$\sigma^m(x) = \sigma^{m-1}(\sigma(x)) = \sigma^{m-1}(x) = \sigma^{m-2}(\sigma(x)) = \ldots = x$$
     - Si ahora consideramos x_i con $i \in \{1, \ldots, m\}$, tendremos que:
$$x_i \underbrace{\overset{\sigma}{\longmapsto} x_{i+1} \overset{\sigma}{\longmapsto} \ldots \overset{\sigma}{\longmapsto} x_{m-1} \overset{\sigma}{\longmapsto}}_{\sigma^{m-i}} x_m \underbrace{\overset{\sigma}{\longmapsto} x_1 \overset{\sigma}{\longmapsto} \ldots \overset{\sigma}{\longmapsto} x_{i-1} \overset{\sigma}{\longmapsto}}_{\sigma^{i}} x_i$$
     Luego: $1 = \sigma^{m-i}\sigma^i = \sigma^{m-i+i} = \sigma^m$
   - Supongamos ahora que existe $k < m$ de forma que $\sigma^k = 1$, esto significaría que $\sigma^k(x_1) = x_1$, pero como σ es un ciclo de longitud m, se tiene que $\sigma^k(x_1) = x_k$ y $x_k \neq x_1$, contradicción, con lo que $k \geqslant m$.
4. Recordamos por la defición de ciclo que si $\sigma = (a_1\ a_2\ \ldots\ a_{m-1}\ a_m)$, entonces se ha de cumplir que:
$$\begin{aligned} \sigma(x) &= x \qquad x \neq x_i, \quad i \in \{1, \ldots, m\} \\ \sigma(x_i) &= x_{i+1} \qquad i \in \{1, \ldots, m-1\} \\ \sigma(x_m) &= x_1 \end{aligned}$$
Si vemos σ como aplicación y tratamos de buscarle su aplicación inversa σ^{-1}, esta ha de cumplir que:
$$\begin{aligned} \sigma^{-1}(x) &= x \qquad x \neq x_i, \quad i \in \{1, \ldots, m\} \\ \sigma^{-1}(x_{i+1}) &= x_i \qquad i \in \{1, \ldots, m-1\} \\ \sigma^{-1}(x_1) &= x_m \end{aligned}$$

Sin embargo, vemos que entonces σ^{-1} también es un ciclo:

$$\sigma^{-1} = (x_m\ x_{m-1}\ \ldots\ x_2\ x_1)$$

□

Con el siguiente teorema veremos que los ciclos son una parte interesante de los grupos simétricos, tanto que cualquier permutación pueda expresarse como una composición de ciertos ciclos de longitud mayor o igual que 2. Para ello, será necesario primero realizar una definición:

Definición 1.14 (Ciclos disjuntos)**.** Sean $\sigma_1, \sigma_2 \in S_n$ ciclos, decimos que son disjuntos si no existe $i \in X = \{1, 2, \ldots, n\}$ de forma que:

$$\sigma_1(i) = j, \quad \sigma_2(i) = k \quad \text{con } j, k \in X, i \neq j \neq k \neq i$$

Es decir, si no hay ningún elemento que se mueva en ambos ciclos.

Ejemplo. Ejemplos de ciclos disjuntos son:

$$\sigma_1 = (1\ 3\ 5), \quad \sigma_2 = (2\ 4\ 6), \quad \sigma_3 = (7\ 8)$$

Un ejemplo de dos ciclos que no son disjuntos son:

$$\tau_1 = (1\ 3\ 5\ 8), \quad \tau_2 = (2\ 4\ 5\ 9)$$

Ya que $\tau_1(5) = 8$ y $\tau_2(5) = 9$, con $5 \neq 8 \neq 9 \neq 5$. Es decir, el 5 se mueve en ambos ciclos.

Teorema 1.12. *Toda permutación $\sigma \in S_n$ con $\sigma \neq 1$ se expresa en la forma:*

$$\sigma = \gamma_1\gamma_2\ldots\gamma_k$$

siendo los γ_i con $i \in \{1, \ldots, k\}$ ciclos disjuntos de longitud mayor o igual que 2. Además, dicha descomposición es única, salvo el orden de los factores.

Demostración. Supuesto que estamos trabajando con permutaciones sobre el conjunto $X = \{1, 2, \ldots, n\}$, sea $\sigma \in S_n$ con $\sigma \neq 1$, definimos la relación:

$$yRx \Longleftrightarrow \exists m \in \mathbb{Z} \mid y = \sigma^m(x)$$

Que es una relación de equivalencia:

- Propiedad reflexiva. Se tiene gracias a la Proposición 1.11.
- Propiedad simétrica. Sean $x, y \in X$ de forma que yRx, tenemos que $\exists m \in \mathbb{Z}$ de forma que $y = \sigma^m(x)$, pero entonces:

$$\sigma^{-m}(y) = \sigma^{-m}(\sigma^m(x)) = x \Longrightarrow xRy$$

- Propiedad transitiva. Sean $x, y, z \in X$ de forma que yRx y que zRx, entonces: $\exists p, q \in \mathbb{Z}$ de forma que:

$$\left.\begin{array}{r} y = \sigma^p(x) \\ z = \sigma^q(y) \end{array}\right\} \Longrightarrow z = \sigma^q(\sigma^p(x)) = \sigma^{p+q}(x) \Longrightarrow zRx$$

De esta forma, dado $x \in X$, podemos considerar su clase de equivalencia:

$$\overline{x} = \{\sigma^m(x) \mid m \in \mathbb{Z}\} \in X/R$$

Que es un conjunto finito, ya que gracias a la Proposición 1.11, existe $m \in \mathbb{N}$ de forma que $\sigma^{m+1}(x) = x$, con lo que:

$$C_x = \overline{x} = \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^m(x)\}$$

Si consideramos ahora el ciclo:

$$\gamma_x = (x\ \sigma(x)\ \sigma^2(x)\ \cdots\ \sigma^m(x)) \in S_n$$

Tenemos que:

$$\gamma_x(y) = \left\{ \begin{array}{cl} \sigma(y) & \text{si } y \in C_x \\ y & \text{si } y \notin C_x \end{array} \right.$$

De esta forma, tenemos una partición de X en clases de equivalencia, cada una de las C_x con $x \in X$, que llevan asociado un ciclo γ_x.

1. Sean $\overline{i}, \overline{j} \in X/R$ con $\overline{i} \neq \overline{j}$, entonces los elementos que se mueven en γ_i son los elementos de C_i, mientras los elementos que se mueven en γ_j son los de C_j. Como se tiene que $C_i \cap C_j = \emptyset$ por ser C_i y C_j clases de equivalencia distintas, llegamos a que γ_i y γ_j son ciclos disjuntos, para $\overline{i} \neq \overline{j}$.

2. Sea $\tau = \gamma_1\gamma_2 \ldots \gamma_n$, sea $y \in X$, entonces:

   $$\tau(y) = \gamma_1\gamma_2 \ldots \gamma_n(y) = \gamma_1\gamma_2 \ldots \gamma_y(y) = \gamma_1\gamma_2 \ldots \gamma_{y-1}(\sigma(y)) = \gamma_1(\sigma(y)) = \sigma(y)$$

   Ya que anteriormente vimos que:

   $$\gamma_j(y) = \left\{ \begin{array}{cl} \sigma(y) & \text{si } y \in C_j \\ y & \text{si } y \notin C_j \end{array} \right. \qquad \forall j \in X$$

   Y se verifica que $y, \sigma(y) \in C_y$. Por tanto, tenemos que $\tau = \sigma$. Si ahora despreciamos de la expresión de τ los ciclos de longitud menor que 2 (la identidad), la permutación σ no cambia y tenemos que σ se expresa como producto de ciclos disjuntos (por el apartado 1) de longitud mayor o igual que 2. □

Notación. A partir del Teorema 1.12, podemos introducir una nueva notación basada en los ciclos disjuntos. Dado $\sigma \in S_n$, como existe una única descomposición en ciclos disjuntos:

$$\sigma = \gamma_1\gamma_2 \ldots \gamma_k$$

Teníamos una notación estandar para cada ciclo. Ahora podemos notar σ como el producto de todas esas notaciones.

Como acabamos de decir, a partir del Teorema 1.12, podremos notar a las permutaciones como su descomposición en ciclos disjuntos. Sin embargo, merece la pena preguntarse sobre el orden de los ciclos en esta descomposición, pregunta a la que contestamos con la siguiente proposición:

Proposición 1.13. *Se verifican:*

1. *Si $\gamma_1, \gamma_2 \in S_n$ son dos ciclos disjuntos, entonces:*

$$\gamma_1\gamma_2 = \gamma_2\gamma_1$$

Es decir, el producto de ciclos disjuntos es conmutativo.

2. *Sea $\sigma \in S_n$ una permutación, si consideramos su descompoisición en ciclos disjuntos:*

$$\sigma = \gamma_1\gamma_2 \dots \gamma_k$$

Entonces, se tiene que:

$$\sigma^{-1} = \gamma_1^{-1}\gamma_2^{-1} \dots \gamma_k^{-1}$$

Demostración. Demostramos cada uno de los resultados:

1. Supongamos que:

$$\gamma_1 = (x_1 \ x_2 \ \dots \ x_n), \qquad \gamma_2 = (y_1 \ y_2 \ \dots \ y_m)$$
$$x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m \in X \text{ todos ellos distintos}$$

Tenemos entonces que:

- Si $x \neq x_i, x \neq y_j$ para $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$:

$$\gamma_1(\gamma_2(x)) = \gamma_1(x) = x = \gamma_2(x) = \gamma_2(\gamma_1(x))$$

- Si consideramos $i \in \{1, \dots, n-1\}$:

$$\gamma_1(\gamma_2(x_i)) = \gamma_1(x_i) = x_{i+1} = \gamma_2(x_{i+1}) = \gamma_2(\gamma_1(x_i))$$

Donde hemos usado que $x_i \neq y_j$ para todo $j \in \{1, \dots, m\}$.

- Si consideramos ahora $j \in \{1, \dots, m-1\}$:

$$\gamma_1(\gamma_2(y_j)) = \gamma_1(y_{j+1}) = y_{j+1} = \gamma_2(y_j) = \gamma_2(\gamma_1(y_j))$$

Donde hemos usado que $y_j \neq x_j$ para todo $i \in \{1, \dots, n\}$.

- Faltan los casos de x_n y y_m, que son análogos:

$$\gamma_1(\gamma_2(x_n)) = \gamma_1(x_n) = x_1 = \gamma_2(x_1) = \gamma_2(\gamma_1(x_n))$$
$$\gamma_1(\gamma_2(y_m)) = \gamma_1(y_1) = y_1 = \gamma_2(y_m) = \gamma_2(\gamma_1(y_m))$$

Como hemos visto que $\gamma_1(\gamma_2(x)) = \gamma_2(\gamma_1(x))$ para todo $x \in X$, concluimos que $\gamma_1\gamma_2 = \gamma_2\gamma_1$.

2. Dado $\sigma = \gamma_1\gamma_2 \dots \gamma_k$, buscamos una permutación $\tau \in S_n$ que verifique que:

$$\sigma\tau = \gamma_1\gamma_2 \dots \gamma_{k-1}\gamma_k\tau = 1$$

Observamos que como τ podemos tomar:

$$\tau = \gamma_k^{-1}\gamma_{k-1}^{-1} \dots \gamma_2^{-1}\gamma_1^{-1}$$

sin embargo, como los γ_i con $i \in \{1, \ldots, k\}$ eran ciclos disjuntos, por la Proposición 1.11, sabemos que los γ_i^{-1} también seguirán siendo ciclos disjuntos y por 1 sabemos que su producto es conmutativo, por lo que podemos escribir:

$$\tau = \gamma_1^{-1}\gamma_2^{-1} \ldots \gamma_k^{-1}$$

Como $\sigma\tau = 1$, concluimos que $\tau = \sigma^{-1}$.

□

Ejemplo. En S_{13}, consideramos:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{pmatrix}$$

De forma por ciclos disjuntos, podemos notar:

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$$

Dada una permutacion en notación de ciclos disjuntos, sabemos que para calcular la permutación inversa basta calcular la inversa de cada uno de los ciclos:

$$\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(2\ 13)(7\ 11\ 5)(6\ 9)$$

Del Teorema 1.12 deducimos el siguiente corolario:

Corolario 1.13.1. *El orden de una permutación $\sigma \in S_n$ es el mínimo común múltiplo de las longitudes de los ciclos disjuntos en los que se descompone.*

Demostración. Supongamos que σ se descompone de la forma:

$$\sigma = \gamma_1\gamma_2 \ldots \gamma_k$$

como $\gamma_i\gamma_j = \gamma_j\gamma_i$ para $i, j \in \{1, \ldots, k\}$, tenemos que $\forall m \in \mathbb{N}$:

$$\sigma^m = \gamma_1^m\gamma_2^m \ldots \gamma_k^m$$

Si $m = O(\sigma)$, entonces:

$$\sigma^m = 1 \Longleftrightarrow \gamma_i^m = 1 \overset{(*)}{\Longrightarrow} O(\gamma_i)|m \quad \forall i \in \{1, \ldots, k\}$$

Donde en $(*)$ hemos usado la Proposición 1.8. Concluimos que m es el mínimo común múltiplo de los órdenes de los ciclos, que por la Proposición 1.11, coincide con el mínimo común múltiplo de las longitudes de los ciclos. □

Ejemplo. Para familizarnos con la notación de permutaciones por ciclos disjuntos, vamos a enumerar todos los elementos de S_n para $n = 2, 3, 4$:

1. Para $n = 2$, tenemos $X = \{1, 2\}$ y por tanto:

$$S_2 = \{id, (1\ 2)\}$$

2. Para $n = 3$, tenemos $X = \{1, 2, 3\}$ y:

$$S_3 = \{id, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2, 3)\}$$

3. Para $n = 4$, tenemos $X = \{1, 2, 3, 4\}$ y:

$$\begin{aligned} S_4 = \{&id, (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), \\ &(1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 3\ 4), (1\ 3\ 2\ 4), (1\ 2\ 4\ 3), \\ &(1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \end{aligned}$$

Definición 1.15 (Elementos conjugados)**.** Sea G un grupo y $a, c \in G$, decimos que son conjugados si $\exists b \in G$ de forma que $a = bcb^{-1}$.

Proposición 1.14. *Si $\gamma \in S_n$ es un ciclo de longitud m, también lo será cualquier conjugado suyo. Es decir, si $\tau \in S_n$ y γ es un ciclo, entonces $\tau\gamma\tau^{-1}$ es un ciclo de longitud m.*

Demostración. Si $\gamma = (x_1\ x_2\ \dots\ x_m)$, sea $\tau \in S_n$, entonces veamos que:

$$\alpha = \tau\gamma\tau^{-1} = (\tau(x_1)\ \tau(x_2)\ \dots\ \tau(x_m))$$

Luego α será un ciclo de longitud m. Para ello, sea $y \in \{1, \dots, n\}$:

- Si $\tau^{-1}(y) = x_i \Longrightarrow y = \tau(x_i)$ con $i \in \{1, \dots, m-1\}$:

$$y \xmapsto{\tau^{-1}} x_i \xmapsto{\gamma} x_{i+1} \xmapsto{\tau} \tau(x_{i+1}) = \alpha(\tau(x_i))$$

- Si $\tau^{-1}(y) = x_m \Longrightarrow y = \tau(x_m)$:

$$y \xmapsto{\tau^{-1}} x_m \xmapsto{\gamma} x_1 \xmapsto{\tau} \tau(x_1) = \alpha(\tau(x_m))$$

- Si $\tau^{-1}(y) = x \Longrightarrow y = \tau(x)$ con $x \neq x_i$ para todo $i \in \{1, \dots, m\}$:

$$y \xmapsto{\tau^{-1}} x \xmapsto{\gamma} x \xmapsto{\tau} \tau(x) = \alpha(\tau(x))$$

Concluimos que $\alpha = (\tau(x_1)\ \tau(x_2)\ \dots\ \tau(x_m))$. □

Ejemplo. Veamos la última Proposición en un caso práctico. Si consideramos:

$$\tau = (1\ 3\ 4), \quad \gamma = (2\ 4\ 5\ 3), \quad \tau^{-1} = (4\ 3\ 1)$$

Y tratamos de estudiar la imagen de $X = \{1, 2, 3, 4, 5\}$ bajo $\alpha = \tau\gamma\tau^{-1}$:

$$\begin{gathered} 1 \xmapsto{\tau^{-1}} 4 \xmapsto{\sigma} 5 \xmapsto{\tau} 5 \\ 2 \longmapsto 2 \longmapsto 4 \longmapsto 1 \\ 3 \longmapsto 1 \longmapsto 1 \longmapsto 3 \\ 4 \longmapsto 3 \longmapsto 2 \longmapsto 2 \\ 5 \longmapsto 5 \longmapsto 3 \longmapsto 4 \end{gathered}$$

Tenemos entonces que α es también un ciclo de longitud 4:

$$\alpha = \tau\gamma\tau^{-1} = \left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{array}\right) = (1\ 5\ 4\ 2)$$

Proposición 1.15. *Sea $\sigma \in S_n$ una permutación de forma que se descompone en ciclos disjuntos de la forma:*

$$\sigma = \gamma_1 \dots \gamma_k$$

Entonces, podemos calcular su conjugado mediante $\tau \in S_n$ componiendo el conjugado de cada uno de los ciclos disjuntos en los que se descompone:

$$\tau\sigma\tau^{-1} = \tau\gamma_1\tau^{-1} \dots \tau\gamma_k\tau^{-1}$$

Demostración.

$$\tau\sigma\tau^{-1} = \tau\gamma_1 \dots \gamma_k\tau^{-1} = \tau\gamma_1 id\gamma_2 id \dots id\gamma_k\tau^{-1} = \tau\gamma_1\tau^{-1}\tau\gamma_2\tau^{-1} \dots \tau\gamma_k\tau^{-1}$$

□

Ejemplo. Para practicar la conjugación de ciclos aplicando las Proposiciones 1.14 y 1.15, se plantea dados:

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9), \qquad \tau = (4\ 8\ 12\ 7\ 5\ 9)$$

calcular $\tau\sigma\tau^{-1}$. Para ello, sabemos por la Proposición 1.15 que si[9] $\sigma = \gamma_1\gamma_2\gamma_3\gamma_4$, entonces basta calcular:

$$\tau\gamma_1\tau^{-1}, \quad \tau\gamma_2\tau^{-1}, \quad \tau\gamma_3\tau^{-1}, \quad \tau\gamma_4\tau^{-1}$$

Por la Proposición 1.14, sabemos que:

$$\begin{aligned}
\tau\gamma_1\tau^{-1} &= (\tau(1)\ \tau(12)\ \tau(8)\ \tau(10)\ \tau(4)) = (1\ 7\ 12\ 10\ 8) \\
\tau\gamma_2\tau^{-1} &= (\tau(2)\ \tau(13)) = (2\ 13) \\
\tau\gamma_3\tau^{-1} &= (\tau(5)\ \tau(11)\ \tau(7)) = (9\ 11\ 5) \\
\tau\gamma_4\tau^{-1} &= (\tau(6)\ \tau(9)) = (6\ 4)
\end{aligned}$$

Si lo escribimos todo junto:

$$\tau\sigma\tau^{-1} = (1\ 7\ 12\ 10\ 8)(2\ 13)(9\ 11\ 5)(6\ 4)$$

Proposición 1.16. *Toda permutación es un producto de transposiciones.*

Demostración. Dada $\sigma \in S_n$, esta tiene su descomposición en ciclos disjuntos:

$$\sigma = \gamma_1 \dots \gamma_k$$

Basta demostrar que todo ciclo es producto de transposiciones.
En efecto, sea $\gamma = (x_1\ x_2\ \dots\ x_m)$, podemos escribir:

$$(x_1\ x_2\ \dots\ x_m) = (x_1\ x_m)(x_1\ x_{m-1}) \dots (x_1 x_3)(x_1 x_2)$$

[9]Observar la descomposición hecha ya de σ.

Para verlo, observemos qué hace la aplicación de la derecha con cada elemento (léase la descomposición de derecha a izquierda):

$$\begin{aligned}
&x_1 \longmapsto x_2\\
&x_2 \longmapsto x_1 \longmapsto x_3\\
&x_3 \longmapsto x_1 \longmapsto x_4\\
&\vdots\\
&x_i \longmapsto x_1 \longmapsto x_{i+1}\\
&\vdots\\
&x_m \longmapsto x_1
\end{aligned}$$

O también podemos escribir:

$$(x_1\ x_2\ \ldots\ x_m) = (x_1\ x_2)(x_2\ x_3)\ldots(x_{m-1}\ x_m)$$

Para verlo:

$$\begin{aligned}
&x_1 \longmapsto x_2\\
&x_2 \longmapsto x_3\\
&x_3 \longmapsto x_4\\
&\vdots\\
&x_i \longmapsto x_{i+1}\\
&\vdots\\
&x_m \longmapsto x_{m-1} \longmapsto x_{m-2} \longmapsto \ldots \longmapsto x_3 \longmapsto x_2 \longmapsto x_1
\end{aligned}$$

□

Ejemplo. Sea $\sigma = (1\ 2\ 3\ 4\ 5)$, veamos que σ se puede descomponer en transposiciones de la forma:

$$\sigma = t_1t_2t_3t_4$$

Con $t_1 = (1\ 5),\ t_2 = (1\ 4),\ t_3 = (1\ 3),\ t_4 = (1\ 2)$.
Para ello, escribamos la imagen de $X = \{1, 2, 3, 4, 5\}$ mediante la permutación resultante de componer las 4 transposiciones $\gamma = t_1t_2t_3t_4$ y veamos que coincide con la de σ:

$$\left.\begin{array}{l}
1 \overset{t_4}{\longmapsto} 2 \overset{t_3}{\longmapsto} 2 \overset{t_2}{\longmapsto} 2 \overset{t_1}{\longmapsto} 2\\
2 \longmapsto 1 \longmapsto 3 \longmapsto 3 \longmapsto 3\\
3 \longmapsto 3 \longmapsto 1 \longmapsto 4 \longmapsto 4\\
4 \longmapsto 4 \longmapsto 4 \longmapsto 1 \longmapsto 5\\
5 \longmapsto 5 \longmapsto 5 \longmapsto 5 \longmapsto 1
\end{array}\right\} \Longrightarrow \left\{\begin{array}{l}
1 \overset{\gamma}{\longmapsto} 2\\
2 \longmapsto 3\\
3 \longmapsto 4\\
4 \longmapsto 5\\
5 \longmapsto 1
\end{array}\right.$$

De esta forma:

$$\gamma = t_1t_2t_3t_4 = \left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5\\ 2 & 3 & 4 & 5 & 1 \end{array}\right) = (1\ 2\ 3\ 4\ 5) = \sigma$$

Si ahora consideramos la descomposición de la forma:

$$\sigma = r_1r_2r_3r_4$$

Con $r_1 = (1\ 2)$, $r_2 = (2\ 3)$, $r_3 = (3\ 4)$, $r_4 = (4\ 5)$, escribimos ahora la imagen de X mediante la permutación $\tau = r_1 r_2 r_3 r_4$:

$$\left.\begin{array}{l} 1 \xmapsto{r_4} 1 \xmapsto{r_3} 1 \xmapsto{r_2} 1 \xmapsto{r_1} 2 \\ 2 \longmapsto 2 \longmapsto 2 \longmapsto 3 \longmapsto 3 \\ 3 \longmapsto 3 \longmapsto 4 \longmapsto 4 \longmapsto 4 \\ 4 \longmapsto 5 \longmapsto 5 \longmapsto 5 \longmapsto 5 \\ 5 \longmapsto 4 \longmapsto 3 \longmapsto 2 \longmapsto 1 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} 1 \xmapsto{\gamma} 2 \\ 2 \longmapsto 3 \\ 3 \longmapsto 4 \\ 4 \longmapsto 5 \\ 5 \longmapsto 1 \end{array}\right.$$

Vemos igual que antes que $\tau = \sigma$.

Proposición 1.17. *Una permutación admite varias descomposiciones en productos de transposiciones, pero todas ellas coinciden en la paridad del número de transposiciones.*

1.3.1. Signatura

Definición 1.16 (Signatura)**.** Consideraremos el siguiente polinomio de n variables:

$$\Delta = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j) \in \mathbb{Z}[x_1, \ldots, x_n]$$

Y definimos para cada $\sigma \in S_n$:

$$\sigma(\Delta) = \prod_{1 \leqslant i < j \leqslant n} (x_{\sigma(i)} - x_{\sigma(j)})$$

Podemos ahora definir la aplicación signatura $\varepsilon : S_n \longrightarrow \{-1, 1\}$ dada por:

$$\varepsilon(\sigma) = \left\{ \begin{array}{rl} 1 & \text{si } \sigma(\Delta) = \Delta \\ -1 & \text{si } \sigma(\Delta) = -\Delta \end{array} \right.$$

- Si $\varepsilon(\sigma) = 1$, diremos que σ es una permutación par.
- Si $\varepsilon(\sigma) = -1$, diremos que σ es una permutación impar.

Observación. A partir de la definición anterior, tenemos que $\sigma(\Delta) = \varepsilon(\sigma)\Delta$.

Ejemplo. Sea $n = 4$, estaremos interesados en el polinomio:

$$\Delta = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

Si consideramos $\sigma = (1\ 2\ 3\ 4)$, queremos comprobar cual es la signatura de σ. Como[10]:

$$\sigma(\Delta) = (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1) = -\Delta$$

Deducimos que $\varepsilon(\sigma) = -1$, es decir, σ es una permutación impar.

[10]Marcamos en rojo los factores que se invierten.

Proposición 1.18. *La aplicación signatura verifica que:*

$$\varepsilon\left(\prod_{i=1}^{m}\sigma_i\right)=\prod_{i=1}^{m}\varepsilon(\sigma_i)$$

Con $\sigma_1,\sigma_2,\ldots,\sigma_m\in S_n$.

Demostración. Por inducción sobre m:

- Para $m=2$: Queremos ver que dadas $\sigma,\tau\in S_n$, entonces:

  $$\varepsilon(\sigma\tau)=\varepsilon(\sigma)\varepsilon(\tau)$$

  Para ello, si vemos que $(\sigma\tau)(\Delta)=\sigma(\tau(\Delta))$ y que:

  $$\sigma(-\Delta)=\varepsilon(\sigma)(-\Delta)=-\varepsilon(\sigma)\Delta=-\sigma(\Delta)$$

  Basta distinguir casos:

  - Si σ es par:
    - Si τ es par, se tendrá $\sigma(\tau(\Delta))=\sigma(\Delta)=\Delta$, con lo que $\sigma\tau$ es par.
    - Si τ es impar, se tendrá $\sigma(\tau(\Delta))=\sigma(-\Delta)=-\sigma(\Delta)=-\Delta$, con lo que $\sigma\tau$ es impar.
  - Si σ es impar:
    - Si τ es par, se tendrá $\sigma(\tau(\Delta))=\sigma(\Delta)=-\Delta$, con lo que $\sigma\tau$ es impar.
    - Si τ es impar, se tendrá $\sigma(\tau(\Delta))=\sigma(-\Delta)=-\sigma(\Delta)=\Delta$, con lo que $\sigma\tau$ es par.

- Supuesto para $m-1$:

$$\varepsilon\left(\prod_{i=1}^{m}\sigma_1\right)=\varepsilon\left(\left(\prod_{i=1}^{m-1}\sigma_i\right)\sigma_m\right)=\varepsilon\left(\prod_{i=1}^{m-1}\sigma_i\right)\varepsilon(\sigma_m)\overset{(*)}{=}\prod_{i=1}^{m-1}\left(\varepsilon(\sigma_i)\right)\varepsilon(\sigma_m)=\prod_{i=1}^{m}\varepsilon(\sigma_i)$$

  Donde en $(*)$ hemos usado la hipótesis de inducción.

□

Proposición 1.19. *Se verifican los siguientes resultados:*

1. *Las transposiciones son permutaciones impares.*
2. *Una permutación es par si y solo si se descompone en el producto de un número par de transposiciones.*
3. *Un ciclo de longitud* $m\geqslant 2$ *es par si y solo si* m *es impar.*
4. *Una permutación es par si y solo si el número de ciclos de longitud par en su descomposición en ciclos disjuntos es par.*

Demostración. Demostramos cada uno de los resultados:

1. Sea $\sigma = (i\ j)$ una transposición (con $1 \leqslant i < j \leqslant n$), estudiemos qué sucede con $\sigma(\Delta)$:

   - Por una parte, está claro que hay un cambio de signo tras aplicar σ al factor $(x_i - x_j)$, ya que este pasa a ser $(x_j - x_i)$.
   - Está claro que los factores de la forma $(x_a - x_b)$ con $a, b \notin \{i, j\}$ se mantienen invariantes ante σ, por lo que no hay cambio de signo en estos.
   - Además, los factores de la forma $(x_a - x_y)$ con $y \in \{i, j\}$ y $a < i$ tampoco alteran el signo de Δ, ya que al aplicar σ:

     $$\begin{aligned}(x_a - x_i) &\stackrel{\sigma}{\longmapsto} (x_a - x_j)\\ (x_a - x_j) &\longmapsto (x_a - x_i)\end{aligned}$$

     Tenemos que un factor va al otro, por lo que no alteran el signo.
   - De forma análoga, los factores de la forma $(x_y - x_b)$ con $y \in \{i, j\}$ y $b > j$ tampoco alteran el signo de Δ:

     $$\begin{aligned}(x_i - x_b) &\stackrel{\sigma}{\longmapsto} (x_j - x_b)\\ (x_j - x_b) &\longmapsto (x_i - x_b)\end{aligned}$$

   - Finalmente, los únicos factores que nos quedan por considerar son los de la forma $(x_i - x_a)$ y $(x_a - x_j)$, con $i < a < j$. En este caso:

     $$\begin{aligned}(x_i - x_a) &\stackrel{\sigma}{\longmapsto} (x_j - x_a) = -(x_a - x_j)\\ (x_a - x_j) &\longmapsto (x_a - x_i) = -(x_i - x_a)\end{aligned}$$

     Fijado a con $i < a < j$, tanto el factor $(x_i - x_a)$ como el $(x_a - x_j)$ cambian de signo, por lo que el doble cambio de signo se compensa, luego estos factores no alteran el signo de Δ al aplicar σ.

   Concluimos que al aplicar $\sigma = (i\ j)$ sobre Δ, el signo obtenido es el mismo salvo por el factor $(x_i - x_j)$, que cambia de signo, por lo que:

   $$\sigma(\Delta) = -\Delta$$

   y llegamos a que σ es impar.

2. Sea $\sigma \in S_n$ una permutación, sabemos que puede descomponerse en k transposiciones:

   $$\sigma = \gamma_1 \gamma_2 \ldots \gamma_k$$

   Usando la Proposición 1.18 y 1, tenemos que:

   $$\varepsilon(\sigma) = \prod_{i=1}^{k} \varepsilon(\gamma_i) = \prod_{i=1}^{k} (-1) = (-1)^k$$

   Por lo que:

- Si k es par, entonces $\varepsilon(\sigma) = 1$.
- Si k es impar, entonces $\varepsilon(\sigma) = -1$.

3. Para $m = 2$, un ciclo de longitud m es una transposición, que ya sabemos que es impar. Sea τ un ciclo de longitud $m \geqslant 3$, en la Proposición 1.16 vimos que τ se podía descomponer como producto de $m-1$ transposiciones:

$$\tau = \gamma_1\gamma_2 \dots \gamma_{m-1}$$

Por tanto, y aplicando 2, tenemos que:

- Si m es par, entonces $m-1$ es impar, con lo que τ es impar.
- Si m es impar, entonces $m-1$ es par, con lo que τ es par.

4. Sea $\sigma \in S_n$, esta se puede descomponer como producto de k ciclos disjuntos de longitud mayor o igual que 2:

$$\sigma = \gamma_1\gamma_2 \dots \gamma_k$$

Usando la Proposición 1.18, tenemos que:

$$\varepsilon(\sigma) = \prod_{i=1}^{k} \varepsilon(\gamma_i)$$

Si consideramos la siguiente partición de $\{1, \dots, k\}$:

$$A = \{i \in \{1, \dots, k\} \mid \gamma_i \text{ tiene longitud impar}\}$$
$$B = \{i \in \{1, \dots, k\} \mid \gamma_i \text{ tiene longitud par}\}$$

Por 3 tenemos que $\varepsilon(\gamma_i) = 1$ para todo $i \in A$ y que $\varepsilon(\gamma_j) = -1$ para todo $j \in B$. De esta forma:

$$\varepsilon(\sigma) = \left(\prod_{i\in A} \varepsilon(\gamma_i)\right)\left(\prod_{i\in B} \varepsilon(\gamma_i)\right) = \left(\prod_{i\in A} 1\right)\left(\prod_{i\in B} -1\right) = \prod_{i\in B} -1 = (-1)^{|B|}$$

Por tanto:

- Si $|B|$ es par, tenemos que σ es par.
- Si $|B|$ es impar, tenemos que σ es impar.

□

Con esta Proposición, la demostración de la Proposición 1.17 se hace ya evidente.

Ejemplo. Ahora, es fácil determinar la signatura de cualquier permutación. Por ejemplo, si consideramos:

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$$

Como tiene 2 ciclos de longitud par (un número par), σ es una permutación par.

1.3.2. Grupos Alternados A_n

Definición 1.17 (Grupos Alternados A_n)**.** En S_n consideramos el conjunto:

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

Se verifica que $(A_n, \circ, 1)$ es un grupo:

- La asociatividad de $\circ$ es heredada de la de $\circ$ en S_n.
- El producto de dos permutaciones pares es par, luego está bien definido el grupo.
- La identidad es una permutación par, que es el neutro de la operación binaria.
- Dado $\sigma \in A_n$, escribimos su descomposición en ciclos disjuntos e invertimos cada ciclo. La longitud de los ciclos no cambia, luego la paridad del ciclo inverso tampoco, por lo que σ^{-1} sigue siendo una permutación par.

Al grupo A_n lo llamamos el grupo alternado de grado n, que verifica:

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

Observación. Notemos que si definimos $B_n = \{\sigma \in S_n \mid \sigma \text{ es impar}\}$, entonces sobre B_n no podemos tener una estructura de grupo con la operación $\circ$, ya que el neutro para $\circ$ de S_n no está en B_n, sino en A_n.

Ejemplo. Listar todos los elementos de los grupos alternados es fácil si previamente listamos todos los elementos de su grupo simétrico correspondiente:

1. Para $n = 3$:

$$S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$
$$A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$$

2. Para $n = 4$:

$$\begin{aligned} S_4 = \{&1, (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4),\\ &(1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4),\\ &(1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \end{aligned}$$

$$\begin{aligned} A_4 = \{&1, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),\\ &(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \end{aligned}$$

Proposición 1.20. *Se tiene que:*

(a) $S_n = \langle (1\ 2), (2\ 3), \dots, (n-1, n) \rangle$

(b) $S_n = \langle (1\ 2), (1\ 2\ \dots\ n) \rangle$

(c) $S_n = \langle (1\ 2), (1\ 3), \dots, (1\ n) \rangle$

(d) $A_n = \langle \{(x_1\ x_2\ x_3) \mid x_1, x_2, x_3 \in \{1, \dots, n\} \text{ distintos}\} \rangle$ *con* $n \geqslant 3$

(e) $A_n = \langle \{(1\ x\ y) \mid x, y \in \{1, \dots, n\} \text{ distintos}\} \rangle$ *con* $n \geqslant 3$

Demostración. Veamos cada uno de los enunciados:

(a) Sabemos que (por la Proposición 1.16):

$$S_n = \langle (i\ j) \mid i, j \in \{1, \dots, n\},\ i < j \rangle$$

Supuesto que $i < j$, vemos que:

$$(i\,j) = (i\,i{+}1)(i{+}1\,i{+}2)\dots(j{-}2\,j{-}1)(j{-}1\,j)(j{-}1\,j{-}2)\dots(i{+}2\,i{+}1)(i{+}1\,i)$$

(b) Por el apartado anterior, basta obtener cualquier transposición de la forma $(i\ i+1)$ con $i \in \{1, \dots, n-1\}$ a partir de $\sigma = (1\ 2\ \dots\ n)$ y $(1\ 2)$. Para ello, como se tiene que:

$$\sigma^{i-1}(1) = i \qquad \sigma^{i-1}(2) = i + 1$$

Podemos considerar el conjugado de $(1\ 2)$ mediante σ^{i-1}:

$$\sigma^{i-1}(1\ 2)\left(\sigma^{i-1}\right)^{-1} = \sigma^{i-1}(1\ 2)\sigma^{1-i} = (\sigma^{i-1}(1)\ \sigma^{i-1}(2)) = (i\ i+1)$$

(c) Basta ver que $(1\ 2\ \dots\ n)$ se puede obtener por composición de transposiciones de la forma $(1\ j)$ con $j \in \{2, \dots, n\}$, lo que ya se hizo en la Proposición 1.16:

$$(1\ 2\ \dots\ n) = (1\ n)(1\ n-1)\dots(1\ 3)(1\ 2)$$

(d) Podemos suponer que $x_1 < x_2 < x_3$, ya que:

$$(x_1\ x_3\ x_2) = (x_1\ x_2\ x_3)^2$$

Sabemos que si $\sigma \in A_n$, entonces será producto de un número par de transposiciones, por lo que basta expresar el producto de dos ciclos en función de ciclos de la forma $(x_1\ x_2\ x_3)$.

- Si hay elementos comunes, escribiremos:

$$(x_1\ x_2)(x_2\ x_3) = (x_1\ x_2\ x_3)$$

- Si no hay elementos comunes (tenemos dos transposiciones disjuntas), entonces:

$$(x_1\ x_2)(x_3\ x_4) = (x_1\ x_2\ x_3)(x_2\ x_3\ x_4)$$

(e) Usando el apartado anterior, tenemos que cualquier terna ordenada $(x_1\ x_2\ x_3)$ podemos escribirla de la forma:

$$(x_1\ x_2\ x_3) = (1\ x_3\ x_2)(1\ x_1\ x_2)(1\ x_1\ x_3)$$

□

Ejemplo. Usando la Proposición 1.20, veamos distintos conjuntos generadores para varios grupos:

(a) Destacamos:

- $S_3 = \langle (1\ 2), (2\ 3) \rangle$ y buscamos expresar la última transposición como producto de estas:
$$(1\ 3) = (1\ 2)(2\ 3)(2\ 1)$$
- En $S_4 = \langle (1\ 2), (2\ 3), (3\ 4) \rangle$ mostramos por ejemplo que:
$$(1\ 4) = (1\ 2)(2\ 3)(3\ 4)(3\ 2)(2\ 1)$$

(b) Ahora:

- En $S_3 = \langle (1\ 2), (1\ 2\ 3) \rangle$:
$$(2\ 3) = (1\ 2\ 3)(1\ 2)(1\ 2\ 3)^{-1}$$
- En $S_4 = \langle (1\ 2), (1\ 2\ 3\ 4) \rangle$:
$$\begin{aligned}(2\ 3) &= (1\ 2\ 3\ 4)(1\ 2)(1\ 2\ 3\ 4)^{-1}\\ (3\ 4) &= (1\ 2\ 3\ 4)^2(1\ 2)(1\ 2\ 3\ 4)^{-2}\end{aligned}$$

(d) Recordamos los elementos de A_4:
$$A_4 = \{1, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),\\ (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$
Tenemos que:
$$A_4 = \langle (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4) \rangle$$
Por ejemplo, podemos escribir:
$$(1\ 2)(3\ 4) = (1\ 2\ 3)(2\ 3\ 4)$$

(e) Tenemos:
$$A_4 = \langle (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4) \rangle$$

1.4. Grupos de matrices

Sea $\mathbb{F}$ un cuerpo, las matrices cuadradas de orden n sobre $\mathbb{F}$ las denotaremos por:
$$\mathcal{M}_n(\mathbb{F})$$
Sabemos que $(\mathcal{M}_n(\mathbb{F}), +, \cdot)$ es un anillo, aunque estaremos interesados en ver el conjunto $\mathcal{M}_n(\mathbb{F})$ como un grupo en su forma más interesante, es decir, como grupo con notación multiplicativa.

1.4.1. Grupo lineal $\mathrm{GL}_n(\mathbb{F})$

Definición 1.18 (Grupo lineal $\mathrm{GL}_n(\mathbb{F})$)**.** Sea $\mathbb{F}$ un cuerpo finito, en $\mathcal{M}_n(\mathbb{F})$ consideramos el conjunto:

$$\mathrm{GL}_n(\mathbb{F}) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det(A) \neq 0\}$$

Se verifica que $(\mathrm{GL}_n(\mathbb{F}), \cdot, I)$ es un grupo:

- La asociatividad de $\cdot$ viene heredada de la de $\cdot$ en $\mathcal{M}_n(\mathbb{F})$.
- Como el determinante del producto es el producto de los determinantes, $\cdot$ es una operación cerrada para $\mathrm{GL}_n(\mathbb{F})$.
- $\det(I) = 1 \neq 0$ y se tiene que I es el elemento neutro para $\cdot$.
- Como consideramos las matrices con determinante no nulo, sabemos que todas estas tienen inversa.

A $\mathrm{GL}_n(\mathbb{F})$ lo llamamos el grupo lineal de orden n.

Proposición 1.21. *Sea $n \in \mathbb{N}$, si $|\mathbb{F}| = q$, entonces se verifica que:*

$$|\mathrm{GL}_n(\mathbb{F})| = (q^n - 1)(q^n - q) \ldots (q^n - q^{n-1}) = \prod_{k=1}^{n} \left(q^n - q^{k-1}\right)$$

Demostración. Como $A \in \mathrm{GL}_n(\mathbb{F}) \Longleftrightarrow A$ es regular $\Longleftrightarrow$ sus filas son vectores linealmente independientes, basta contar de cuántas formas podemos elegir n vectores linealmente independientes con n entradas en $\mathbb{F}$ (que recordamos tenía q elementos). Para ello:

- Para elegir el primer vector $v_1 \in \mathbb{F}^n$, podemos elegir cualquiera, luego el problema es elegir n números de entre q posibilidades, q^n posibles elecciones.

  Sin embargo, como queremos que v_1 sea linealmente independiente con el resto de vectores que forman las filas de una matriz, hemos de exigir $v_1 \neq 0$, con lo que tenemos $q^n - 1$ posibilidades para v_1.
- Una vez elegido v_1, para elegir v_2 no podemos elegir un vector de $\mathcal{L}(v_1) \cong \mathbb{F}$, por lo que tenemos q vectores que no podemos elegir; elegimos un vector de los $q^n - q$ restantes.
- Repitiendo el proceso, una vez elegido v_{k-1}, para elegir v_k (con $k \in \{2, \ldots, n\}$), no podemos elegir ningún vector de $\mathcal{L}(v_1, \ldots, v_{k-1}) \cong \mathbb{F}^{k-1}$, por lo que tenemos q^{k-1} vectores que no podemos elegir y elegimos entre los $q^n - q^{k-1}$ restantes.

Este proceso ilusta que las posibles elecciones totales de vectores para las filas de una matriz de $\mathrm{GL}_n(\mathbb{F})$ son:

$$\prod_{k=1}^{n} \left(q^n - q^{k-1}\right)$$

Por lo que este debe ser el cardinal de $|\mathrm{GL}_n(\mathbb{F})|$. $\square$

Ejemplo. Veamos:

- En $|\operatorname{GL}_2(\mathbb{Z}_2)| = (2^2-1)(2^2-2) = 6$:

  $$\operatorname{GL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

  Podemos escribirlos sin que se nos olvide ninguna pensando en que tenemos que escribir todas las matrices de forma que los vectores formados por las columnas sean linealmente independientes entre sí (para así conseguir un determinante no nulo).

- Tenemos $|\operatorname{GL}_3(\mathbb{Z}_2)| = 168$. Se deja como ejercicio escribir todas las matrices.

- Tenemos $|\operatorname{GL}_2(\mathbb{Z}_3)| = 48$.

1.4.2. Grupo lineal especial $\operatorname{SL}_n(\mathbb{F})$

Definición 1.19 (Grupo lineal especial $\operatorname{SL}_n(\mathbb{F})$)**.** Sea $\mathbb{F}$ un cuerpo finito, en $\mathcal{M}_n(\mathbb{F})$ consideramos el conjunto:

$$\operatorname{SL}_n(\mathbb{F}) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det(A) = 1\}$$

Se verifica que $(\operatorname{SL}_n(\mathbb{F}), \cdot, I)$ es un grupo:

- La asociatividad de $\cdot$ viene heredada de la de $\cdot$ en $\mathcal{M}_n(\mathbb{F})$.
- Como el determinante del producto es el producto de los determinantes, $\cdot$ es una operación cerrada para $\operatorname{SL}_n(\mathbb{F})$.
- $\det(I) = 1$ y se tiene que I es el elemento neutro para $\cdot$.
- Como consideramos las matrices con determinante $1 \neq 0$, sabemos que todas estas tienen inversa.

A $\operatorname{SL}_n(\mathbb{F})$ lo llamamos el grupo lineal especial de orden n.

Proposición 1.22. *Sea $n \in \mathbb{N}$, si $|\mathbb{F}| = q$, entonces se verifica que:*

$$|\operatorname{SL}_n(\mathbb{F})| = \frac{|\operatorname{GL}_n(\mathbb{F})|}{q-1}$$

Demostración. Sea $A \in \operatorname{GL}_n(\mathbb{F})$, observemos que $\det(A)$ puede[11] tomar $q-1$ valores distintos, uno por cada elemento de $\mathbb{F}^*$. De esta forma, si dado $k \in \mathbb{F}^*$ definimos:

$$D_k = \{A \in \operatorname{GL}_n(\mathbb{F}) : \det(A) = k\}$$

Es claro que estos conjuntos forman una partición de $\operatorname{GL}_n(\mathbb{F})$:

$$\operatorname{GL}_n(\mathbb{F}) = \biguplus_{k \in \mathbb{F}^*} D_k$$

[11] De hecho los toma, es fácil comprobar que $\det : \operatorname{GL}_n(\mathbb{F}) \to \mathbb{F}^*$ es una aplicación sobreyectiva.

Veamos que $|D_k| = |D_1|$ para todo $k \in \mathbb{F}^*$. Para ello, sea $k \in \mathbb{F}^*$, definimos la aplicación $\varphi_k : \mathrm{GL}_n(\mathbb{F}) \to \mathrm{GL}_n(\mathbb{F})$ dada por:

$$\varphi_k(A) = \varphi_k((a_{ij})_{i,j}) = (\overline{a_{ij}})_{i,j} \qquad \forall A = (a_{ij})_{i,j} \in \mathrm{GL}_n(\mathbb{F})$$

Donde:

$$\overline{a_{ij}} = \left\{ \begin{array}{ll} ka_{ij} & \text{si } i = 1 \\ a_{ij} & \text{si } i \neq 1 \end{array} \right.$$

Es decir, φ_k multiplica la primera fila de una matriz por k. De esta forma, las propiedades de los determinantes nos dicen que si $A \in D_1$, entonces:

$$\det(\varphi_k(A)) = k \cdot \det(A) = k$$

Por lo que $\varphi_k(A) \in D_k$ para todo $k \in \mathbb{F}^*$. Por tanto, podemos definir la aplicación $\psi_k : D_1 \to D_k$ de forma que $\psi_k = \varphi_{k_{|D_1}}$. Veamos que ψ_k es biyectiva para terminar el razonamiento. Para ello, dada ψ_k para un cierto $k \in \mathbb{F}^*$, consideramos $\psi_{k^{-1}}$. Como:

$$kk^{-1}a_{ij} = k^{-1}ka_{ij} = a_{ij} \qquad \forall a_{ij} \in \mathbb{F}^*$$

Concluimos que $\psi_k^{-1} = \psi_{k^{-1}}$ y además vemos que $\varphi_{k^{-1}}(D_k) \subseteq D_1$. Llegamos a que ψ_k es biyectiva, por lo que $|D_k| = |D_1|$ para todo $k \in \mathbb{F}^*$.

Sea ahora $\phi : \{1, \ldots, q-1\} \to \mathbb{F}^*$ cualquier biyección de forma que $\phi(1) = 1$, como los D_k formaban una partición finita de $\mathrm{GL}_n(\mathbb{F})$, tenemos que:

$$|\mathrm{GL}_n(\mathbb{F})| = \sum_{k=1}^{q-1} |D_{\phi(k)}| = \sum_{k=1}^{q-1} |D_1| = (q-1)|D_1| = (q-1)|\mathrm{SL}_n(\mathbb{F})|$$

De donde deducimos que:

$$|\mathrm{SL}_n(\mathbb{F})| = \frac{|\mathrm{GL}_n(\mathbb{F})|}{q-1}$$

□

Ejemplo. Tenemos:

- $|\mathrm{SL}_2(\mathbb{Z}_3)| = 24$.
- $\mathrm{SL}_n(\mathbb{Z}_2) = \mathrm{GL}_n(\mathbb{Z}_2)\ \forall n \in \mathbb{N}$

1.5. Homomorfismos de grupos

Definición 1.20 (Homomorfismo)**.** Dados dos grupos G y H, un homomorfismo de grupos de G en H es una aplicación $f : G \to H$ que verifica:

$$f(xy) = f(x)f(y) \qquad \forall x, y \in G$$

Proposición 1.23. *Si $f : G \to H$ es un homomorfismo de grupos, entonces:*

1. $f(1) = 1$

2. $f(x^{-1}) = (f(x))^{-1}$
3. $f(x^n) = (f(x))^n \ \forall n \in \mathbb{N}$

Demostración. Veamos cada una:

1. $f(1) = f(1 \cdot 1) = f(1)f(1) \Longrightarrow f(1) = 1$
2. $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1}) \Longrightarrow f(x^{-1}) = (f(x))^{-1}$
3. $f(x^n) = f(\underbrace{x \cdot \ldots \cdot x}_{n \text{ veces}}) = \underbrace{f(x) \cdot \ldots \cdot f(x)}_{n \text{ veces}} = (f(x))^n$

□

Definición 1.21. Sea $f : G \to H$ un homomorfismo de grupos, distinguimos:

- $\ker f = \{x \in G \mid f(x) = 1\}$
- $Imf = \{f(x) \mid x \in G\}$

Ejemplo. Ejemplos de homomorfismos de grupos son:

1. Dado G un grupo, $id : G \to G$.
2. Dados G, H grupos, consideramos el siguiente homomorfismo, denominado *homomorfismo trivial*:
$$\begin{array}{rccc} f: & G & \longrightarrow & H \\ & x & \longmapsto & 1 \end{array}$$
3. La exponencial es también un homomorfismo:
$$\begin{array}{rccc} \exp: & (\mathbb{R}, +) & \longrightarrow & (\mathbb{R}^+, \cdot) \\ & x & \longmapsto & e^x \end{array}$$
4. La aplicación determinante de matrices con determinante no nulo:
$$\begin{array}{rccc} \det: & \mathrm{GL}_n(\mathbb{F}) & \longrightarrow & \mathbb{F}^* \\ & A & \longmapsto & \det(A) \end{array}$$
5. La aplicación signatura:
$$\begin{array}{rccc} \varepsilon: & S_n & \longrightarrow & \mathcal{U}(\mathbb{Z}) = \{-1, 1\} \\ & \sigma & \longmapsto & \varepsilon(\sigma) \end{array}$$

Proposición 1.24. *Sean $f : G \to H$ y $g : H \to T$ dos homomorfismos de grupos, entonces la aplicación $g \circ f : G \to T$ es un homomorfismo de grupos.*

Demostración. Sean $x, y \in G$, entonces:

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$$

□

Definición 1.22. Dado $f : G \to H$ un homomorfismo de grupos, decimos que:

- f es un monomorfismo si es inyectiva.
- f es un epimorfismo si es sobreyectiva.
- f es un isomorfismo si es biyectiva.
- Si $G = H$, diremos que f es un endomorfismo.
- Si f es un endomorfismo biyectivo, diremos que es un automorfismo.

Proposición 1.25. *Sea $f : G \to H$ un homomorfismo de grupos, entonces:*

i) *f es monomorfismo* $\iff \ker(f) = \{1\}$

ii) *f es isomorfismo* $\iff f^{-1}$ *es un isomorfismo.*

Demostración. Veamos los dos resultados:

i) Para el primero, demostramos las dos implicaciones:

$\Longrightarrow$) $x \in \ker(f) \Longrightarrow f(x) = 1 = f(1)$, pero como f es inyectiva, tenemos que $x = 1$.

$\Longleftarrow$) Sean $x, y \in G$ de forma que $f(x) = f(y)$, entonces:

$$f(x)(f(y))^{-1} = 1 \Longrightarrow f(xy^{-1}) = 1 \Longrightarrow xy^{-1} = 1 \Longrightarrow x = y$$

Concluimos que f es inyectiva.

ii) Demostramos las dos implicaciones:

$\Longrightarrow$) Si f es un isomorfismo, entonces es biyectiva, por lo que tendrá una aplicación inversa f^{-1}, que por lo pronto ya sabemos que es biyectiva. Basta ver que esta aplicación es un homomorfismo. Para ello, sean $y, y' \in H$, por ser f un biyectiva, existirán $x, x' \in G$ de forma que $f(x) = y$ y $f(x') = y'$, luego $x = f^{-1}(y)$ y $x' = f^{-1}(y')$. Por tanto:

$$f^{-1}(yy') = f^{-1}(f(x)f(x')) = f^{-1}(f(xx')) = xx' = f^{-1}(y)f^{-1}(y')$$

Lo que demuestra que f^{-1} es un homomorfismo biyectivo, luego isomorfismo.

$\Longleftarrow$) Si f^{-1} es un isomorfismo, entonces por la implicación que acabamos de demostrar, $(f^{-1})^{-1} = f$ también es un isomorfismo. $\square$

Definición 1.23 (Grupos isomorfos)**.** Sean G y H dos grupos, decimos que son isomorfos si existe un isomorfismo entre ellos, que se denotará por $G \cong H$.

Proposición 1.26. *La propiedad de ser isomorfo es una relación de equivalencia.*

Demostración. Demostramos cada una de las propiedades:

- Propiedad reflexiva. Sea G un grupo, como $id : G \to G$ es un homomorfismo, tenemos que $G \cong G$.

- Propiedad simétrica. Sean G y H dos grupos de forma que $G \cong H$, entonces existe un isomorfismo $f : G \to H$. Por la Proposición 1.25, $f^{-1} : H \to G$ también será un isomorfismo, por lo que $H \cong G$.
- Propiedad transitiva. Sean G, H y T tres grupos de forma que $G \cong H$ y $H \cong T$, entonces existen dos isomorfismos: $f : G \to H$ y $g : H \to T$. Si consideramos $g \circ f : G \to T$, tenemos por la Proposición 1.24 que $g \circ f$ es un isomorfismo de G en T, por lo que $G \cong T$.

□

Proposición 1.27. *Se verifican:*

i) *Si $f : X \to Y$ es una aplicación biyectiva, se tiene que la aplicación siguiente es un isomorfismo de grupos:*

$$\begin{array}{rccc} \varphi : & \text{Perm}(X) & \longrightarrow & \text{Perm}(Y) \\ & \sigma & \longmapsto & f\sigma f^{-1} \end{array}$$

ii) *$Aut(G) = \{f : G \to G \mid f \text{ automorfismo}\}$ con la composición forman un grupo.*

iii) *Si $f : G \to H$ es un isomorfismo, entonces $|G| = |H|$.*

iv) *Si G y H son isomorfos, entonces G es abeliano $\Longleftrightarrow$ H es abeliano.*

v) *Si $f : G \to H$ es un isomorfismo, entonces se mantiene el orden:*

$$O(x) = O(f(x)) \qquad \forall x \in G$$

vi) *Si $f : G \to H$ es un epimorfismo y $S \subseteq G$ cumple que $G = \langle S \rangle$, entonces $H = \langle f(S) \rangle$.*

Demostración. Veamos cada una:

i) Hemos de ver que φ es un homomorfismo biyectivo:

- Sean $\sigma, \tau \in \text{Perm}(X)$, entonces:

$$\varphi(\sigma\tau) = f\sigma\tau f^{-1} = f\sigma id\tau f^{-1} = f\sigma f^{-1} f\tau f^{-1} = \varphi(\sigma)\varphi(\tau)$$

- Definimos la siguiente aplicación:

$$\begin{array}{rccc} \psi : & \text{Perm}(Y) & \longrightarrow & \text{Perm}(X) \\ & \tau & \longmapsto & f^{-1}\tau f \end{array}$$

Veamos que ψ es la inversa de φ:

$$\begin{array}{c} \psi(\varphi(\sigma)) = \psi(f\sigma f^{-1}) = f^{-1} f\sigma f^{-1} f = \sigma \\ \varphi(\psi(\tau)) = \varphi(f^{-1}\tau f) = f(f^{-1}\tau f)f^{-1} = \tau \end{array}$$

Por tanto, φ es biyectiva.

Como φ es un homomorfismo biyectivo, es un isomorfismo.

ii) La asociatividad viene heredada de la asociatividad de funciones, el neutro del grupo es $id : G \to G$ y como son automorfismos, son aplicaciones biyectivas, con lo que cada una tiene inversa.

iii) Por ser f biyectiva, se tiene $|G| = |H|$.

iv) Veamos las dos implicaciones:

$\Longrightarrow$) Sean $x, y \in H$, existirá un isomorfismo $f : G \to H$, luego:

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

$\Longleftarrow$) Como $G \cong H \Longleftrightarrow H \cong G$ por la propiedad simétrica, se tiene la otra implicación.

v) Si $O(x) = n$, entonces:

$$(f(x))^n = f(x^n) = f(1) = 1$$

Por tanto, tenemos que $O(f(x)) \leqslant n$. Si suponemos ahora que $\exists m \in \mathbb{N}$ tal que $(f(x))^m = 1$, entonces $f(x^m) = 1 = f(1)$ y por inyectividad tenemos que $x^m = 1$, luego $n \leqslant m$. De todo esto deducimos que $O(f(x)) = n$.

Si $O(x) = +\infty$, basta observar que $f(x^n) = (f(x))^n$ para todo $n \in \mathbb{N} \setminus \{0\}$, para concluir que $O(f(x)) = +\infty$. Si $O(f(x)) = +\infty$, basta usar f^{-1}.

vi) Sea $y \in H$, buscamos una descomposición de y en función de los elementos $f(s_i)$. Para ello, como f es sobreyectiva, existirá $x \in G$ de forma que $y = f(x)$. Como $G = \langle S \rangle$, tendremos que existen $s_1, \ldots, s_k \in S$ y $\gamma_1, \ldots, \gamma_k \in \mathbb{Z}$ de forma que:

$$x = s_1^{\gamma_1} s_2^{\gamma_2} \ldots s_k^{\gamma_k}$$

Luego:

$$y = f(x) = f(s_1^{\gamma_1} s_2^{\gamma_2} \ldots s_k^{\gamma_k}) = f(s_1)^{\gamma_1} f(s_2)^{\gamma_2} \ldots f(s_k)^{\gamma_k}$$

Por lo que $H = \langle f(S) \rangle$.

□

1.5.1. Ejemplos

Teorema 1.28 (de Dyck)**.** *Sea G un grupo finito con una presentación*

$$G = \langle S \mid R_1, R_2, \ldots, R_k \rangle \qquad S = \{s_1, \ldots, s_m\}$$

Sea H otro grupo finito con $\{r_1, \ldots, r_m\} \subseteq H$, y supongamos que cualquier relación satisfecha en G por los s_i con $i \in \{1, \ldots, m\}$ es también satisfecha en H para los r_i con $i \in \{1, \ldots, m\}$. Entonces existe un único homomorfismo de grupos $f : G \to H$ de forma que:

$$f(s_i) = r_i \qquad i \in \{1, \ldots, n\}$$

- *Si además $\{r_1, \ldots, r_m\}$ son un conjunto de generadores de H, entonces f es un epimorfismo.*
- *Más aún, si $|G| = |H|$, entonces f es un isomorfismo.*

Ejemplo. Usando el Teorema 1.28, podemos dar muchos ejemplos de grupos isomorfos:

1. Si consideramos el grupo cíclico de orden n: $C_n = \langle x \mid x^n = 1\rangle$.

   Observamos que en $\mathbb{Z}_n$ el elemento $\overline{1}$ también verifica la propiedad $x^n = 1$, ya que:
   $$n \cdot \overline{1} = \underbrace{\overline{1} + \ldots + \overline{1}}_{n \text{ veces}} = 0$$
   De esta forma, por el Teorema 1.28, sabemos que existe un homomorfismo $f : C_n \to \mathbb{Z}_n$, de forma que $f(x) = 1$.

   Más aún, como $\mathbb{Z}_n = \left\langle \overline{1} \right\rangle$ y $|C_n| = n = |\mathbb{Z}_n|$, tenemos que f es un isomorfismo de grupos, por lo que $C_n \cong \mathbb{Z}_n$.

2. Si ahora consideramos el grupo de Klein abstracto:
   $$V^{\text{abs}} = \langle x, y \mid x^2 = y^2 = 1, xy = yx\rangle$$
   Podemos intentar relacionarlo con el grupo directo $\mathbb{Z}_2 \times \mathbb{Z}_2$, ya que los elementos $(0, 1)$ y $(1, 0)$ cumplen las relaciones enunciadas:
   $$\begin{gathered} 2 \cdot (0, 1) = (0, 1) + (0, 1) = (0, 0) \\ 2 \cdot (1, 0) = (1, 0) + (1, 0) = (0, 0) \\ (0, 1) + (1, 0) = (1, 1) = (1, 0) + (0, 1) \end{gathered}$$
   Por lo que existirá un homomorfismo $f : V^{\text{abs}} \to \mathbb{Z}_2 \times \mathbb{Z}_2$ de forma que $f(x) = (0, 1)$ y $f(y) = (1, 0)$.

   Más aún, como $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (0, 1), (1, 0)\rangle$ y es claro que $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4 = |V^{\text{abs}}|$, tenemos que f es un isomorfismo, por lo que $V^{\text{abs}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

3. Si tratamos ahora de relacionar el grupo de Klein abstracto (visto en el ejemplo anterior) con el grupo de Klein:
   $$V = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$
   Como $(1\ 2)(3\ 4)$ y $(1\ 3)(2\ 4)$ verifican que:
   $$\begin{aligned} &(1\ 2)(3\ 4)^2 = (1\ 2)(3\ 4)(1\ 2)(3\ 4) = 1 \\ &(1\ 3)(2\ 4)^2 = (1\ 3)(2\ 4)(1\ 3)(2\ 4) = 1 \\ &(1\ 2)(3\ 4)(1\ 3)(2\ 4) = (1\ 4)(2\ 3) = (1\ 3)(2\ 4)(1\ 2)(3\ 4) \end{aligned}$$
   Por el Teorema de Dyck, existe un homomorfismo $g : V^{\text{abs}} \to V$ de forma que $g(x) = (1\ 2)(3\ 4)$ y $g(y) = (1\ 3)(2\ 4)$.

   Como hemos visto ya que $V = \langle g(x), g(y)\rangle$ y que $|V^{\text{abs}}| = 4 = |V|$, g es un isomorfismo. Tenemos que $V^{\text{abs}} \cong V$.

   Como vimos que $\cong$ es una relación de equivalencia, también tendremos que $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

4. Consideramos ahora el grupo diédrico de orden 3:

$$D_3 = \langle r, s \mid r^3 = 1, s^2 = 1, sr = r^2 s\rangle$$

Que vamos a intentar relacionar con S_3. Como $(1\ 2)$ y $(1\ 2\ 3)$ verifican que:

$$\begin{aligned}
&(1\ 2\ 3)^3 = (1\ 2\ 3)(1\ 2\ 3)(1\ 2\ 3) = 1\\
&(1\ 2)^2 = (1\ 2)(1\ 2) = 1\\
&(1\ 2)(1\ 2\ 3) = (2\ 3) = (1\ 3\ 2)(1\ 2) = (1\ 2\ 3)^2(1\ 2)
\end{aligned}$$

Tenemos que existe un homomorfismo $f : D_3 \to S_3$ de forma que $f(r) = (1\,2\,3)$ y $f(s) = (1\ 2)$. Como además tenemos que[12] $S_3 = \langle (1\ 2), (1\ 2\ 3)\rangle$ y que $|D_3| = 2 \cdot 3 = 6 = 3! = |S_3|$, concluimos que f es un isomorfismo, por lo que $D_3 \cong S_3$.

5. Si consideramos el grupo lineal de orden 2 sobre $\mathbb{Z}_2$:

$$\mathrm{GL}_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

Y tratamos de relacionarlo con $S_3 = \langle r, s \mid r^3 = 1, s^2 = 1, sr = r^2 s\rangle$, como tenemos que:

$$\begin{aligned}
\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^3 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\\
\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\\
\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\end{aligned}$$

Entonces, existe un homomorfismo $f : S_3 \to \mathrm{GL}_2(\mathbb{Z}_2)$ de forma que:

$$f(r) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \qquad f(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Además, como (ver el Ejercicio 10 de la Relación 2):

$$\mathrm{GL}_2(\mathbb{Z}_2) = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$$

Y ambos tienen el mismo número de elementos, f es un isomorfismo.

6. Fijado $n \in \mathbb{N} \setminus \{0, 3\}$, si ahora consideramos el grupo simétrico de orden n, S_n y el grupo diédrico de orden n, D_n, como $|D_n| = 2n \neq n! = |S_n|$ no vamos a tener un isomorfismo de grupos. Sin embargo, los elementos:

$$(1\ 2\ \dots\ n), \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix} \in S_n$$

[12] Esto se vio en la Proposición 1.20.

Verifican todas las propiedades de la presentación de D_n, por lo que existirá un homomorfismo $f : D_n \to S_n$ de forma que

$$f(r) = (1\ 2\ \dots\ n)$$
$$f(s) = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}$$

7. Si consideramos ahora:

$$Q_2^{\text{abs}} = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle$$

Y pensamos en relacionarlo con $Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$, como tenemos que:

$$\begin{aligned} &i^4 = 1 \\ &j^2 = -1 = i^2 \\ &ji(-j) = j(-k) = -i \end{aligned}$$

Sabemos que existe un homomorfismo $f : Q_2^{\text{abs}} \to Q_2$ de forma que $f(x) = i$ y $f(y) = j$. Además, como $Q_2 = \langle i, j \rangle$ y $|Q_2^{\text{abs}}| = 4 = |Q_2|$, tenemos que f es un isomorfismo, por lo que $Q_2^{\text{abs}} \cong Q_2$.

8. Como último ejemplo, si consideramos $k, n \in \mathbb{N}$, $k \geqslant 3$ con $k \mid n$ y consideramos los grupos diédricos:

$$\begin{aligned} D_n &= \langle r, s \mid r^n = 1, s^2 = 1, sr = r^{-1}s \rangle \\ D_k &= \langle r_1, s_1 \mid r_1^k = 1, s_1^2 = 1, s_1r_1 = r_1^{-1}s_1 \rangle \end{aligned}$$

Y tratamos de relacionarlos, como $k \mid n$, existirá $p \in \mathbb{N}$ de forma que $n = kp$.

Como $r_1, s_1 \in D_k$ verifican que:

$$\begin{aligned} &r_1^n = r_1^{kp} = (r_1^k)^p = 1^p = 1 \\ &s_1^2 = 1 \\ &s_1r_1 = r_1^{-1}s_1 \end{aligned}$$

Tenemos por el Teorema 1.28 que existe un homomorfismo $f : D_n \to D_k$ de forma que $f(r) = r_1$ y $f(s) = s_1$.

1.6. Resumen de grupos

Para finalizar este capítulo, haremos un breve repaso de los grupos vistos hasta el momento, ya que los usaremos de forma constante a lo largo de la asignatura, por lo que conviene tenerlos siempre presentes.

Grupo Trivial. $(\{e\}, *, e)$.

Grupos de los enteros módulo n. $(\mathbb{Z}_n, +)$, $(\mathcal{U}(\mathbb{Z}_n), \cdot)$.

Grupo de raíces $n-$ésimas de la unidad.

$$\mu_n = \left\{1, \xi, \xi^2, \dots, \xi^{n-1} \mid \xi = \cos\left(\frac{2\pi}{n}\right) + i \operatorname{sen}\left(\frac{2\pi}{n}\right)\right\} \subseteq \mathbb{C}$$

Grupo lineal de orden n. Sea $\mathbb{F}$ un cuerpo:

$$\mathrm{GL}_n(\mathbb{F}) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det(A) \neq 0\}$$

Grupo lineal especial de orden n. Sea $\mathbb{F}$ un cuerpo:

$$\mathrm{SL}_n(\mathbb{F}) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det(A) = 1\}$$

Potencias de grupos. Sea G un grupo y X un conjunto:

$$G^X = Apl(X, G) = \{f : X \to G \mid f \text{ aplicación}\}$$

$n-$**ésimo grupo diédrico.** Sea $n \in \mathbb{N}$:

$$D_n = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$$

$n-$**ésimo grupo simétrico.** Sea X un conjunto con $|X| = n \in \mathbb{N}$:

$$S_n = \mathrm{Perm}(X) = \{f : X \to X \mid f \text{ biyectiva}\}$$

$n-$**ésimo grupo alternado.** Sea $n \in \mathbb{N}$:

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

Grupo cíclico de orden n. Sea $n \in \mathbb{N}$:

$$C_n = \langle x \mid x^n = 1\rangle = \{1, x, x^2, x^3, \dots, x^{n-1}\}$$

Grupo de los cuaternios.

$$Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$$

Grupo abstracto $Q_2^{\mathbf{abs}}$.

$$\begin{aligned} Q_2^{\mathrm{abs}} &= \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1}\rangle \\ &= \{1, x, x^2, x^3, y, yx, yx^2, yx^3\} \end{aligned}$$

Grupo de Klein. Sea $n \in \mathbb{N}$ con $n \geqslant 4$:

$$V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subseteq S_n$$

Grupo de Klein abstracto.

$$V^{\mathrm{abs}} = \langle x, y \mid x^2 = y^2 = 1, xy = yx\rangle = \{1, x, y, xy\}$$

2. Subgrupos, Generadores, Retículos y Grupos cíclicos

Definición 2.1 (Subgrupo)**.** Dados dos grupos G y H, decimos que H es un subgrupo de G, denotado por $H < G$, si $H \subseteq G$ y la aplicación de inclusión[1] $i : H \to G$ es un homomorfismo de grupos.

Observación. Dado un grupo $(G, *, e)$, este tendrá siempre dos subgrupos:

- $(\{e\}, *, e)$, al que llamaremos subgrupo trivial.
- El propio $(G, *, e)$

Definición 2.2. Sea H un subgrupo de otro G, diremos que H es un subgrupo impropio de G si H es el grupo trivial o el propio G. En otro caso, diremos que H es un subgrupo propio de G.

Notación. Recordamos la notación que ya usábamos en Álgebra I para, fijado $n \in \mathbb{N} \setminus \{0\}$, denotar a todos los múltiplos de n en $\mathbb{Z}$:

$$n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$$

Ejemplo. Vemos claramente que:

1. $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$
2. $\{r^k \mid k \leqslant n, r \in D_n\} < D_n$
3. $n\mathbb{Z} < \mathbb{Z}$ para todo $n \in \mathbb{N}$.
4. $\mathrm{SL}_n(\mathbb{F}) < \mathrm{GL}_n(\mathbb{F})$
5. $(\mathbb{Q}^*, \cdot) \not< (\mathbb{R}, +)$ No es un subgrupo, ya que $i(1) = 1 \neq 0$.
6. $(\mathbb{Z}^+, +) \not< (\mathbb{Z}, +)$, ya que $(\mathbb{Z}^+, +)$ no es un grupo.
7. $D_6 \not< D_8$, ya que $D_6 \not\subseteq D_8$.

Observación. Si G, H y T son grupos de forma que $G < H < T$, entonces $G < T$.

Demostración. La transitividad de $\subseteq$ nos da que $G \subseteq H \subseteq T$. Por otra parte, como las inclusiones $j : G \to H$ y $k : H \to T$ son homomorfismos, tendremos que $i = k \circ j : G \to T$ es un homomorfismo. $\square$

[1]Viene dada por $i(x) = x$, para todo $x \in H$.

Proposición 2.1. *Sea G un grupo y $\emptyset \neq H \subseteq G$, entonces son equivalentes:*

i) $H < G$

ii) *Se verifican:*

  (a) *Si* $x, y \in H$ *entonces* $xy \in H$.
  (b) $1 \in H$.
  (c) *Si* $x \in H$, *entonces* $x^{-1} \in H$.

iii) *Si* $x, y \in H$, *entonces* $xy^{-1} \in H$.

Demostración. Veamos las implicaciones de forma cíclica:

$i) \Longrightarrow ii)$ Como H es un grupo, por su definición se han de cumplir (a), (b) y (c).

$ii) \Longrightarrow iii)$ Si $x, y \in H$, entonces $y^{-1} \in H$, por lo que tendremos que $xy^{-1} \in H$.

$iii) \Longrightarrow i)$ Como $\emptyset \neq H$, existirá al menos un $x \in H$, por lo que $xx^{-1} = 1 \in H$. Además, si $x \in H$ también tendremos que $1x^{-1} = x^{-1} \in H$. Para ver que H es un grupo, tan solo nos falta ver que su operación interna está bien definida; es decir, que si $x, y \in H$, entonces $xy \in H$. Dados $x, y \in H$, tendremos que $y^{-1} \in H$, por lo que:

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

Con esto tenemos ya que H es un grupo. Al considerar en H la misma operación que en G, tenemos directamente que $i : H \to G$ es un homomorfismo, ya que $id : H \to H$ es un homomorfismo y al extender el codominio para considerar la aplicación inclusión i, seguirá siendo un homomorfismo[2].

Esta observación la usaremos con frecuencia en toda la asignatura: cada vez que tengamos G un grupo y $H \subseteq G$, como casi siempre consideraremos en H la misma operación que en G, bastará simplemente demostrar también que H es un grupo, para así concluir que $H < G$.

□

Proposición 2.2. *Sea G un grupo finito y $\emptyset \neq H \subseteq G$, entonces son equivalentes:*

i) $H < G$

ii) *Si* $x, y \in H$, *entonces* $xy \in H$

Demostración. Veamos las dos implicaciones:

$i) \Longrightarrow ii)$ Se verifica por ser H un grupo.

$ii) \Longrightarrow i)$ Como G es finito, por la Proposición 1.9, para todo $x \in G$ existirá $n > 0$ de forma que $x^n = 1$, por lo que $x^{-1} = x^{n-1}$. De esto deducimos que $x^{-1} \in H$ y que $1 = xx^{-1} \in H$. Por la Proposición 2.1, $H < G$.

[2]Notemos que si en H tenemos una operación distinta que en G esto no siempre será cierto y habrá que comprobar que $i : H \to G$ es un homomorfismo.

□

Ejemplo. Se deja como ejercicio comprobar que:

1. $A_n < S_n$
2. Todo subgrupo de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$ con $n \in \mathbb{N}$.
3. $V < S_4$
4. Si $n \mid m$, entonces $D_n < D_m$

Definición 2.3. Sea G un grupo, $f : G \to G'$ una aplicación, y $H \subseteq G$, $H' \subseteq G'$, definimos:

- El conjunto imagen directa de H por f como el conjunto:

$$f_*(H) = \{f(x) \mid x \in H\} \subseteq G'$$

- El conjunto imagen inversa de H' por f como el conjunto:

$$f^*(H') = \{x \in G \mid f(x) \in H'\} \subseteq G$$

Proposición 2.3. *Sea $f : G \to G'$ un homomorfismo de grupos, entonces:*

i) *Si $H < G$, entonces $f_*(H) < G'$*

ii) *Si $H' < G'$, entonces $f^*(H') < G$*

Demostración. Demostramos las dos implicaciones:

i) Sean $x, y \in f_*(H)$, entonces $\exists a, b \in H$ de forma que $x = f(a), y = f(b)$. Como H es un subgrupo de G, tendremos que $ab^{-1} \in H$, por lo que:

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

Concluimos que $f_*(H)$ es un subgrupo de G'.

ii) Sean $x, y \in f^*(H')$, entonces $a = f(x), b = f(y) \in H'$. Por ser H' un subgrupo de G', tendremos que

$$ab^{-1} = f(x)f(y)^{-1} = f(xy^{-1}) \in H'$$

Por tanto, $xy^{-1} \in f^*(H')$. Concluimos que $f^*(H')$ es un subgrupo de G.

□

Proposición 2.4. *Sea $\{H_i\}_{i\in I}$ una familia de subgrupos de G, entonces la intersección de todos ellos sigue siendo un subgrupo de G:*

$$\bigcap_{i\in I} H_i < G$$

Demostración. En primer lugar, como $H_i < G$ para todo $i \in I$, se ha de verificar que $1 \in H_i$ $\forall i \in I$, por lo que $1 \in \bigcap_{i\in I} H_i \neq \emptyset$. Como la intersección es no vacía, podemos pensar en aplicar el tercer punto de la Proposición 2.1 para comprobar que es un subgrupo de G.

Para ello, sean $x, y \in \bigcap_{i\in I} H_i$, entonces $x, y \in H_i$ para todo $i \in I$, por lo que por ser $H_i < G$, tendremos que $xy^{-1} \in H_i$ $\forall i \in I$, luego:

$$xy^{-1} \in \bigcap_{i\in I} H_i$$

Concluimos que $\bigcap_{i\in I} H_i$ es un subgrupo de G. □

Ejemplo. En general, la unión de subgrupos no es un subgrupo:

$$2\mathbb{Z} \cup 3\mathbb{Z} \not< \mathbb{Z}$$

Ya que $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ y $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

2.1. Generadores de subgrupos

Definición 2.4 (Subgrupo generado)**.** Sea G un grupo y $S \subseteq G$, definimos el subgrupo generado por S como el menor subgrupo de G que contiene a S, es decir:

$$\langle S\rangle = \bigcap\{H < G \mid S \subseteq H\}$$

Observación. Notemos que, gracias a la Proposición 2.4, $\langle S\rangle$ efectivamente es un subgrupo de G.

Proposición 2.5. *Sea $(G, \cdot, e)$ un grupo, $S \subseteq G$, entonces:*

- *Si $S = \emptyset$, entonces $\langle S\rangle = \{e\}$, el grupo trivial.*
- *Si $S \neq \emptyset$, entonces $\langle S\rangle = \{x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \mid m \geqslant 1, x_i \in S, \gamma_i \in \mathbb{Z}\}$*

Demostración. Distinguimos casos:

- Si $S = \emptyset$, entonces $\{e\} < G$ con $S \subseteq \{e\}$. Como $\{e\}$ solo tiene un elemento y todo subgrupo de G contiene a e, concluimos que:

$$\langle S\rangle = \bigcap\{H < G \mid S \subseteq H\} = \{e\}$$

- Si $S \neq \emptyset$, por doble inclusión:

$\supseteq$) Como $S \subseteq \langle S\rangle$ y $\langle S\rangle$ es un grupo, tendremos que:

$$x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \in \langle S\rangle \qquad x_i \in S, \gamma_i \in \mathbb{Z} \quad \forall 1 \leqslant i \leqslant m$$

$\subseteq$) Si llamamos A al conjunto de la derecha, A es un grupo, ya que si tomamos $a, b \in A$, existirán $x_1, \dots, x_p$ y $y_1, \dots, y_q$ en S y $\gamma_1, \dots, \gamma_p, \alpha_1, \dots, \alpha_q \in \mathbb{Z}$ de forma que:

$$a = x_1^{\gamma_1} \dots x_p^{\gamma_p} \qquad b = y_1^{\alpha_1} \dots y_q^{\alpha_q}$$

Por lo que

$$ab^{-1} = x_1^{\gamma_1} \dots x_p^{\gamma_p} y_q^{-\alpha_q} \dots y_1^{-\alpha_1} \in A$$

Lo que demuestra que A es un subgrupo de G. Además, como es claro que $S \subseteq A$, tenemos un grupo del que S es subconjunto, por lo que por ser $\langle S \rangle$ el menor subgrupo que contiene a S, está claro que $\langle S \rangle \subseteq A$. □

Corolario 2.5.1. *Si $S \subseteq G$ de forma que $\langle S \rangle = G$, entonces S es un conjunto de generadores de G.*

Demostración. Por la Proposición 2.5, sabemos que si $\langle S \rangle = G$, entonces cualquier elemento $x \in G$ se puede expresar de la forma:

$$x = x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \qquad x_i \in S, \gamma_i \in \mathbb{Z}, \quad \forall 1 \leqslant i \leqslant m$$

Por lo que S es un conjunto de generadores de G. □

Ejemplo. Ejemplos interesantes de subgrupos generados por ciertos conjuntos son:

1. Si $S = \{r\} \subseteq D_n$, entonces $\langle S \rangle = \{1, r, r^2, \dots, r^{n-1}\}$
2. Si $S = \{s\} \subseteq D_n$, entonces $\langle S \rangle = \{1, s\}$
3. Si $S = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4)\} \subseteq S_4$, entonces $\langle S \rangle = V$
4. Si $S = \{(x_1\ x_2\ x_3) \mid x_1 < x_2 < x_3\} \subseteq S_n$, entonces $\langle S \rangle = A_n$
5. Si $S = \left\{ \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{C})$, entonces $\langle S \rangle < \mathrm{GL}_2(\mathbb{C})$.

En la Proposición 2.4 vimos que la intersección de una familia arbitraria de subgrupos era un subgrupo, mientras que con el ejemplo de $2\mathbb{Z} \cup 3\mathbb{Z} \subseteq \mathbb{Z}$, vimos que, en general, la unión de dos subgrupos no es un subgrupo. Sin embargo, cabe preguntarse de qué forma podemos hacer una operación parecida con subgrupos para sí obtener un subgrupo. De esto nace la siguiente definición.

Definición 2.5 (Compuesto)**.** Sea $\{H_i\}_{i \in I}$ una familia de subgrupos de un grupo G, llamamos compuesto de los subgrupos H_i, denotado por $\bigvee\limits_{i \in I} H_i$, al subgrupo:

$$\bigvee_{i \in I} H_i = \left\langle \bigcup_{i \in I} H_i \right\rangle$$

Cuando tengamos un número finito de subgrupos $\{H_1, H_2, \dots, H_n\}$, notaremos:

$$H_1 \vee H_2 \vee \ldots \vee H_n$$

Notemos que es natural la definición, ya que como la unión de subgrupos no es en general un subgrupo, buscamos el menor subgrupo que contenga a la unión de subgrupos, que por definición es el compuesto de la familia de subgrupos que queríamos unir.

2.2. Retículo de subgrupos de un grupo

Introduciremos ahora el concepto de retículo[3], estructura algebraica de gran interés que usaremos brevemente para trabajar de forma cómoda con el conjunto de todos los subgrupos de un grupo.

Definición 2.6 (Retículo)**.** Un retículo es una tripleta $(L, \vee, \wedge)$ donde:

- L es un conjunto no vacío.
- $\wedge$ y $\vee$ son dos operaciones[4] binarias en L que verifican las leyes:

  i) Conmutativa:
  $$a \vee b = b \vee a \qquad a \wedge b = b \wedge a$$

  ii) Asociativa:
  $$a \vee (b \vee c) = (a \vee b) \vee c \qquad a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

  iii) de Absorción:
  $$a \vee (a \wedge b) = a \qquad a \wedge (a \vee b) = a$$

  iv) de Idempotencia:
  $$a \vee a = a \qquad a \wedge a = a$$

En el caso de que $(L, \vee, \wedge)$ sea un retículo, es común definir una relación binaria notada por "$\leqslant$" y definida por:

$$a \leqslant b \Longleftrightarrow a \vee b = b \Longleftrightarrow a \wedge b = a$$

donde para la segunda equivalencia hemos empleado la conmutatividad y la propiedad de absorción.

Proposición 2.6. *Todo retículo $(L, \vee, \wedge)$ junto con la relación de orden $\leqslant$ que se define a partir de sus operaciones es un conjunto parcialmente ordenado.*

Demostración. Hemos de probar las propiedades:

- <u>Reflexiva.</u> Por la propiedad de idempotencia, dado $a \in L$, tenemos que:
  $$a \vee a = a \Longrightarrow a \leqslant a$$
- <u>Antisimétrica.</u> Sean $a, b \in L$ de forma que $a \leqslant b$ y $b \leqslant a$. Por definición de $\leqslant$, tenemos que:
  $$a \vee b = b \qquad b \vee a = a$$
  Y aplicando la conmutatividad de $\vee$ llegamos a que:
  $$a = a \vee b = b \vee a = b$$

[3]Que en el contexto de teoría de conjuntos o del orden puede tener otra definición.

[4]Es común referirse a $\vee$ por "supremo" y a $\wedge$ por "ínfimo".

- Transitiva. Sean $a, b, c \in L$ de forma que $a \leqslant b$ y $b \leqslant c$, es decir, $a \vee b = b$ y $b \vee c = c$, entonces:

$$a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$$

De donde deducimos que $a \leqslant c$.

□

Ejemplo. Ejemplos de retículos son:

1. El retículo endoplasmático rugoso.
2. Dado un número $n \in \mathbb{N}$, el conjunto de divisores de n:

$$D(n) = \{m \in \mathbb{N} : m \text{ divide a } n\}$$

Junto con las operaciones de:

$$\begin{aligned} a \vee b &= \text{mcm}(a, b) \\ a \wedge b &= \text{mcd}(a, b) \end{aligned}$$

forma un retículo[5]. En este, la relación de orden que obtenemos es la de "ser divisor de"; es decir, si $a, b \in D(n)$, entonces:

$$a \leqslant b \Longleftrightarrow a \mid b$$

3. En la asignatura LMD vimos que los álgebras de Boole eran retículos.

Lema 2.7. *Sea G un grupo y $T, U < G$, entonces:*

$$\langle \langle T \rangle \cup U \rangle = \langle T \cup U \rangle$$

Demostración. Hagámoslo por doble inclusión:

$\supseteq$) Basta ver que:

$$T \subseteq \langle T \rangle \Longrightarrow T \cup U \subseteq \langle T \rangle \cup U \Longrightarrow \langle T \cup U \rangle \subseteq \langle \langle T \rangle \cup U \rangle$$

$\subseteq$) Sea $x \in \langle \langle T \rangle \cup U \rangle$, entonces existirán $\alpha_1, \ldots, \alpha_n \in \langle T \rangle$, $u_1, \ldots, u_m \in U$ y $\gamma_1, \ldots, \gamma_{n+m} \in \mathbb{Z}$ de forma que:

$$x = \alpha_1^{\gamma_1} \ldots \alpha_n^{\gamma_n} u_1^{\gamma_{n+1}} \ldots u_m^{\gamma_{n+m}}$$

Pero por ser $\alpha_1, \ldots, \alpha_n \in \langle T \rangle$, podemos encontrar $t_{ij} \in T$ y $\delta_{ij} \in \mathbb{Z}$ de forma que:

$$\begin{aligned} \alpha_1 &= t_{11}^{\delta_{11}} \ldots t_{1n_1}^{\delta_{1n_1}} \\ &\vdots \\ \alpha_n &= t_{n1}^{\delta_{n1}} \ldots t_{nn_n}^{\delta_{nn_n}} \end{aligned}$$

Por lo que:

$$x = t_{11}^{\delta_{11}} \ldots t_{1n_1}^{\delta_{1n_1}} \ldots t_{nn_n}^{\delta_{nn_n}} u_1^{\gamma_{n+1}} \ldots u_m^{\gamma_{n+m}} \in \langle T \cup U \rangle$$

[5]Es un buen ejercicio comprobarlo.

□

Proposición 2.8. *Sea G un grupo, si definimos el conjunto de subgrupos de G:*

$$\Lambda_G = \{H \subseteq G \mid H < G\}$$

Se verifica que Λ_G es un retículo, junto con las operaciones:

$$\begin{aligned} T \vee U &= \langle T \cup U \rangle \\ T \wedge U &= T \cap U \end{aligned}$$

Además, la relación de orden en Λ_G es $\subseteq$.

Demostración. De Álgebra I ya sabemos que la intersección de conjuntos es conmutativa, asociativa y que tiene la propiedad de idempotencia. Veamos estas para el compuesto de dos subgrupos, que se deducen a partir de las propiedades conmutativa, asociativa y de idempotencia para la unión de dos conjuntos:

- Conmutativa. Sean $T, U \in \Lambda_G$:

$$T \vee U = \langle T \cup U \rangle = \langle U \cup T \rangle = U \vee T$$

- Asociativa. Sean $T, U, V \in \Lambda_G$:

$$\begin{aligned} T \vee (U \vee V) = T \vee \langle U \cup V \rangle = \langle T \cup \langle U \cup V \rangle \rangle &\overset{(*)}{=} \langle T \cup U \cup V \rangle \\ &\overset{(*)}{=} \langle \langle T \cup U \rangle \cup V \rangle = \langle T \cup U \rangle \vee V = (T \vee U) \vee V \end{aligned}$$

  Donde en $(*)$ hemos aplicado el Lema anterior.

- Idempotencia. Sea $T \in \Lambda_G$:

$$T \vee T = \langle T \cup T \rangle = \langle T \rangle \overset{(*)}{=} T$$

  Donde en $(*)$ hemos usado que T es un grupo, por ser subgrupo de G.

Finalmente, nos queda comprobar las propiedades de absorción. Para ello, sean $T, U \in \Lambda_G$:

$$\begin{gathered} T \vee (T \cap U) = \langle T \cup (T \cap U) \rangle = \langle (T \cup T) \cap (T \cup U) \rangle = \langle T \cap (T \cup U) \rangle = \langle T \rangle = T \\ T \cap (T \vee U) = T \cap \langle T \cup U \rangle = T \end{gathered}$$

Para ver que la relación de orden es $\subseteq$, notemos que si $T, U \in \Lambda_G$, entonces:

$$A \subseteq B \Longleftrightarrow A \cap B = A$$

Que es como se define la relación de orden para los retículos. □

Al trabajar con retículos, una estructura que surge de forma natural son los diagramas de Hasse, que nos permiten comprender mucho mejor la estructura de un retículo concreto.

Definición 2.7 (Diagrama de Hasse)**.** Sea $(L, \leqslant)$ un conjunto finito parcialmente ordenado, definimos su diagrama de Hasse como el grafo dirigido (V, E) donde:

- Los vértices son cada uno de los elementos de L, es decir: $V = L$.

- Dados dos vértices $a, b \in V$ con $a \neq b$, tendremos una arista de a a b $(a \to b)$ si $a \leqslant b$ y no existe ningún elemento $c \in V$ con $a \neq c \neq b$ de forma que $a \leqslant c \leqslant b$.

  Es decir, escribiremos $a \to b$ en el caso en el que $a \leqslant b$, obviando los ciclos (ya que $\leqslant$ es una relación reflexiva) y las relaciones que puedan deducirse de la transitividad de $\leqslant$: si $a \leqslant b$ y $b \leqslant c$, no consideraremos la arista $a \to c$.

Notación. Por comodidad y claridad a la hora de dibujar los diagramas de Hasse, no dibujaremos grafos dirigidos, sino lo que haremos será primero ordenar los vértices por "niveles" en función de la cardinalidad de los subgrupos: colocaremos en el nivel más bajo el menor subgrupo del grupo que consideremos (notemos que siempre será el subgrupo trivial $\{e\}$) e iremos subiendo en niveles por la cardinalidad del subgrupo, hasta llegar al nivel superior, donde colocaremos al grupo de mayor cardinal (que coincidirá con el grupo que consideramos inicialmente).

En segundo lugar, uniremos aquellos nodos que han de estar unidos mediante aristas no dirigidas (entendiendo que en realidad son aristas dirigidas, todas ellas apuntando hacia arriba, que es donde están los conjuntos más grandes).

De esta forma, tendremos el diagrama de Hasse ordenado por niveles, donde podremos ver "qué tan grande" es cada subgrupo, así como las relaciones de inclusión entre ellos gracias a las aristas.

2.2.1. Ejemplos

Ejemplo. Diagramas de Hasse para ciertos retículos[6] son:

1. Para $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$:

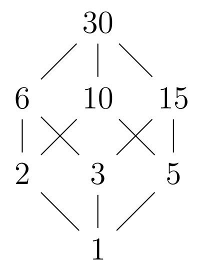


Figura 2.1: Diagragama de Hasse para $D(30)$.

2. Para $\mathcal{B}^3$, el álgebra de Boole con 3 elementos, tenemos:

[6] Notemos que cualquier retículo es un conjunto parcialmente ordenado.

$$\begin{tikzcd}[arrows=dash]
 & (1,\ 1,\ 1) \arrow[dl] \arrow[d] \arrow[dr] & \\
(1,\ 1,\ 0) \arrow[d] \arrow[dr] & (1,\ 0,\ 1) \arrow[dl] \arrow[dr] & (0,\ 1,\ 1) \arrow[dl] \arrow[d] \\
(1,\ 0,\ 0) \arrow[dr] & (0,\ 1,\ 0) \arrow[d] & (0,\ 0,\ 1) \arrow[dl] \\
 & (0,\ 0,\ 0) &
\end{tikzcd}$$

Figura 2.2: Diagragama de Hasse para $\mathcal{B}^3$.

Centrándonos ya en los retículos que nos interesan, daremos a continuación varios ejemplos de retículos formados por los subgrupos de un grupo dado, que representaremos mediante sus diagramas de Hasse (en estos aparecerán las aristas etiquetadas con números, que por ahora ignoraremos, pero que luego señalaremos lo que significan).

Ejemplo. Veamos varios ejemplos con grupos de la forma $\mathbb{Z}_n$:

1. Para calcular el retículo de subgrupos de $\mathbb{Z}_4$, hemos de pensar primero en todos los subgrupos posibles de $\mathbb{Z}_4$. Para ello[7], vemos que:

$$\begin{aligned}
\langle 0\rangle &= \{0\}\\
\langle 1\rangle &= \mathbb{Z}_4\\
\langle 2\rangle &= \{0,2\}\\
\langle 3\rangle &= \mathbb{Z}_4
\end{aligned}$$

Concluimos que $\Lambda_{\mathbb{Z}_4} = \{\{0\},\{0,2\},\mathbb{Z}_4\}$. Pasamos ahora a ver cómo se relacionan mediante su diagrama de Hasse.

$$\begin{tikzcd}
\mathbb{Z}_4 \arrow[d, dash, "2"] \\
\langle 2\rangle \arrow[d, dash, "2"] \\
\{0\}
\end{tikzcd}$$

Figura 2.3: Diagrama de Hasse para los subgrupos de $\mathbb{Z}_4$.

2. En $\mathbb{Z}_6$ tenemos que[8]:

$$\begin{aligned}
\langle 1\rangle = \langle 5\rangle &= \mathbb{Z}_6\\
\langle 2\rangle = \langle 4\rangle &= \{0,2,4\}\\
\langle 3\rangle &= \{0,3\}
\end{aligned}$$

[7] Al final del tema se entenderá por qué es suficiente con esto.

[8] Hemos escrito directamente los subgrupos de $\mathbb{Z}_6$, pero lo que hemos hecho para buscarlos todos es pensar en todos los posibles conjuntos de generadores.

Y podemos dibujar su diagrama de Hasse:

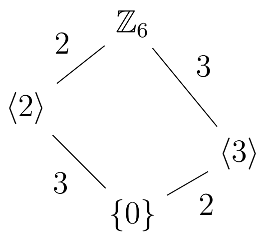


Figura 2.4: Diagrama de Hasse para los subgrupos de $\mathbb{Z}_6$.

3. En $\mathbb{Z}_8$, tenemos que:

$$\begin{aligned}
\langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle &= \mathbb{Z}_8\\
\langle 2\rangle = \langle 6\rangle &= \{0,2,4,6\}\\
\langle 4\rangle &= \{0,4\}
\end{aligned}$$

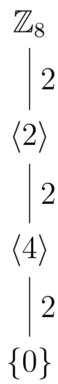


Figura 2.5: Diagrama de Hasse para los subgrupos de $\mathbb{Z}_8$.

4. En $\mathbb{Z}_{12}$, tenemos:

$$\begin{aligned}
\langle 1\rangle = \langle 5\rangle = \langle 7\rangle = \langle 11\rangle &= \mathbb{Z}_{12}\\
\langle 2\rangle = \langle 10\rangle &= \{0,2,4,6,8,10\}\\
\langle 3\rangle = \langle 9\rangle &= \{0,3,6,9\}\\
\langle 4\rangle = \langle 8\rangle &= \{0,4,8\}\\
\langle 6\rangle &= \{0,6\}
\end{aligned}$$

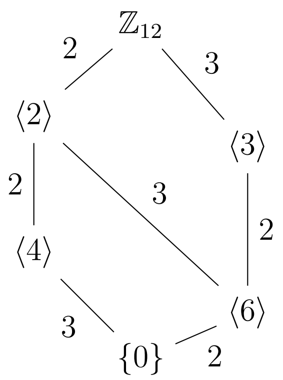


Figura 2.6: Diagrama de Hasse para los subgrupos de $\mathbb{Z}_{12}$.

Ejemplo. Si trabajamos ahora con otro tipo de grupos:

1. Si consideramos el grupo de Klein:

$$V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Todos sus subgrupos posibles son:

$$V, \langle(1\ 2)(3\ 4)\rangle, \langle(1\ 3)(2\ 4)\rangle, \langle(1\ 4)(2\ 3)\rangle, \{1\}$$

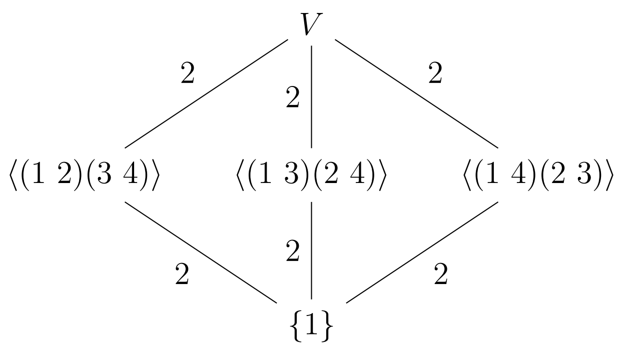


Figura 2.7: Diagrama de Hasse para los subgrupos del grupo de Klein.

2. En el grupo de los cuaternios:

$$Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$$

Los subgrupos posibles son:

$$Q_2, \langle i\rangle, \langle j\rangle, \langle k\rangle, \langle -1\rangle, \{1\}$$

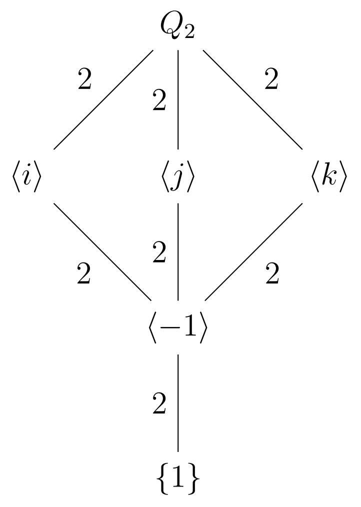


Figura 2.8: Diagrama de Hasse para los subgrupos del grupo de los cuaternios.

3. En $S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, los posibles subgrupos son:

$$S_3, \langle (1\ 2\ 3) \rangle, \langle (1\ 2) \rangle, \langle (1\ 3) \rangle, \langle (2\ 3) \rangle, \{1\}$$

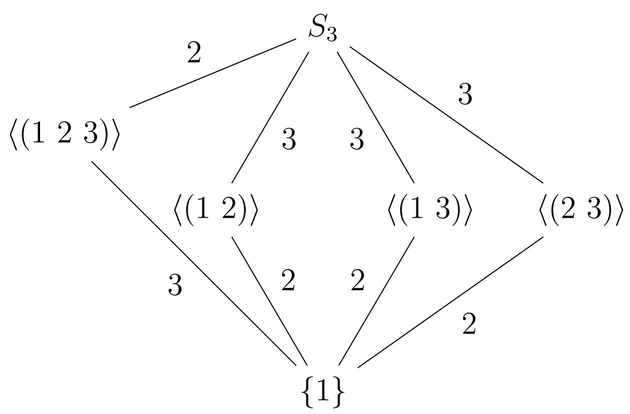


Figura 2.9: Diagrama de Hasse para los subgrupos de S_3.

4. En $D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$, los posibles subgrupos son:

$$\begin{gathered}
\langle r \rangle = \langle r^3 \rangle = \{1, r, r^2, r^3\} \\
\langle r^2 \rangle = \{1, r^2\} \\
\langle s \rangle = \{1, s\} \\
\langle sr \rangle = \{1, sr\} \\
\langle sr^2 \rangle = \{1, sr^2\} \\
\langle sr^3 \rangle = \{1, sr^3\} \\
\langle r^2, s \rangle = \{1, r^2, s, sr^2\} \\
\langle r^2, sr \rangle = \{1, r^2, sr, sr^3\}
\end{gathered}$$

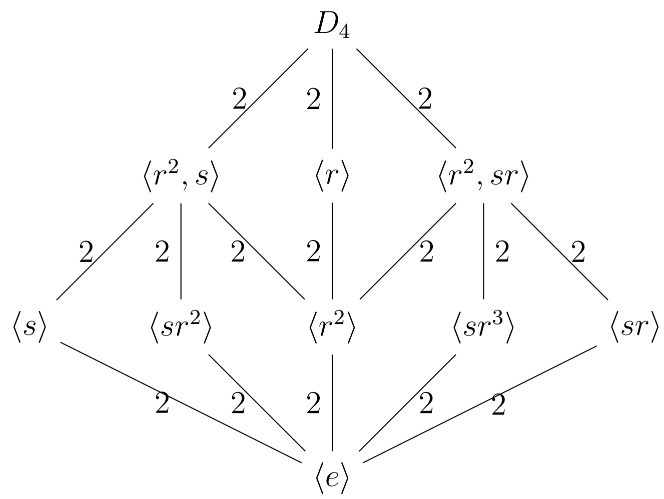


Figura 2.10: Diagrama de Hasse para los subgrupos de D_4.

Ejemplo. Obtenemos un ejemplo interesante al considerar los grupos:

$$G = \langle x, y \mid x^8 = y^2 = 1, xy = yx\rangle$$
$$H = \langle u, v \mid u^2 = v^8 = 1, vu = uv^5\rangle$$

Donde H recibe el nombre de "grupo modular de orden 16", notemos que ambos grupos tienen orden 16. En general, si consideramos dos grupos isomorfos, obtendremos dos diagramas de Hasse que serán grafos isomorfos entre sí. Sin embargo, el recíproco no es cierto, si tenemos dos diagramas de Hasse que sean grafos isomorfos, los grupos de los que partían no tienen por qué ser isomorfos. En este ejemplo se pone de manifiesto, ya que G y H no son isomorfos (basta con observar que G es conmutativo y H no), pero veremos que tienen diagramas de Hasse isomorfos. Antes de ello, debemos calcular todos los subgrupos de cada uno, cosa que no vamos a detallar pero sí daremos aquellos subgrupos más grandes:

- G tiene 3 subgrupos de orden 8: $\langle x^2, y\rangle$, $\langle x\rangle$, $\langle xy\rangle$.

- H tiene 3 subgrupos de orden 8: $\langle u, v^2\rangle$, $\langle u\rangle$, $\langle uv\rangle$.

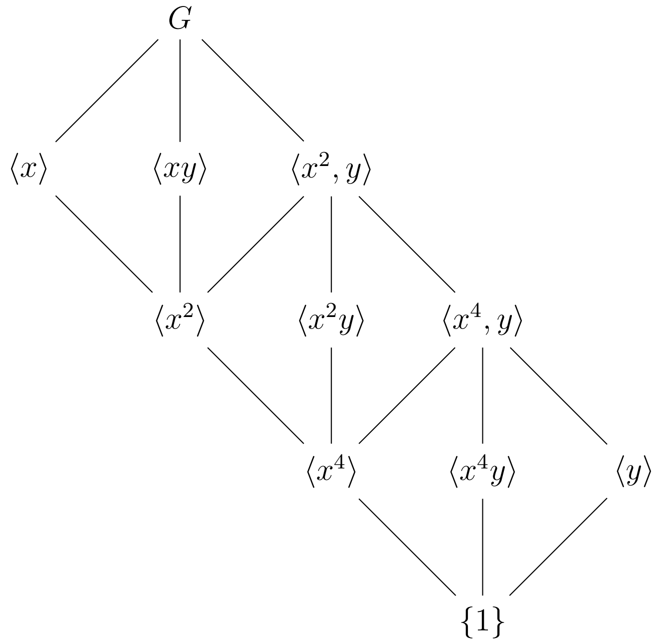


Figura 2.11: Diagrama de Hasse para los subgrupos de G.

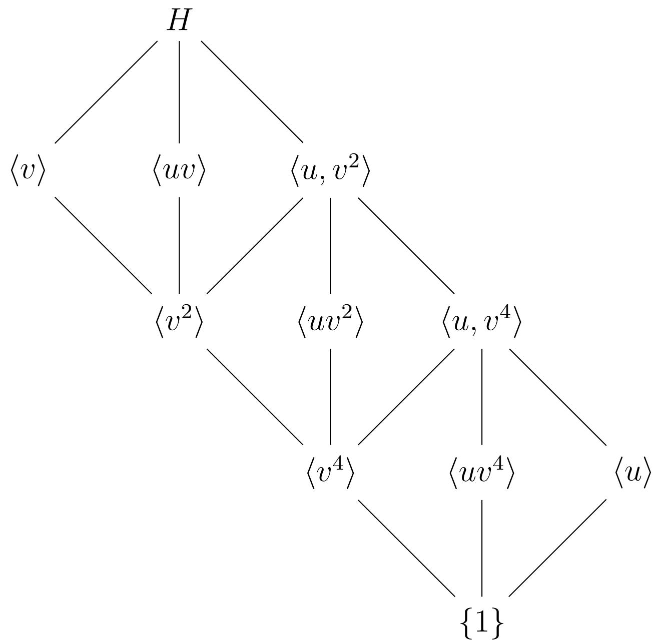


Figura 2.12: Diagrama de Hasse para los subgrupos de H.

A lo largo de todos estos ejemplos hemos debido darnos cuenta de una particularidad, que se pone de manifiesto especialmente en el ejemplo de los $\mathbb{Z}_n$. Resulta que los órdenes de los subgrupos que hemos ido obteniendo dividían al orden del grupo, resultado que luego demostraremos en general. Sin embargo, estamos ya en condiciones de demostrar que el contrarrecíproco no es cierto en general, es decir, no todos los divisores del orden de un grupo se corresponden con el orden de algún subgrupo suyo.

Proposición 2.9. *El orden del subgrupo divide al orden del grupo, pero no todos los divisores del orden del grupo se corresponden con el orden de algún subgrupo suyo.*

Veremos que el orden de todo subgrupo divide al orden del grupo (en caso de ser el grupo finito) en el Teorema de Lagrange (Teorema 2.13).

Ejemplo. Para ver que el recíproco no se cumple, consideramos:

$$A_4 = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 4\ 3), (2\ 4\ 3)\}$$

Que recordamos tiene de orden:

$$|A_4| = \frac{4!}{2} = 4 \cdot 3 = 12$$

Y todos los posibles divisores de 12 son:

$$D(12) = \{1, 2, 3, 4, 6, 12\}$$

Sin embargo, A_4 tiene:

- Un subgrupo de orden 1, $\{1\}$.
- Cuatro subgrupos de orden 3.
- Un subgrupo de orden 4, $V < A_4$.
- Tres subgrupos de orden 2.
- Un subgrupo de orden 12, A_4.

Más aún, veamos que es imposible que tenga un subgrupo de orden 6.

Demostración. Supongamos que existe $H < A_4$ de forma que $|H| = 6$. En dicho caso, viendo todos los elementos de A_4, concluimos que H debe contener al menos un 3−ciclo:

$$(x_1\ x_2\ x_3) \in H$$

En dicho caso, por ser H un subgrupo de A_4, también debe estar su elemento inverso:

$$(x_1\ x_3\ x_2) \in H$$

Ahora, distingamos casos:

- Si H no tiene más 3−ciclos, la única posibilidad (observando nuevamente todos los elementos de A_4) es que H sea de la forma:

  $$H = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (x_1\ x_2\ x_3), (x_1\ x_3\ x_2)\}$$

  En cuyo caso, observemos que $V < H$. Sin embargo, $|V| = 4 \nmid 6 = |H|$, contradicción.

- Si H tiene otro 3−ciclo, por ejemplo $(x_1\ x_2\ x_4)$, también ha de contener a su inverso, por lo que:

$$\{(x_1\ x_2\ x_3), (x_1\ x_3\ x_2), (x_1\ x_2\ x_4), (x_1\ x_4\ x_2)\} \subseteq H$$

Sin embargo, como:

$$(x_1\ x_2\ x_3)(x_1\ x_4\ x_2) = (x_1\ x_4\ x_3)$$

Concluimos que también $(x_1\ x_4\ x_3)$ y su inverso: $(x_1\ x_3\ x_4)$ deben estar en H, luego H es un subgrupo formado por 6 3−ciclos, contradicción, ya que H debe también contener al 1.

Concluimos que no puede existir un subgrupo de A_4 con 6 elementos. □

2.3. Índice y Teorema de Lagrange

Definición 2.8. Sea G un grupo, $H, K < G$, definimos:

$$HK = \{hk \mid h \in H, k \in K\}$$

Proposición 2.10. *Sea G un grupo, $H, K < G$, tenemos que HK es un subgrupo de G si y solo si $HK = KH$. En cuyo caso, tendremos que:*

$$HK = H \vee K$$

Demostración. Por doble implicación:

$\Longrightarrow$) Veamos que $KH = HK$ por doble inclusión:

$\subseteq$) Sean $k \in K, h \in H$, tenemos que:

$$kh = \left(h^{-1}k^{-1}\right)^{-1} \in HK \Longrightarrow KH \subseteq HK$$

$\supseteq$) Observemos que la única hipótesis que tenemos es que HK es un subgrupo de G (nada tenemos sobre KH). Sean $h \in H, k \in K$:

$$hk = \left(k^{-1}h^{-1}\right)^{-1} \in HK$$

Por lo que $k^{-1}h^{-1} \in HK$, luego existirán $h_1 \in H$, $k_1 \in K$ de forma que:

$$k^{-1}h^{-1} = h_1k_1$$

Finalmente:

$$hk = \left(k^{-1}h^{-1}\right)^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$$

$\Longleftarrow$) Sean $hk, h_1k_1 \in HK$, queremos ver qué pasa con $hk(h_1k_1)^{-1}$:

$$hk(h_1k_1)^{-1} = hkk_1^{-1}h_1^{-1} \overset{(*)}{=} hk_2h_2 \overset{(**)}{=} hh_3k_3 \in HK$$

Donde:

- En $(*)$ hemos aplicado que K es un grupo, ya que si $k, k_1 \in K$, entonces $kk_1^{-1} \in K$, por lo que existirá $k_2 = kk_1^{-1} \in K$.

  De forma análoga, como $h_1 \in H$, tenemos que $h_1^{-1} \in H$, por lo que existirá $h_2 = h_1^{-1} \in H$.
- En $(**)$ hemos aplicado que $k_2h_2 \in KH = HK$, por lo que existirán $h_3 \in H$, $k_3 \in K$ de forma que $k_2h_2 = h_3k_3$.

Falta ver que si $HK < G$ con $HK = KH$ (que ya sabemos que son equivalentes), entonces:

$$HK = H \vee K$$

$\subseteq$) Sea $x \in HK$, entonces $\exists h \in H, k \in K$ de forma que $x = hk \in \langle H \cup K\rangle = H \vee K$.

$\supseteq$) Sea $x \in H \vee K$, entonces sabemos que existen $\alpha_1, \dots, \alpha_n \in H \cup K$ y $\gamma_1, \dots, \gamma_n \in \mathbb{Z}$ de forma que:

$$x = \alpha_1^{\gamma_1} \dots \alpha_n^{\gamma_n}$$

Como $HK = KH$, tras varias conmutaciones de términos, existirán $h_1, \dots, h_p \in H$, $k_{p+1}, \dots, k_n \in K$ y $\delta_1, \dots, \delta_n \in \mathbb{Z}$ de forma que:

$$x = h_1^{\delta_1} \dots h_p^{\delta_p} k_{p+1}^{\delta_{p+1}} \dots k_n^{\delta_n}$$

Y por ser H y K grupos, tendremos que:

$$h = h_1^{\delta_1} \dots h_p^{\delta_p} \in H$$
$$k = k_{p+1}^{\delta_{p+1}} \dots k_n^{\delta_n} \in K$$

Por lo que $x = hk \in HK$. □

Definición 2.9. Sea G un grupo y $H < G$, definimos dos relaciones binarias en G:

- La relación ${}_H\!\sim$ definida por:

$$y \;{}_H\!\sim x \Longleftrightarrow x^{-1}y \in H$$

- La relación $\sim_H$ definida por:

$$y \sim_H x \Longleftrightarrow yx^{-1} \in H$$

Proposición 2.11. *Sea G un grupo y $H < G$, se verifica que ${}_H\!\sim$ y $\sim_H$ son relaciones de equivalencia en G. Además, dado $x \in G$, se tiene que sus clases de equivalencia*[9] *son de la forma:*

$$_H[x] = \{xh \mid h \in H\}$$
$$[x]_H = \{hx \mid h \in H\}$$

Demostración. Comprobemos primero que ${}_H\!\sim$ y $\sim_H$ son relaciones de equivalencia:

[9]Que denotaremos por $_H[x]$ y por $[x]_H$ respectivamente.

- Propiedad reflexiva. Como H es un grupo, $1 \in H$, por lo que dado $x \in G$:

$$xx^{-1} = x^{-1}x = 1 \in H$$

De donde deducimos que $x \sim_H x$ y $x \;{}_H\!\sim x$, de forma respectiva.

- Propiedad simétrica. Sean $x, y \in G$:

  - Si $x \;{}_H\!\sim y$, entonces $y^{-1}x \in H$, pero por ser H un grupo, también tendremos:
  $$(y^{-1}x)^{-1} = x^{-1}y \in H$$
  De donde deducimos que $y \;{}_H\!\sim x$.
  - Si $x \sim_H y$, entonces $xy^{-1} \in H$, y por ser H un grupo:
  $$(xy^{-1})^{-1} = yx^{-1} \in H$$
  De donde deducimos que $y \sim_H x$.

- Propiedad transitiva. Sean $x, y, z \in G$:

  - Si $x \;{}_H\!\sim y$ y $y \;{}_H\!\sim z$, entonces: $y^{-1}x, z^{-1}y \in H$ y por ser H un grupo, deducimos que:
  $$(z^{-1}y)(y^{-1}x) = z^{-1}x \in H$$
  De donde $x \;{}_H\!\sim z$.
  - Si $x \sim_H y$ y $y \sim_H z$, entonces $xy^{-1}, yz^{-1} \in H$ y por ser H un grupo:
  $$(xy^{-1})(yz^{-1}) = xz^{-1} \in H$$
  De donde $x \sim_H z$.

Concluimos que ${}_H\!\sim$ y $\sim_H$ son relaciones de equivalencia en G. Falta comprobar las igualdades:

$$\begin{aligned} {}_H[x] &\overset{(1)}{=} \{xh \mid h \in H\} \\ [x]_H &\overset{(2)}{=} \{hx \mid h \in H\} \end{aligned}$$

1. Sean $x, y \in G$, tenemos que:
$$\begin{aligned} x \;{}_H\!\sim y &\Longleftrightarrow y^{-1}x \in H \Longleftrightarrow \exists h \in H \text{ con } y^{-1}x = h \Longleftrightarrow \exists h \in H \text{ con } y^{-1} = hx^{-1} \\ &\Longleftrightarrow \exists h \in H \text{ con } y = xh^{-1} \Longleftrightarrow \exists h' \in H \text{ con } y = xh' \end{aligned}$$
Concluimos que se cumple (1).

2. Sean $x, y \in G$:
$$\begin{aligned} x \sim_H y &\Longleftrightarrow xy^{-1} \in H \Longleftrightarrow \exists h \in H \text{ con } xy^{-1} = h \Longleftrightarrow \exists h \in H \text{ con } y = h^{-1}x \\ &\Longleftrightarrow \exists h' \in H \text{ con } y = hx \end{aligned}$$
Concluimos que también se cumple (2).

□

Definición 2.10. Sea G un grupo y $H < G$:

- Si consideramos la relación ${}_H\sim$, dado $x \in G$, definimos la clase lateral por la izquierda de G en H definida por x a la clase de equivalencia de x por la relación de equivalencia ${}_H\sim$, que denotamos por:
$$xH = \{xh \mid h \in H\}$$
De esta forma, tendremos que el conjunto cociente dado por la relación es de la forma:
$$G/\ {}_H\sim\ = \{xH \mid x \in G\}$$

- Si consideramos ahora la relación $\sim_H$, dado $x \in G$, definimos la clase lateral por la derecha de G en H definida por x a la clase de equivalencia de x por la relación de equivalencia $\sim_H$, denotada por:
$$Hx = \{hx \mid h \in H\}$$
Y consideraremos el conjunto cociente:
$$G/\sim_H = \{Hx \mid x \in G\}$$

Ejemplo. En $S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, si consideramos como H:
$$H = \langle (1\ 2) \rangle = \{1, (1\ 2)\}$$
Podemos calcular todas las clases laterales por la izquierda de G en H si consideramos la relación ${}_H\sim$:
$$\begin{aligned}
1H &= \{1 \cdot 1, 1(1\ 2)\} = \{1, (1\ 2)\} = H \\
(1\ 2)H &= \{(1\ 2)1, (1\ 2)(1\ 2)\} = \{(1\ 2), 1\} = H \\
(1\ 3)H &= \{(1\ 3)1, (1\ 3)(1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\} \\
(2\ 3)H &= \{(2\ 3)1, (2\ 3)(1\ 2)\} = \{(2\ 3), (1\ 3\ 2)\} \\
(1\ 2\ 3)H &= \{(1\ 2\ 3)1, (1\ 2\ 3)(1\ 2)\} = \{(1\ 2\ 3), (1\ 3)\} = (1\ 3)H \\
(1\ 3\ 2)H &= \{(1\ 3\ 2)1, (1\ 3\ 2)(1\ 2)\} = \{(1\ 3\ 2), (2\ 3)\} = (2\ 3)H
\end{aligned}$$
Por lo que el conjunto cociente $G/\ {}_H\sim$ vendrá dado por:
$$G/\ {}_H\sim\ = \{H, (1\ 3)H, (2\ 3)H\}$$
Si ahora calculamos todas las clases laterales por la derecha de G en H, considerando la relación $\sim_H$, entonces:
$$\begin{aligned}
H1 &= \{1 \cdot 1, (1\ 2)1\} = \{1, (1\ 2)\} = H \\
H(1\ 2) &= \{1(1\ 2), (1\ 2)(1\ 2)\} = \{(1\ 2), 1\} = H \\
H(1\ 3) &= \{1(1\ 3), (1\ 2)(1\ 3)\} = \{(1\ 3), (1\ 3\ 2)\} \\
H(2\ 3) &= \{1(2\ 3), (1\ 2)(2\ 3)\} = \{(2\ 3), (1\ 2\ 3)\} \\
H(1\ 2\ 3) &= \{1(1\ 2\ 3), (1\ 2)(1\ 2\ 3)\} = \{(1\ 2\ 3), (2\ 3)\} = H(2\ 3) \\
H(1\ 3\ 2) &= \{1(1\ 3\ 2), (1\ 2)(1\ 3\ 2)\} = \{(1\ 3\ 2), (1\ 3)\} = H(1\ 3)
\end{aligned}$$
Por lo que el conjunto cociente $G/\sim_H$ vendrá dado por:
$$G/\sim_H = \{H, H(1\ 3), H(2\ 3)\}$$

Proposición 2.12. *Sea G un grupo, $H < G$ y $x \in G$, entonces:*

i) $x \in xH$ *y* $x \in Hx$.

ii) *Los conjuntos H, xH y Hx son biyectivos.*

iii) *Los conjuntos cocientes $G/_H\!\sim$ y $G/\sim_H$ son biyectivos.*

Demostración. Veamos cada una de ellas:

i) Como H es un grupo, tendremos que $1 \in H$, por lo que:

$$x = x \cdot 1 \in xH \qquad x = 1 \cdot x \in Hx$$

ii) Sean $f : xH \longrightarrow H$, $g : H \longrightarrow Hx$ dadas por:

$$\begin{aligned} f(xh) &= h \qquad \forall xh \in xH \\ g(h) &= hx \qquad \forall h \in H \end{aligned}$$

Es fácil comprobar que f y g son biyectivas, por lo que xH es biyectivo con H y H es biyectivo con Hx. Basta considerar $g \circ f$ para obtener una biyección de xH con Hx.

iii) Sea $f : G/_H\!\sim \longrightarrow G/\sim_H$ dada por:

$$f(xH) = Hx^{-1} \qquad \forall xH \in G/_H\!\sim$$

En primer lugar, hemos de ver que f está bien definida. Para ello, sean $x, y \in G$ de forma que $xH = yH$, entonces $x\ _H\!\sim y$, luego $y^{-1}x \in H$, pero por ser H un grupo:

$$\left(y^{-1}x\right)^{-1} = x^{-1}y \in H \Longrightarrow x^{-1} \sim_H y^{-1}$$

Por lo que $Hx^{-1} = Hy^{-1}$, luego f está bien definida. Finalmente, es fácil ver que f es biyectiva. □

Definición 2.11 (Índice de un grupo en un subgrupo)**.** Sea G un grupo y $H < G$, en la Proposición 2.12, vimos que:

$$|G/_H\!\sim| = |G/\sim_H|$$

Los cardinales de estos conjuntos recibirán el nombre de <u>índice de G en H</u>, y los denotaremos por $[G : H]$.

Ejemplo. En los diagramas de Hasse de las Figuras 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9 y 2.10, los números que dibujábamos en las aristas de los diagramas de Hasse eran los índices de los grupos en los respectivos subgrupos marcados por la arista. Por ejemplo, en la Figura 2.9, observamos que $[S_3 : \langle(1\ 2)\rangle] = 3$, algo que comprobamos en el último ejemplo, donde tomábamos:

$$H = \langle(1\ 2)\rangle = \{1, (1\ 2)\}$$

En esta situación, teníamos que $[S_3 : H] = |G/\sim_H| = |G/_H\!\sim| = 3$.

Teorema 2.13 (de Lagrange). *Sea G un grupo finito y $H < G$, entonces:*

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

Observemos que a partir de esta igualdad deducimos que $|H|$ divide a $|G|$.

Demostración. Como ${}_H\sim$ es una relación de equivalencia, tenemos una partición de G a partir de las clases de equivalencia dadas por esta relación:

$$G = \bigcup_{x \in G} xH$$

Como G es finito, habrá un número finito de clases de equivalencia. Si elegimos un elemento en cada una de estas, tendremos un conjunto con cada uno de los representantes de las clases $\{x_1, x_2, \ldots, x_n\}$, con lo que:

$$|G| = |x_1H| + |x_2H| + \ldots + |x_nH| \overset{(*)}{=} n|H|$$

Donde en $(*)$ hemos usado la Proposición 2.12, ya que como xH es biyectivo con H para cualquier $x \in G$, concluimos que $|x_iH| = |x_1H|$ para todo $i \in \{1, \ldots, n\}$. Sin embargo, n es el número de clases de equivalencia distintas del conjunto cociente, es decir, $n = [G : H]$, con lo que:

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

□

Observación. Notemos que a partir del Teorema de Lagrange podemos deducir resultados ya vistos y demostrados, como por ejemplo, la Proposición 1.22, donde deducíamos el orden de los grupos $|\operatorname{SL}_n(\mathbb{F})|$, pero resulta que $[\operatorname{GL}_n(\mathbb{F}) : \operatorname{SL}_n(\mathbb{F})] = q-1$ si $|\mathbb{F}| = q$, por lo que:

$$|\operatorname{GL}_n(\mathbb{F})| = (q-1)|\operatorname{SL}_n(\mathbb{F})|$$

Corolario 2.13.1. *Sea G un grupo finito, el orden de cualquier elemento de G divide a $|G|$.*

Demostración. Sea $x \in G$, basta ver que $O(x) = |\langle x \rangle|$. Sin embargo, por la Proposición 1.9, ya vimos que por ser G un grupo finito, entonces $\exists n \in \mathbb{N} \setminus \{0\}$ de forma que $O(x) = n$. En esta misma Proposición vimos que entonces x tenía n potencias distintas, por lo que:

$$\langle x \rangle = \{1, x, x^2, \ldots, x^{n-1}\} \Longrightarrow |\langle x \rangle| = n$$

Basta aplicar el Teorema de Lagrange, puesto que $\langle x \rangle < G$. □

Corolario 2.13.2. *Sea G un grupo finito y $K < H < G$, entonces:*

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

Demostración. Por el Teorema de Lagrange, sabemos que:

$$\left.\begin{array}{r} |G| = [G : K]|K| \\ |G| = [G : H]|H| = [G : H][H : K]|K| \end{array}\right\} \Longrightarrow [G : K] = [G : H][H : K]$$

□

2.4. Propiedades de grupos cíclicos

Terminaremos este capítulo repasando varias propiedades de los grupos cíclicos que debemos conocer, no sin antes recordar la definición de un grupo cíclico. Decimos que un grupo G es cíclico si $\exists a \in G$ de forma que $G = \langle a \rangle$. En cuyo caso, todos los elementos de G serán potencias de a: si $x \in G$, existirá $n \in \mathbb{Z}$ de forma que $x = a^n$.

Antes de continuar, recordamos una propiedad de los grupos cíclicos: sea $G = \langle a \rangle$ un grupo cíclico, entonces:

$$|G| = O(a)$$

Proposición 2.14. *Si G es un grupo con $|G| = p$ primo, entonces G es cíclico.*

Demostración. Sea $a \in G$, $a \neq 1$ (como p es primo, $p \geqslant 2$), observamos que:

$$\{1\} \neq \langle a \rangle < G$$

Por el Teorema de Lagrange, $1 \neq |\langle a \rangle|$ divide a $|G|$, pero p es primo, por lo que $|\langle a \rangle| = p$ y ha de ser $\langle a \rangle = G$. □

Lema 2.15. *Sea G un grupo, $a \in G$, existe un homomorfismo de grupos*

$$\varphi_a : \mathbb{Z} \to G$$

De forma que $\varphi_a(1) = a$ y $Im(\varphi_a) = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$.

Demostración. Definimos φ_a como la aplicación:

$$\varphi_a(n) = a^n \qquad \forall n \in \mathbb{Z}$$

Es claro que $\varphi_a(1) = a$ y que $Im(\varphi_a) = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$. Falta ver que φ_a es un homomorfismo. Para ello:

$$\varphi_a(n + m) = a^{n+m} = a^n a^m = \varphi_a(n)\varphi_a(m) \qquad \forall n, m \in \mathbb{Z}$$

□

Teorema 2.16. *Sea G un grupo cíclico, entonces:*

- *Si G es infinito, $G \cong \mathbb{Z}$.*
- *Si $|G| = n$, $G \cong \mathbb{Z}_n$.*

Demostración. Como G es cíclico, existirá $a \in G$ de forma que $\langle a \rangle = G$. El Lema anterior nos da una aplicación $\varphi_a : \mathbb{Z} \to G$ sobreyectiva, veamos cómo conseguir la inyectividad:

- Si G es infinito, entonces ha de ser $O(a) = +\infty$, por lo que $\nexists n \in \mathbb{N} \setminus \{0\}$ de forma que $\varphi_a(n) = a^n = 1$, por lo que:

  $$\ker(\varphi_a) = \{0\} \Longrightarrow \varphi_a \text{ inyectiva}$$

  Concluimos que $G \cong \mathbb{Z}$.

- Si G es finito y tiene cardinal $n \in \mathbb{N} \setminus \{0\}$, entonces tendremos que $O(a) = n$, por lo que $\varphi_a(n) = a^n = 1$ y φ_a no será inyectiva por ser $\{0, n\} \subseteq \ker(\varphi_a)$. Sin embargo, podemos definir la aplicación $\psi_a : \mathbb{Z}_n \to G$ dada por $\psi_a(\overline{r}) = a^r$ para todo $\overline{r} \in \mathbb{Z}_n$:

  - ψ_a está bien definida, ya que si $\overline{r}, \overline{s} \in \mathbb{Z}_n$ de forma que $\overline{r} = \overline{s}$, entonces:
  $$r - s \in n\mathbb{Z} \Longrightarrow \exists t \in \mathbb{Z} \text{ con } a^{r-s} = a^{nt} = (a^n)^t = 1 \Longrightarrow a^r = a^s$$
  - ψ_a es un homomorfismo:
  $$\psi_a(\overline{r} + \overline{s}) = a^{r+s} = a^r a^s = \psi_a(\overline{r})\psi_a(\overline{s}) \qquad \forall \overline{r}, \overline{s} \in \mathbb{Z}_n$$
  - ψ_a es inyectiva, ya que si $\overline{r} \in \mathbb{Z}_n$ con $\psi_a(\overline{r}) = a^r = 1$, entonces $n \mid r$, luego $\overline{r} = \overline{0}$ y se tiene que:
  $$\ker(\psi_a) = \{\overline{0}\}$$
  - Como $\langle a \rangle = G$ y $|G| = n = O(a)$, está claro que ψ_a es sobreyectiva.

  Por todo esto, concluimos que ψ_a es un isomorfismo, luego $G \cong \mathbb{Z}_n$.

□

Proposición 2.17. *Sea $G = \langle a \rangle$ un grupo cíclico con $O(a) = n$, entonces para cada divisor m de n, existe un único subgrupo de G de orden m, el subgrupo cíclico $\left\langle a^{\frac{n}{m}} \right\rangle$. Además, estos son los únicos subgrupos de G.*

Demostración. Sea m un divisor de n, veamos que $\left\langle a^{\frac{n}{m}} \right\rangle$ es un grupo cíclico de orden m. Para ello, veamos que $O\left(a^{\frac{n}{m}}\right) = m$:

- En primer lugar, tenemos que:
$$\left(a^{\frac{n}{m}}\right)^m = a^n = 1$$
- Sea $t \in \mathbb{N} \setminus \{0\}$ de forma que:
$$\left(a^{\frac{n}{m}}\right)^t = 1 \Longrightarrow n \mid \frac{nt}{m}$$
  En cuyo caso, existe $r \in \mathbb{N}$ de forma que:
$$\frac{nt}{m} = rn \Longrightarrow t = rm \Longrightarrow m \mid t$$

Concluimos que $O(a^{\frac{n}{m}}) = m$. Ahora, si $H < G$, nos gustaría probar que si $|H| = m$, entonces:
$$m \in Div(n) \quad \text{y} \quad H = \left\langle a^{\frac{n}{m}} \right\rangle$$
En primer lugar, observemos que si $H < G$, por el Teorema de Lagrange tenemos que $m \mid n$. Para ver la igualdad, sea:
$$k = \text{mín}\{t \in \mathbb{N} \setminus \{0\} \mid a^t \in H\}$$
Veamos que $H = \langle a^k \rangle$:

$\supseteq$) Se tiene por la definición de k.

$\subseteq$) Sea $b \in H < G = \langle a \rangle$, entonces $\exists s \in \mathbb{N}$ de forma que $b = a^s$. Si dividimos s entre k, tenemos que $\exists q, r \in \mathbb{N}$ de forma que:

$$s = kq + r \qquad 0 \leqslant r < k$$

Y por ser $a^s, a^k \in H$, vemos que:

$$a^r = a^s a^{-kq} \in H$$

Por esto, concluimos que $r = 0$, ya que k era el menor natural no nulo que cumplía esta propiedad (y $r < k$), por lo que $s = kq$ y:

$$b = (a^k)^q \in \langle a^k \rangle$$

Falta finalmente ver que $k = {}^n/_m$. Para ello, como $a^n = 1 \in H$ por ser H un grupo, tenemos que $k \leqslant n$ y si dividimos n entre k, $\exists q, r \in \mathbb{N}$ de forma que:

$$n = qk + r \qquad 0 \leqslant r < k$$

De donde: $1 = a^n = a^{qk}a^r$, pero por ser $1 \in H$ y $a^{qk} \in H$, deducimos que $a^r \in H$ con $r < k$, luego ha de ser $r = 0$ (ya que si no entraría en contradicción con la definición de k), por lo que $k \mid n$. De aquí deducimos que:

$$m = |H| = O(a^k) \overset{(*)}{=} \frac{n}{k} \Longrightarrow k = \frac{n}{m}$$

Donde en $(*)$ hemos usado que $O(a^k) = \dfrac{n}{k}$, ya que:

- En primer lugar:
$$\left(a^k\right)^{\frac{n}{k}} = a^n = 1$$

- Si $t \in \mathbb{N}$ de forma que:
$$\left(a^k\right)^t = 1 = a^n$$

  Como $O(a) = n$, por la Proposición 1.8, tenemos que $n \mid kt$, luego existe s de forma que:
$$ns = kt \Longrightarrow \frac{n}{k}s = t$$

  Por lo que $\frac{n}{k} \mid t$.

Lo que nos dice que $O(a^k) = \dfrac{n}{k}$. □

Observación. De la Proposición anterior, deducimos que dado G un grupo cíclico con $|G| = n$, entonces la aplicación $\phi : Div(n) \to \Lambda_G$ con:

$$\Lambda_G = \{H \subseteq G \mid H < G\}$$

dada por:

$$\phi(m) = \left\langle a^{\frac{n}{m}} \right\rangle \qquad \forall m \in Div(n)$$

Es una biyección.

Ejemplo. A partir de esta última observación, es muy fácil calcular todos los subgrupos de cualquier grupo cíclico, ya que el problema se reduce a estudiar todos los divisores del orden del grupo. Ilustramos el procedimiento con el grupo cíclico de orden 12:

$$C_{12} = \langle x \mid x^{12} = 1 \rangle$$

Tenemos que:

$$Div(12) = \{1, 2, 3, 4, 6, 12\}$$

Y usando nuestra aplicación ϕ, podemos listar todos los subgrupos de C_{12}:

$$\begin{aligned}
1 &\overset{\phi}{\longmapsto} \left\langle x^{\frac{12}{1}} \right\rangle = \langle x^{12} \rangle = \langle 1 \rangle = \{1\} \\
2 &\longmapsto \left\langle x^{\frac{12}{2}} \right\rangle = \langle x^6 \rangle = \{1, x^6\} \\
3 &\longmapsto \left\langle x^{\frac{12}{3}} \right\rangle = \langle x^4 \rangle = \{1, x^4, x^8\} \\
4 &\longmapsto \left\langle x^{\frac{12}{4}} \right\rangle = \langle x^3 \rangle = \{1, x^3, x^6, x^9\} \\
6 &\longmapsto \left\langle x^{\frac{12}{6}} \right\rangle = \langle x^2 \rangle = \{1, x^2, x^4, x^6, x^8, x^{10}\} \\
12 &\longmapsto \left\langle x^{\frac{12}{12}} \right\rangle = \langle x \rangle = C_{12}
\end{aligned}$$

Por lo que su diagrama de Hasse será de la forma:

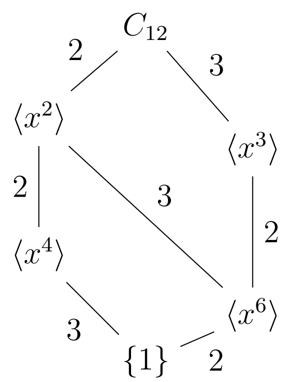


Figura 2.13: Diagrama de Hasse para los subgrupos de C_{12}.

Corolario 2.17.1. *Si tenemos un grupo cíclico de orden p^n con p primo, entonces todos sus subgrupos serán cíclicos y de orden p^r, con $0 \leqslant r \leqslant n$.*

Proposición 2.18. *Sea G un grupo, $a \in G$ con $O(a) = n$ y $k \in \mathbb{N} \setminus \{0\}$, entonces:*

$$\langle a^k \rangle = \langle a^d \rangle \qquad \text{siendo } d = \text{mcd}(n, k)$$

En cuyo caso, $O(a^k) = \dfrac{n}{d}$.

Demostración. Por doble inclusión:

$\subseteq$) Como $d \mid k$, tenemos que $k = dt$ para cierto t, luego $a^k = a^{dt} \in \langle a^d \rangle$.

$\supseteq$) Como $d = \text{mcd}(n, k)$, entonces la ecuación:

$$nX + kY = d$$

tiene solución[10], por lo que existen $u, v \in \mathbb{N}$ de forma que $nu + kv = d$, luego:

$$a^d = a^{nu}a^{kv} = \cancelto{1}{(a^n)^u} (a^k)^v \in \langle a^k \rangle$$

Para ver que $O(a^k) = {}^n/_d$, como $\langle a^k \rangle = \langle a^d \rangle$, tenemos que $O(a^k) = O(a^d)$ y como:

- Tenemos que:

$$(a^d)^{\frac{n}{d}} = a^n = 1$$

- Si $t \in \mathbb{N}$ de forma que:

$$(a^d)^t = 1 \Longrightarrow n \mid dt \Longrightarrow \frac{n}{d} \mid t$$

Concluimos que $O(a^k) = O(a^d) = {}^n/_d$. □

Ejemplo. Por ejemplo, ¿por qué en $\mathbb{Z}_{12}$ el subgrupo generado por el 8 coincide con el generado por el 4? Porque $4 = \text{mcd}(8, 12)$.

Corolario 2.18.1. *Sea G un grupo y $a \in G$ con $O(a) = n$, entonces:*

$$\langle a^p \rangle = \langle a^q \rangle \Longleftrightarrow \text{mcd}(n, p) = \text{mcd}(n, q)$$

Demostración. Veamos la doble implicación:

$\Longleftarrow$) Si $\text{mcd}(n, p) = d = \text{mcd}(n, q)$, entonces (por la Proposición anterior):

$$\langle a^p \rangle = \langle a^d \rangle = \langle a^q \rangle$$

$\Longrightarrow$) Si $\langle a^p \rangle = \langle a^q \rangle$, entonces (por la Proposición anterior):

$$\frac{n}{\text{mcd}(n, p)} = O(a^p) = O(a^q) = \frac{n}{\text{mcd}(n, q)} \Longrightarrow \text{mcd}(n, p) = \text{mcd}(n, q)$$

□

Corolario 2.18.2. *Sea $G = \langle a \rangle$ un grupo cíclico con $O(a) = n$, entonces:*

$$G = \langle a^k \rangle \Longleftrightarrow \text{mcd}(k, n) = 1$$

Es decir, el número de generadores de G es $\varphi(n)$, siendo φ la función de Euler:

$$\varphi(n) = |\{m \in \mathbb{N} \mid 1 \leqslant m \leqslant n \wedge \text{mcd}(n, m) = 1\}|$$

Demostración. Basta usar el Corolario anterior:

$$G = \langle a \rangle = \langle a^k \rangle \Longleftrightarrow 1 = \text{mcd}(n, 1) = \text{mcd}(n, k)$$

□

Ejemplo. En $\mathbb{Z}_{12}$:

$$\mathbb{Z}_{12} = \langle \overline{1} \rangle = \langle \overline{5} \rangle = \langle \overline{7} \rangle = \langle \overline{11} \rangle$$

[10]Se vió en Álgebra I, se trata de la Identidad de Bezout.

3. Grupos cocientes y Teoremas de isomorfía

Este tema se centrará en las relaciones de equivalencia $_H\sim$ y $\sim_H$ definidas en el capítulo anterior, donde ya vimos propiedades de estas relaciones (recordamos la Proposición 2.12), como que $G/\,_H\sim$ y $G/\sim_H$ eran biyectivos o el Teorema de Lagrange. Estaremos especialmente interesados en el caso en el que los conjuntos cocientes de estas dos relaciones de equivalencia coincidan, propiedad que nos dará los Teoremas de Isomorfía, que son el principal objeto de estudio de este tema.

3.1. Subgrupos normales

Definición 3.1 (Subgrupos normales)**.** Sea G un grupo y $H < G$, diremos que H es un subgrupo normal de G, denotado por $H \lhd G$, si las clases laterales de cada elemento coinciden, es decir, si:

$$xH = Hx \qquad \forall x \in G$$

En cuyo caso, tendremos que $G/\,_H\sim\ = G/\sim_H$, y notaremos a este conjunto como G/H, al que llamaremos conjunto de las clases laterales de H en G.

Definición 3.2 (Conjugado)**.** Sea G un grupo, $H \subseteq G$ y $x \in G$, definimos el conjugado de H por x como el conjunto:

$$xHx^{-1} = \{xhx^{-1} \mid h \in H\}$$

Proposición 3.1. *Sea G un grupo, $H < G$ y $x \in G$, entonces $xHx^{-1} < G$.*

Demostración. Para ello, sean $xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1}$, entonces:

$$xh_1x^{-1}(xh_2x^{-1})^{-1} = xh_1x^{-1}xh_2^{-1}x^{-1} = xh_1h_2^{-1}x^{-1} \in xHx^{-1}$$

Ya que como H es un subgrupo de G, entonces $h_1h_2^{-1} \in H$. □

Buscamos ahora formas cómodas de detectar cuándo un subgrupo de un grupo es normal o no, ya que es tedioso comprobar la igualdad $xH = Hx$ para todo elemento x del grupo que estemos considerando en cada caso.

Proposición 3.2 (Caracterización de subgrupos normales)**.**
Sea G un grupo y $H < G$, son equivalentes:

i) $H \lhd G$.

ii) $xhx^{-1} \in H \ \forall x \in G, \forall h \in H$.

iii) $xHx^{-1} \subseteq H \ \forall x \in G$.

iv) $xHx^{-1} = H \ \forall x \in G$.

Demostración. Veamos todas las implicaciones:

$i) \Longrightarrow ii)$ Sean $x \in G$ y $h \in H$, entonces $xh \in xH = Hx$ por ser $H \lhd G$, lo que nos dice que $\exists h' \in H$ de forma que $xh = h'x$ y multiplicando por x^{-1} a la derecha, llegamos a que:

$$xhx^{-1} = h' \in H$$

$ii) \Longleftrightarrow iii)$ Es claro.

$iii) \Longrightarrow iv)$ Sea $h \in H$ y dado $x \in G$, en particular tendremos que $x^{-1} \in G$, por lo que usando la hipótesis, tenemos que $x^{-1}hx \in x^{-1}Hx \subseteq H$, por lo que $x^{-1}hx \in H$ y tendremos que:

$$xx^{-1}hxx^{-1} = h \in xHx^{-1}$$

$iv) \Longrightarrow i)$ Fijado $x \in G$, veamos que $xH = Hx$:

$\subseteq)$ Si $xh \in xH$, entonces tendremos que:

$$xhx^{-1} \in xHx^{-1} = H$$

Con lo que existirá $h' \in H$ de forma que $xhx^{-1} = h'$. Si multilicamos por x a la derecha, obtenemos que:

$$xh = h'x \in Hx$$

$\supseteq)$ Para la otra inclusión, si $hx \in Hx$, tendremos que:

$$x^{-1}hx \in x^{-1}Hx = H$$

Por lo que existirá $h' \in H$ de forma que $x^{-1}hx = h'$. Si multiplicamos por x a la izquierda:

$$hx = xh' \in xH$$

□

Comprobar que $xhx^{-1} \in H$ para todo $x \in G$ y para todo $h \in H$ puede ser una labor tediosa, por lo que presentamos la siguiente Proposición, que puede resultar de utilidad a la hora de comprobar si un subgrupo H de un grupo G es normal o no.

Proposición 3.3. *Sea G un grupo, $H < G$ y $S \subseteq G$ de forma que $G = \langle S \rangle$, entonces:*

$$xhx^{-1} \in H \quad \forall x \in G, \forall h \in H \Longleftrightarrow shs^{-1} \in H \quad \forall s \in S \cup S^{-1}, \forall h \in H$$

Donde $S^{-1} = \{x \in G \mid x^{-1} \in S\}$. Es decir, basta comprobar la condición con los generadores de G y con los inversos de los generadores de G.

Demostración. Veamos las dos implicaciones:

$\Longrightarrow$) En particular, tenemos que $x \in S \cup S^{-1} \subseteq G$.

$\Longleftarrow$) Sea $x \in G = \langle S \rangle$, entonces existirán $s_1, \ldots, s_n \in S$ y $\gamma_1, \ldots, \gamma_n \in \{\pm 1\}$ de forma que:

$$x = s_1^{\gamma_1} \ldots s_n^{\gamma_n}$$

Por inducción sobre n:

- Si $n = 1$: Entonces $x = s^\gamma$ con $s \in S$ y $\gamma \in \{\pm 1\}$. Distinguimos casos:
  - Si $\gamma = 1$, entonces:
  $$xhx^{-1} = shs^{-1} \in H \qquad \forall h \in H$$
  - Si $\gamma = -1$, entonces:
  $$xhx^{-1} = s^{-1}hs \in H \qquad \forall h \in H$$
- Supuesto para $m < n$, veámoslo para n:
$$xhx^{-1} = s_1^{\gamma_1} s_2^{\gamma_2} \ldots s_n^{\gamma_n} h s_n^{-\gamma_n} \ldots s_2^{-\gamma_2} s_1^{-\gamma_1}$$
Si cogemos $y = s_2^{\gamma_2} \ldots s_n^{\gamma_n}$, por hipótesis de inducción tendremos que:
$$yhy^{-1} = s_2^{\gamma_2} \ldots s_n^{\gamma_n} h s_n^{-\gamma_n} \ldots s_2^{-\gamma_2} \in H$$
Por lo que:
$$xhx^{-1} = s_1^{\gamma_1} yhy^{-1} s_1^{-\gamma_1} \in H$$

□

Ejemplo. Hemos caracterizado ya a los grupos normales, pero veamos ejemplos de ellos:

1. Dado un grupo G, los dos subgrupos impropios de G siempre son subgrupos normales del mismo:
   - Para el caso $H = \{e\}$:
   $$xex^{-1} = xx^{-1} = e \in \{e\} \qquad \forall x \in G$$
   Y por la Proposición anterior, tenemos que $\{e\} \lhd G$.
   - Para el caso $H = G$:
   $$xhx^{-1} \in G \qquad \forall x \in G, \forall h \in G$$
   Y por la misma razón, también tenemos que $G \lhd G$.
2. En un grupo abeliano G, todos sus subgrupos son normales (sea $H < G$):
$$xH = \{xh \mid h \in H\} = \{hx \mid h \in H\} = Hx \qquad \forall x \in G$$

3. Todo subgrupo de índice 2 es normal, es decir, si $H < G$ con $[G : H] = 2$, entonces $H \lhd G$.

   Para verlo, si tomamos $x \in G \setminus H$, como $[G : H] = 2$, tenemos que:

$$H \cup xH = G = H \cup Hx$$

   En ambos casos, como son particiones disjuntas, tenemos que $xH = Hx$ para todo $x \in G \setminus H$ (y si $x \in H$, entonces $xH = H = Hx$), con lo que $H \lhd G$.

4. En S_3, si consideramos $H = \langle(1\ 2)\rangle$, H no es un subgrupo normal de S_3, como se vio en el correspondiente ejemplo del tema anterior, y podemos volverlo a comprobar con la caracterización, ya que $(2\ 3) \in S_3$ y:

$$(2\ 3)(1\ 2)(2\ 3)^{-1} = (1\ 3) \notin H$$

   Igual les pasa a los subgrupos $\langle(2\,3)\rangle$ y $\langle(1\,3)\rangle$. Sea ahora $A_3 = \{1, (1\,2\,3), (1\,3\,2)\}$, como $[S_3 : A_3] = 2$, tenemos que $A_3 \lhd S_3$:

$$S_3/A_3 = \{A_3, A_3(1\ 2)\} = \{A_3, (1\ 2)A_3\}$$

5. La relación de "ser un subgrupo normal de" no es transitiva, es decir, si G es un grupo con $K < H < G$, $K \lhd H$ y $H \lhd G$, entonces no necesariamente se tiene que $K \lhd G$. La situación es la descrita en la Figura 3.1

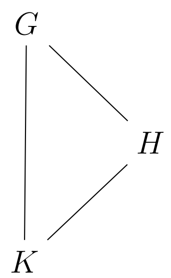
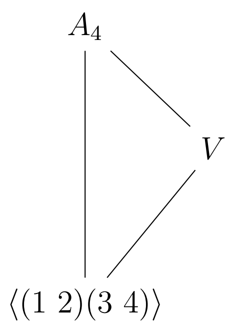


   Figura 3.1: Situación descrita.

   Por ejemplo, en A_4 consideramos el grupo de Klein V y $\langle(1\ 2)(3\ 4)\rangle$. Vamos a ver que $\langle(1\ 2)(3\ 4)\rangle \lhd V$ y que $V \lhd A_4$ pero no se cumple que $\langle(1\ 2)(3\ 4)\rangle \lhd A_4$:



   - En primer lugar, $\langle(1\ 2)(3\ 4)\rangle \lhd V$, por ser $[V : \langle(1\ 2)(3\ 4)\rangle] = 2$.

- Veamos ahora que $V \lhd A_4$. Para ello, consideramos:

$$A_4 = \langle (1\ 2\ 3), (1\ 2\ 4) \rangle$$

  Por la Proposición 3.3, basta comprobar la caracterización para todos los generadores de $A_4 = \langle (1\ 2\ 3), (1\ 2\ 4) \rangle$:

$$\begin{aligned}
&(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} \in V \\
&(1\ 2\ 3)(1\ 3)(2\ 4)(1\ 2\ 3)^{-1} \in V \\
&(1\ 2\ 3)(1\ 4)(2\ 3)(1\ 2\ 3)^{-1} \in V \\
&(1\ 2\ 3)1(1\ 2\ 3)^{-1} \in V \\
&(1\ 2\ 4)(1\ 2)(3\ 4)(1\ 2\ 4)^{-1} \in V \\
&(1\ 2\ 4)(1\ 3)(2\ 4)(1\ 2\ 4)^{-1} \in V \\
&(1\ 2\ 4)(1\ 4)(2\ 3)(1\ 2\ 4)^{-1} \in V \\
&(1\ 2\ 4)1(1\ 2\ 4)^{-1} \in V
\end{aligned}$$

- Veremos ahora que no se tiene que $\langle (1\ 2)(3\ 4) \rangle \lhd A_4$, ya que:

$$(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} = (1\ 4)(2\ 3) \notin \langle (1\ 2)(3\ 4) \rangle$$

Hemos visto ya que la relación $\lhd$ no es en general transitiva. Sin embargo, de ella podemos deducir ciertas relaciones, como se pone de manifiesto en este Corolario:

Corolario 3.3.1. *Como corolario de la Proposición 3.2, si G es un grupo de forma que $A \subseteq B \subseteq G$ con $A \lhd G$ y $B < G$, entonces $A \lhd B$.*

Demostración. Por la Proposición 3.2, tendremos que $xax^{-1} \in A$ para todo $x \in G$ y $a \in A$. Sea $b \in B$, como en particular $b \in G$, también se cumplirá:

$$bab^{-1} \in A \qquad \forall b \in B, a \in A$$

Concluimos que $A \lhd B$. $\square$

Definición 3.3 (Centro)**.** Sea G un grupo, definimos el centro de G como el conjunto de los elementos de G que conmutan con todos los demás, es decir, el conjunto:

$$Z(G) = \{a \in G \mid ax = xa, \forall x \in G\}$$

Podemos entender $Z(G)$ como "la parte abeliana del grupo" G.

Proposición 3.4. *Sea G un grupo, se verifica:*

i) $Z(G) < G$.

ii) $Z(G) \lhd G$.

iii) *G es abeliano si y solo si $Z(G) = G$.*

Demostración. Demostramos las propiedades:

i) Sean $a, b \in Z(G)$ y dado $x \in G$, entonces:

$$(ab^{-1})x = a(b^{-1}x) = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} = a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})$$

Por lo que $ab^{-1} \in Z(G)$, lo que nos dice que $Z(G)$ es un subgrupo de G.

ii) Sea $x \in G$, entonces:

$$xZ(G) = \{xz \mid z \in Z(G)\} = \{zx \mid z \in Z(G)\} = Z(G)x$$

iii) Tenemos que:

$$G \text{ abeliano} \Longleftrightarrow xy = yx \quad \forall y \in G, \forall x \in G \Longleftrightarrow y \in Z(G) \quad \forall y \in G \Longleftrightarrow Z(G) = G$$

□

Ejemplo. Ejemplos interesantes:

- Veamos que $Z(S_n) = 1$ cuando $n \geqslant 3$. Para ello, supongamos que $n \geqslant 3$ y consideremos $1 \neq \sigma \in S_n$, con lo que existirán $i, j \in \{1, \ldots, n\}$ con $i \neq j$ de forma que $\sigma(i) = j$.

  En dicho caso, $\exists k \in \{1, \ldots, n\} \setminus \{i, j\}$ $(n \geqslant 3)$. Si consideramos $\tau = (j\ k)$:

  $$\left.\begin{array}{r} \sigma\tau(i) = \sigma(i) = j \\ \tau\sigma(i) = \tau(j) = k \end{array}\right\} \Longrightarrow \sigma\tau \neq \tau\sigma$$

  Por tanto, $\sigma \notin Z(S_n)$, para todo $\sigma \in S_n \setminus \{1\}$.

- Veamos que que $Z(A_n) = 1$ cuando $n \geqslant 4$. Para $n \geqslant 4$, $\exists i, j \in \{1, \ldots, n\}$ con $i \neq j$ de forma que $\sigma(i) = j$, con lo que podemos encontrar $k, l \in \{1, \ldots, n\}$, distintos entre sí y distintos de i y j. Consideramos:

  $$\tau = (j\ k\ l) \in A_4$$

  Y tenemos de la misma forma que:

  $$\left.\begin{array}{r} \sigma\tau(i) = j \\ \tau\sigma(i) = k \end{array}\right\} \Longrightarrow Z(A_n) = \{1\}$$

Proposición 3.5. *Sea G un grupo, $H < G$, entonces, equivalen:*

i) $H \lhd G$.

ii) $\forall x, y \in G$ *con* $xy \in H$*, entonces* $yx \in H$

Demostración. Veamos las dos implicaciones:

i) $\Longrightarrow$ *ii)* Sean $x, y \in G$ con $xy \in H$, entonces $\exists h \in H$ de forma que $xy = h$, de donde $y = x^{-1}h \in x^{-1}H = Hx^{-1}$, por lo que $\exists h' \in H$ con $y = h'x^{-1}$ y multiplicando a la derecha por x, llegamos a que $yx = h' \in H$.

ii) $\Longrightarrow$ *i)* Sean $x \in G$ y $h \in H$, tenemos que:

$$h = x^{-1}(xh) \in H$$

De donde deducimos por hipótesis que $(xh)x^{-1} \in H$, lo que nos dice que $H \lhd G$. □

3.2. Grupo cociente

Mostraremos ahora la propiedad que más nos interesa de los grupos normales: dotan al conjunto cociente de estructura de grupo.

Teorema 3.6. *Sea G un grupo y $H \lhd G$, entonces en el conjunto G/H podemos definir una operación binaria $G/H \times G/H \longrightarrow G/H$ que dota a G/H de estructura de grupo, de modo que la proyección canónica $p : G \to G/H$ sea un homomorfismo de grupos. De esta forma, llamaremos a G/H grupo cociente.*

Demostración. Definimos la operación binaria $\cdot : G/H \times G/H \longrightarrow G/H$ dada por:

$$xH \cdot yH = xyH \qquad \forall xH, yH \in G/H$$

A esta operación la denotaremos a partir de ahora por yuxtaposición.

- En primer lugar, comprobemos que está bien definida, es decir, si $xH = x'H$ y $yH = y'H$, entonces $xyH = x'y'H$. Para ello:

$$\left.\begin{array}{l} xH = x'H \\ yH = y'H \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} \exists h_1, h_2 \in H \\ x' = xh_1 \\ y' = yh_2 \end{array}\right.$$

  Vemos ahora que dado $h \in H$:

  $\supseteq$)

  $$x'y'h = xh_1yh_2h \overset{(*)}{=} xyh_1'h_2h \in xyH$$

  Donde en $(*)$ hemos usado que $H \lhd G$, por lo que $Hy = yH$ y podemos encontrar un h_1' de forma que $h_1y = yh_1'$. Tenemos $x'y'H \subseteq xyH$.

  $\subseteq$)

  $$xyh = x'h_1^{-1}y'h_2^{-1}h \overset{(*)}{=} x'y'h_1''h_2^{-1}h \in x'y'H$$

  Donde en $(*)$ hemos usado una idea similar a la anterior, lo que nos da la otra inclusión.

- Que la operación es asociativa es claro, ya que la operación de G era asociativa.
- El elemento neutro de la operación es $1H = H$.
- Fijado un elemento $xH \in G/H$, tendremos que $(xH)^{-1} = x^{-1}H$.

Concluimos que G/H es un grupo.

Ahora, consideramos la proyección canónica $p : G \to G/H$, que viene definida por $p(x) = xH$ para todo $x \in G$. Gracias a la definición de la operación de G/H, tenemos que:

$$p(xy) = xyH = xHyH = p(x)p(y) \qquad \forall x, y \in G$$

Lo que demuestra que p es un homomorfismo de grupos. □

Notemos la importancia de considerar en el teorema anterior H como subgrupo normal de G, ya que es lo que nos ha permitido comprobar que la operación de G/H estaba bien definida. Como propiedades a destacar del grupo cociente G/H:

- Sabemos por el capítulo anterior que el orden del grupo G/H es (si G es finito):
$$|G/H| = [G : H] = \frac{|G|}{|H|}$$
- Además, si $p : G \to G/H$ es la proyección al cociente, tenemos que:
$$\ker(p) = \{x \in G \mid p(x) = H\} = \{x \in G \mid xH = H\} = \{x \in H\} = H$$

Ejemplo. Algunas consecuencias de que G/H sea un grupo:

1. En S_3, si consideramos $A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\} \lhd S_3$, tenemos que:
$$S_3/A_3 = \{A_3, (1\ 2)A_3\}$$
Que por ser un grupo de orden 2, ya sabemos por el capítulo anterior que ha de ser $S_3/A_3 \cong \mathbb{Z}_2$.

2. Si consideramos $H < \mathbb{Z}$, entonces $H \lhd \mathbb{Z}$, ya que $\mathbb{Z}$ es abeliano. Además, sabemos que $\exists n \in \mathbb{Z}$ de forma que $H = n\mathbb{Z}$. De esta forma, tendremos que:
$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$
Por lo que el grupo cociente de $\mathbb{Z}$ bajo cualquier subgrupo normal suyo ya era conocido para nosotros, puesto que todos ellos son de la forma $\mathbb{Z}_n$, para cierto $n \in \mathbb{N}$.

3. Veamos otra vez que A_4 no tiene subgrupos de orden 6. Si $H < A_4$ con $|H| = 6$, entonces:
$$[A_4 : H] = \frac{A_4}{H} = 2$$
Por tanto, $H \lhd A_4$. De esta forma, $A_4/H \cong \mathbb{Z}_2$, por ser el único grupo de orden 2. Si el cociente es isomorfo con $\mathbb{Z}_2$ y consideramos $xH \in A_4/H$, entonces:
$$(xH)^2 = x^2H = H \qquad \forall x \in A_4$$
Por tanto, los cuadrados de los 8 $3-$ciclos de A_4 pertenecerían a H, de donde $|H| \geqslant 8$, <u>contradicción</u>.

Proposición 3.7. *Sea G un grupo y $H < G$, entonces: $H \lhd G$ si y solo si existe un homomorfismo de grupos $f : G \to G'$ de forma que* $\ker(f) = H$.

Demostración. Veamos las dos implicaciones:

$\Longrightarrow)$ Si $H \lhd G$, entonces la proyección canónica $p : G \to G/H$ es un homomorfismo de grupos de forma que $\ker(p) = H$, gracias al Teorema 3.6.

$\Longleftarrow)$ Supongamos ahora que existe un homomorfismo $f : G \to G'$ de grupos de forma que $\ker(f) = H$, sabemos ya que $H < G$ por ser $H = f^*(\{1\})$. Sean $x \in G$ y $h \in H$, tenemos que:
$$f(xhx^{-1}) = f(x)f(h)(f(x))^{-1} = f(x)(f(x))^{-1} = 1$$
De donde deducimos que $xhx^{-1} \in \ker(f) = H$, lo que nos dice que $H \lhd G$. □

Observación. De esta forma, dado un homomorfismo de grupos $f : G \to G'$, tendremos siempre que $\ker(f) \lhd G$, ya que por ser $\{1\} < G'$ un subgrupo, tendremos que $\ker(f) = f^*(\{1\}) < G$ y por la Proposición 3.7, automáticamente tenemos que $\ker(f) \lhd G$.

Teorema 3.8 (Propiedad universal del grupo cociente)**.** *Sea G un grupo, $H \lhd G$, $p : G \to G/H$ la proyección canónica al cociente, entonces para cualquier homomorfismo $f : G \to G'$ tal que $H \subseteq \ker(f)$, existe un único homomorfismo de grupos $\varphi : G/H \to G'$ de forma que $\varphi \circ p = f$.*

Más aún, tendremos que:

$$f \text{ sobreyectiva} \Longleftrightarrow \varphi \text{ sobreyectiva}$$
$$H = \ker(f) \Longleftrightarrow \varphi \text{ inyectiva}$$

La situación descrita podemos observarla en la Figura 3.2. Este resultado nos dice que el diagrama conmuta.

Demostración. Definimos $\varphi : G/H \to G'$ de la forma más natural posible:

$$\varphi(xH) = f(x) \qquad \forall xH \in G/H$$

- En primer lugar, veamos que está bien definida. Para ello, sean $x, y \in G$ de forma que $xH = yH$, entonces $y^{-1}x \in H \subseteq \ker(f)$, de donde:

$$1 = f(y^{-1}x) = (f(y))^{-1}f(x) \Longrightarrow f(x) = f(y)$$

- Veamos ahora que φ es un homomorfismo:

$$\varphi(xHyH) = \varphi(xyH) = f(xy) = f(x)f(y) = \varphi(xH)\varphi(yH) \qquad \forall x, y \in G$$

- Veamos que $\varphi \circ p = f$:

$$(\varphi \circ p)(x) = \varphi(p(x)) = \varphi(xH) = f(x) \qquad \forall x \in G$$

- Para la unicidad, supongamos que existe otra función $\psi : G/H \to G'$ de forma que $\psi \circ p = f$. En cuyo caso:

$$\psi(xH) = \psi(p(x)) = (\psi \circ p)(x) = f(x) = \varphi(xH) \qquad \forall xH \in G/H$$

  Por lo que $\psi = \varphi$.

Veamos la relación entre la sobreyectividad de f y φ:

$$f \text{ sobreyectiva} \Longleftrightarrow \varphi \text{ sobreyectiva}$$

$\Longleftarrow$) Como $f = \varphi \circ p$ y la composición de aplicaciones sobreyectivas es sobreyectiva, concluimos que f será sobreyectiva.

$\Longrightarrow$) Supongamos que f es sobreyectiva y sea $y \in G'$, por lo que $\exists x \in G$ de forma que $f(x) = y$, pero:

$$y = f(x) = \varphi(p(x)) = \varphi(xH)$$

Concluimos que φ es sobreyectiva.

Veamos ahora la relación de inyectividad:

$$H = \ker(f) \Longleftrightarrow \varphi \text{ inyectiva}$$

$\Longrightarrow$) Si $H = \ker(f)$ y $\varphi(xH) = 1$, entonces:

$$1 = \varphi(xH) = f(x) \Longrightarrow x \in \ker(f) = H$$

Con lo que $xH = H$, lo que nos dice que φ es inyectiva[1] ($\ker(\varphi) = \{H\}$).

$\Longleftarrow$) Vamos a ver que $\ker(f) \subseteq H$, ya que conocemos $H \subseteq \ker(f)$ por hipótesis. Para ello, sea $x \in \ker(f)$, entonces:

$$1 = f(x) = \varphi(p(x)) = \varphi(xH) \Longrightarrow xH \in \ker(\varphi)$$

Pero como φ es inyectiva, tenemos que $\ker(\varphi) = \{H\}$, con lo que $xH = H$, de donde $x \in H$.

□

La idea que subyace y que debemos entender de la propiedad universal del grupo cociente es la siguiente: G/H es la mejor forma de "colapsar H al elemento neutro sin perder las propiedades de grupo". Como ya vimos en el Teorema 3.6, en el que definimos al grupo cociente y donde vimos que la proyección canónica era un homomorfismo, resulta que en el grupo cociente, H es el elemento neutro de la operación, por lo que hemos conseguido colapsar H al elemento neutro.

Ahora, la propiedad universal del grupo cociente nos dice que si tenemos cualquier homomorfismo de grupos que "mata a H" (es decir, lo envía al núcleo del homomorfismo), entonces necesariamente ese homomorfismo ha de pasar por G/H, es decir, que existirá un único homomorfismo $\varphi : G/H \to G'$ que haga que el diagrama siguiente conmute. Cualquier homomorfismo que "mate a H" podremos factorizarlo pasando por el grupo cociente, luego este grupo ha de ser el que mejor colapsa a H.

$$\begin{tikzcd}
G \arrow[r, "p"] \arrow[dr, "f"'] & G/H \arrow[d, dotted, "\varphi"] \\
& G'
\end{tikzcd}$$

Figura 3.2: Situación del Teorema 3.8.

[1] Ya que H es el elemento neutro en G/H.

3.3. Teoremas de isomorfía

Teorema 3.9 (Primer Teorema de Isomorfía para grupos)**.** *Sea $f : G \to G'$ un homomorfismo de grupos, entonces existe un isomorfismo de grupos de forma que*

$$G/\ker(f) \cong Imf$$

Y vendrá definido por $x\ker(f) \longmapsto f(x)$.

Demostración. En primer lugar, por un resultado de la Proposición 3.7, tenemos que $\ker(f) \lhd G$. De esta forma, podemos considerar la proyección canónica al cociente $p : G \to G/\ker(f)$. Consideramos ahora la restriccion del codominio de f a su imagen, lo que nos da un epimorfismo. Por la propiedad universal del grupo cociente, tenemos que existe un único homomorfismo $\varphi : G/\ker(f) \to Im(f)$ que hace conmutar el siguiente diagrama:

$$\begin{tikzcd}
G \arrow[r, "p"] \arrow[dr, "f"'] & G/\ker(f) \arrow[d, dotted, "\varphi"] \\
 & Im(f)
\end{tikzcd}$$

Finalmente, aplicando el Teorema 3.8:

- φ es sobreyectiva debido a que la restricción de f en codominio a su imagen es sobreyectiva.
- φ es inyectiva ya que el grupo normal que consideramos para hacer el cociente es $\ker(f)$. □

Ejemplo. Como consecuencia del primer teorema de isomorfía: consideramos $\mathbb{K}$, un cuerpo finito con $|\mathbb{K}| = q$ elementos. La aplicación $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$ es un homomorfismo de grupos y tenemos que:

$$\ker(\det) = \mathrm{SL}_n(\mathbb{K})$$

Con lo que $\mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K}) \cong Im(\det) = \mathbb{K}^*$. Usémoslo para calcular $|\mathrm{SL}_n(\mathbb{K})|$, ya que la isomorfía recién encontrada nos dice que:

$$|\mathbb{K}^*| = |\mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K})| = \frac{|\mathrm{GL}_n(\mathbb{K})|}{|\mathrm{SL}_n(\mathbb{K})|} \Longrightarrow |\mathrm{SL}_n(\mathbb{K})| = \frac{|\mathrm{GL}_n(\mathbb{K})|}{|\mathbb{K}^*|} = \frac{|\mathrm{GL}_n(\mathbb{K})|}{q-1}$$

Teorema 3.10 (Segundo Teorema de Isomorfía para grupos)**.** *Sea G un grupo, $H, K < G$ de forma que $K \lhd G$, entonces:*

$$H \cap K \lhd H$$

Y existe un isomorfismo de grupos de forma que

$$H/H \cap K \cong HK/K$$

La situación descrita podemos observarla en la Figura 7.2.

Demostración. En primer lugar, justifiquemos de forma breve que el grupo de la derecha del isomorfismo tiene todo el sentido, es decir, que HK es efectivamente un grupo (no lo sabemos a priori) y que $K \lhd HK$. Para ello:

- Para ver que HK es un grupo (un subgrupo de G), como vimos en la Proposición 2.10, hemos de ver que $HK = KH$. Para ello, como $K \lhd G$, tenemos que:
$$xK = Kx \qquad \forall x \in G$$
En particular, para $x \in H$, por lo que $HK = KH$.

- Como tenemos que $K < HK < G$ con $K \lhd G$, tendremos que $K \lhd HK$.

Consideramos ahora el homomorfismo resultante de componer la inclusión de H en G con la proyección al cociente G/K:

$$\begin{aligned} H &\xrightarrow{i} G \xrightarrow{p} G/K \\ x &\longmapsto x \longmapsto xK \end{aligned}$$

Si calculamos ahora la imagen y el núcleo de este homomorfismo:

$$\begin{aligned} Im(p \circ i) &= \{(p \circ i)(h) \mid h \in H\} = \{p(h) \mid h \in H\} = \{hK \mid h \in H\} \overset{(*)}{=} HK/K \\ \ker(p \circ i) &= \{h \in H \mid hK = (p \circ i)(h) = K\} = \{h \in H \mid h \in K\} = H \cap K \end{aligned}$$

Como $H \cap K = \ker(p \circ i)$, tenemos por la Proposición 3.7 que $H \cap K \lhd H$. Si aplicamos el Primer Teorema de Isomorfía al homomorfismo $p \circ i$, llegamos a que:

$$\frac{H}{H \cap K} = \frac{H}{\ker(p \circ i)} \cong Im(p \circ i) = HK/K$$

La igualdad $(*)$ anterior puede parecer rara, pero es muy natural, veamos que:

$$\{hK \mid h \in H\} = HK/K$$

$\subseteq$) Dado $h \in H$, en particular tendremos que $h = h \cdot 1 \in HK$, con lo que $hK \in HK/K$.

$\supseteq$) Sea $hkK \in HK/K$ para ciertos $h \in H$, $k \in K$, por la definición del producto en el grupo cociente tenemos:

$$hkK = (hK)(kK) = (hK)K = hK \in \{hK \mid h \in H\}$$

□

El Segundo Teorema de Isomorfía para grupos puede recordarse fácilmente observando la siguiente figura, donde pensamos en que $HK/K \cong H/H \cap K$ bajo las hipótesis del Teorema, que podemos recordar observando las diagonales del paralelogramo:

$$\begin{tikzcd}
 & G \arrow[d, dash] \arrow[ddr, dash, "\rhd"] & \\
 & HK \arrow[dl, dash] \arrow[dr, dash, "\rhd"'] & \\
H \arrow[dr, dash, "\rhd"'] & & K \arrow[dl, dash] \\
 & H \cap K &
\end{tikzcd}$$

Figura 3.3: Situación del Teorema 3.10.

Ejemplo. Sea $H < S_n$ un subgrupo conteniendo una permutación impar, entonces $[H : H \cap A_n] = 2$. Es decir, H tiene el mismo número de permutaciones pares que de impares.

Para verlo, sabemos que $[S_n : A_n] = 2$, luego $A_n \lhd S_n$ y además, como H tiene una permutación impar, tenemos que $H \nsubseteq A_n$, por lo que tenemos:

$$HA_n = S_n$$

Que se puede deducir observando el retículo de subgrupos de S_n. Por el Segundo Teorema de Isomorfía, tenemos que:

$$H/H \cap A_n \cong S_n/A_n \cong \mathbb{Z}_2$$

Teorema 3.11 (Tercer Teorema de Isomorfía para grupos, o del doble cociente)**.** *Sea G un grupo, $N \lhd G$, entonces existe una biyección entre los subgrupos de G que contienen a N y los subgrupos de G/N, dada por $H \longmapsto H/N$.*

Además, $H \lhd G \Longleftrightarrow H/N \lhd G/N$. En este caso:

$$\frac{G/N}{H/N} \cong G/H$$

Demostración. Si consideramos la proyección al cociente $p : G \to G/N$ dada por $p(x) = xN$ para todo $x \in G$, consideramos las aplicaciones imagen directa e imagen inversa por p, dadas por:

$$\begin{gathered}
p_* : \mathcal{P}(G) \to \mathcal{P}(G/N) \\
p^* : \mathcal{P}(G/N) \to \mathcal{P}(G) \\
p_*(H) = \{p(h) \mid h \in H\} \subseteq G/N \\
p^*(J) = \{x \in G \mid p(x) \in J\} \subseteq G
\end{gathered}$$

Que podemos restringirlas en dominio y codominio a los conjuntos:

$$\begin{aligned}
\mathcal{A} &= \{H < G \mid N \subseteq H\} \\
\mathcal{B} &= \{J < G/N\}
\end{aligned}$$

Obteniendo aplicaciones (que nombramos igual ya que nos olvidamos de las otras):

$$p_* : \mathcal{A} \to \mathcal{B}$$
$$p^* : \mathcal{B} \to \mathcal{A}$$

Veamos que estas aplicaciones están bien definidas (es decir, que podemos poner $\mathcal{B}$ como codominio de p_* y $\mathcal{A}$ como codominio de p^*):

- Para p_*, hemos de observar primero que si cogemos $H \in \mathcal{A}$, entonces tendremos por el Corolario 3.3.1 que $N \lhd H$. En segundo lugar, ya vimos en la Proposición 2.3 que si $H < G$ entonces $p_*(H) < G/N$, por lo que la aplicación p_* está bien definida. Vemos lo que pasa cuando la aplicamos a un elemento de $\mathcal{A}$:
$$p_*(H) = \{p(h) \mid h \in H\} = \{hN \mid h \in H\} = H/N < G/N$$
- Para p^*, vimos también en la Proposición 2.3 que si $J < G/N$ (es decir, $J \in \mathcal{B}$), entonces $p^*(J) < G$. Veamos que $N \subseteq p^*(J)$. Para ello, vemos que:
$$p(n) = nN = N \in J \qquad \forall n \in N$$
Donde $N \in J$ por ser N el elemento neutro para el grupo G/N y ser $J < G/N$. En conclusión, $n \in p^*(J)$ $\forall n \in N$, y concluimos que p^* está bien definida.

Veamos ahora qué sucede con la composición de las aplicaciones:

- Por una parte, dado $J \in \mathcal{B}$:
$$(p_* \circ p^*)(J) = p_*(\{x \in G \mid p(x) \in J\}) \overset{(*)}{=} J$$
Donde en $(*)$ hemos aplicado que p es sobreyectiva, por lo que si tenemos $yN \in J$, existirá un $x \in G$ de forma que $p(x) = yN$, luego todos los valores de J se alcanzan.
- Dado $H \in \mathcal{A}$, veamos si $H = (p^* \circ p_*)(H)$:

  $\subseteq$) Sea $h \in H$, tenemos que:
$$\{h\} \subseteq p^*(\{p(h)\}) \subseteq p^*(p_*(\{h\})) \subseteq p^*(p_*(H))$$
  $\supseteq$) Sea $x \in p^*(p_*(H))$, entonces:
$$xN = p(x) \in p_*(H) = H/N = \{hN \mid h \in H\}$$
  Por lo que $x \in H$.

Concluimos que $(p_*)^{-1} = p^*$, por lo que p_* es biyectiva y $\mathcal{A}$ es biyectivo con $\mathcal{B}$.

Veamos ahora que:
$$H \lhd G \iff H/N \lhd G/N$$

$\Longrightarrow$) Sean $xN \in G/N$, $hN \in H/N$:

$$xNhN(xN)^{-1} = xNhNx^{-1}N \overset{(*)}{=} xhx^{-1}N \overset{(**)}{\in} H/N$$

Donde en $(*)$ hemos aplicado la definición del producto en el cociente y en $(**)$ hemos aplicado que $H \lhd G$, con lo que $xhx^{-1} \in H$.

$\Longleftarrow$) Ahora, sean $x \in G$ y $h \in H$:

$$xhx^{-1}N = xNhN(xN)^{-1} \in H/N$$

De donde concluimos que $xhx^{-1} \in H$, con lo que $H \lhd G$.

Finalmente, en este caso veamos que $\frac{G/N}{H/N} \cong G/H$. Para ello, consideramos las proyecciones $p_N : G \to G/N$ y $p_H : G \to G/H$. Como $N \subseteq H = \ker(p_H)$, sabemos por la Propiedad Universal del grupo cociente (Teorema 3.8) que existe un único homomorfismo $\varphi : G/N \to G/H$ que hace conmutar el siguiente diagrama:

$$\begin{tikzcd}
G \arrow[r, "p_N"] \arrow[dr, "p_H"'] & G/N \arrow[d, dotted, "\varphi"] \\
& G/H
\end{tikzcd}$$

Es decir, φ cumplirá que:

$$\varphi \circ p_N = p_H$$

Si aplicamos ahora el Primer Teorema de Isomorfía sobre φ:

$$\frac{G/N}{\ker(\varphi)} \cong Im(\varphi)$$

Y basta observar que:

- Por ser p_H sobreyectiva (es una proyección), φ también será sobreyectiva, por lo que $Im(\varphi) = G/H$.
- Veamos que $\ker(\varphi) = H/N$:

  $\subseteq$) Sea $xN \in \ker(\varphi)$, entonces:

  $$H = \varphi(xN) = \varphi(p_N(x)) = p_H(x) = xH \Longrightarrow x \in H$$

  $\supseteq$) Sea $hN \in H/N$, entonces:

  $$\varphi(hN) = \varphi(p_N(h)) = p_H(h) = hH = H$$

  Por lo que $hN \in \ker(\varphi)$.

En definitiva, hemos probado que:

$$\frac{G/N}{H/N} \cong G/H$$

□

Ejemplo. Recordando el retículo de subgrupos de D_4:

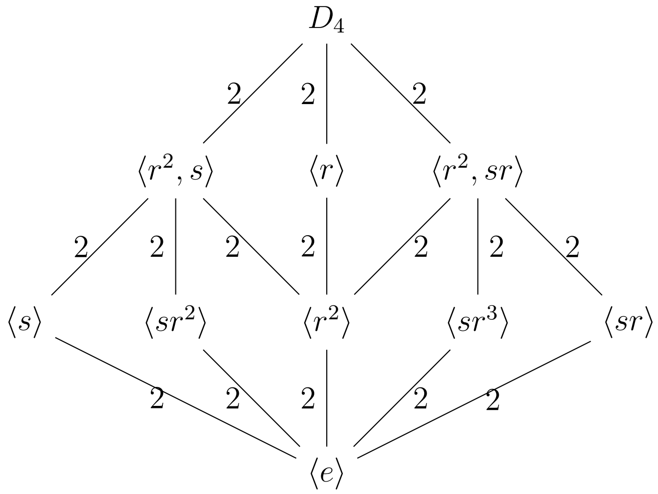
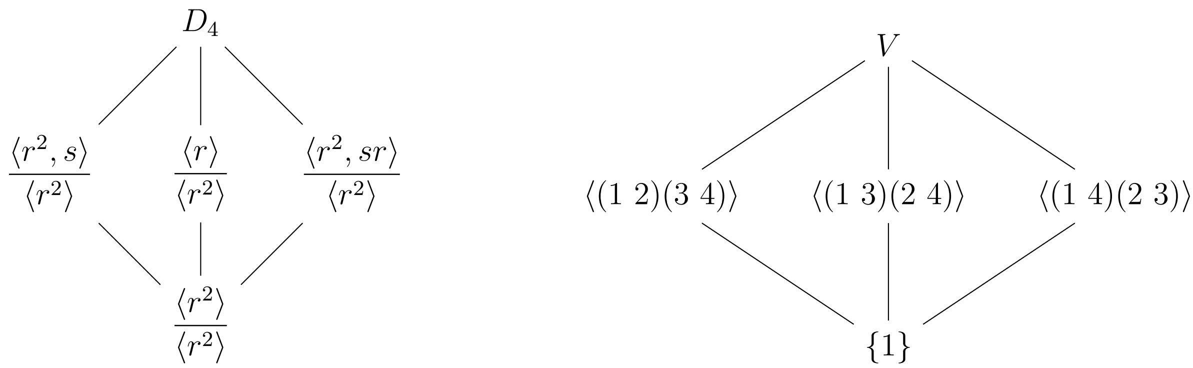


Figura 3.4: Diagrama de Hasse para los subgrupos de D_4.

Si consideramos los 5 grupos del centro del diagrama y los dividimos entre $\langle r^2\rangle$, llegamos a que el conjunto que contiene a estos es isomorfo al grupo de Klein:



Cuarto Teorema de Isomorfía

Antes de ver el Cuarto Teorema de Isomorfía, hemos de ver dos Lemas previos que nos ayudarán en su demostración:

Lema 3.12 (Ley modular o regla de Dedekind)**.** *Sea G un grupo y $A, B, C < G$ con $A < C$, entonces:*

$$A(B \cap C) = AB \cap C$$

Demostración. Por doble implicación:

$\subseteq$) Sea $z \in A(B \cap C)$, entonces existen $a \in A$ y $x \in B \cap C$ de forma que $z = ax$, con lo que $ax \in AB$ y $ax \in AC = C$ por ser $A < C$, de donde deducimos que $z = ax \in AB \cap C$.

$\supseteq$) Sea $z \in AB \cap C$, entonces:

- Por una parte, como $z \in AB$, tenemos que $\exists a \in A$ y $b \in B$ de forma que $z = ab$.
- Además, como $z \in C$, tenemos que $z = ab \in C$

Por ser $A < C$, tenemos que $a \in C$, por lo que $a^{-1} \in C$, de donde:

$$b = a^{-1}z \in C$$

Como además teniamos $b \in B$, llegamos a que $z = ab \in A(B \cap C)$.

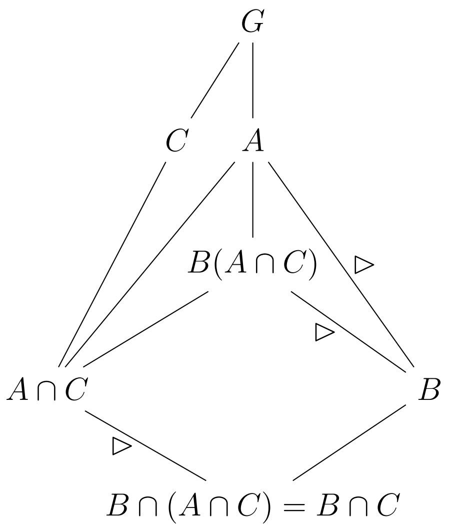
$\square$

Observación. La hipótesis $A < C$ no es necesaria, basta con tener $A \subseteq C$.

Lema 3.13. *Sea G un grupo y $A, B, C < G$ con $B \lhd A$, entonces:*

i) $B \cap C \lhd A \cap C$ *y* ${}^{A\cap C}/_{B\cap C} \cong {}^{B(A\cap C)}/_{B}$.

ii) *Si además $C \lhd G$, entonces: $BC \lhd AC$ y* ${}^{AC}/_{BC} \cong {}^{A}/_{B(A\cap C)}$



Demostración. Veamos los dos apartados:

i) Aplicando el Segundo Teorema de Isomorfía sobre el diagrama (observamos el paralelogramo), tenemos el resultado de forma directa:

$${}^{A\cap C}/_{B\cap C} \cong {}^{B(A\cap C)}/_{B}$$

ii) Ahora, si $C \lhd G$ (los elementos de G conmutan con los de C), tendremos que $BC = CB$ y $AC = CA$, por lo que $BC, AC < G$. Además, como $B < A$, también tendremos que $BC < AC$. Veamos que esta última relación es normal. Para ello, sean $bc \in BC$, $ax \in AC$:

$$axbc(ax)^{-1} = axbcx^{-1}a^{-1} = axa^{-1}aba^{-1}acx^{-1}a^{-1} = (axa^{-1})(aba^{-1})(acx^{-1}a^{-1})$$

Para ver dónde está este último elemento:

- Como $x \in C$ y $C \lhd G$, $axa^{-1} \in C$.
- Como $b \in B$ y $B \lhd A$, $aba^{-1} \in B$.
- Como $c, x \in C$, tendremos $cx^{-1} \in C$ y por ser $C \lhd G$, $acx^{-1}a^{-1} \in C$.

En definitiva:

$$axbc(ax)^{-1} \in CBC = BCC = BC$$

De donde deducimos que $BC \lhd AC$. Ahora, si tenemos en mente el siguiente diagrama, podemos aplicar el Segundo Teorema de Isomorfía, ya que tenemos $A, BC < AC$ y $BC \lhd AC$.

$$\begin{tikzcd}
 & AC \arrow[dl, dash] \arrow[dr, dash] & \\
A \arrow[dr, dash] & & BC \arrow[dl, dash] \\
 & BC \cap A = B(A \cap C) &
\end{tikzcd}$$

El Segundo Teorema de Isomorfía nos dice que $B(C \cap A) \lhd A$, y que:

$${}^{A}/_{B(A\cap C)} \cong {}^{AC}/_{BC}$$

$\square$

Observación. Sin embargo, el Lema anterior se podría hacer también suponiendo solo que $A, B \subseteq G$ para A y B, solo es necesario suponer que $C < G$.

A continuación, veremos el Cuarto Teorema de Isomorfía, o Teorema de Zassenhaus, para el cual conviene pensar en la Figura 3.6 (aunque en esta figura el retículo de subgrupos está al revés de a lo que estamos acostumbrados: arriba los conjuntos de menor tamaño y debajo los conjuntos mayores).

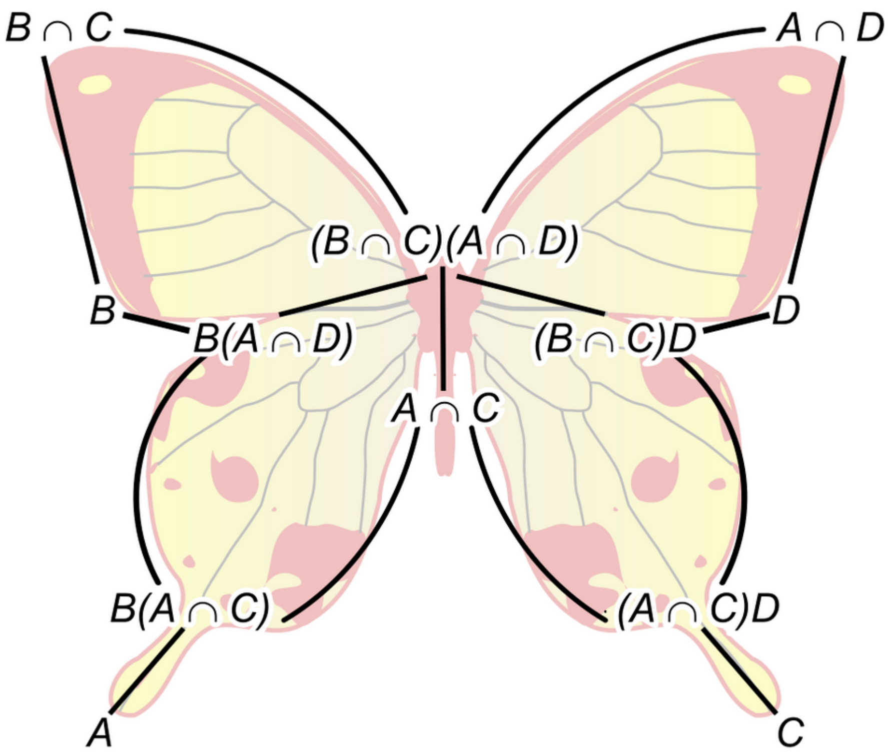


Figura 3.6: Situación del Teorema 3.14

Teorema 3.14 (Cuarto Teorema de Isomorfía para grupos)**.** *Sea G un grupo y $A_1, C_1, A_2, C_2 < G$ y $C_1 \lhd A_1$, $C_2 \lhd A_2$, entonces:*

i) $(A_1 \cap C_2)C_1 \lhd (A_1 \cap A_2)C_1$.

ii) $(A_2 \cap C_1)C_2 \lhd (A_1 \cap A_2)C_2$.

iii) ${}^{(A_1\cap A_2)C_1}/{}_{(A_1\cap C_2)C_1} \cong {}^{A_1\cap A_2}/{}_{(A_1\cap C_2)(A_2\cap C_1)} \cong {}^{(A_1\cap A_2)C_2}/{}_{(A_2\cap C_1)C_2}$

Demostración. Veamos cada apartado:

i) En primer lugar[2], como $C_1 \lhd A_1$, entonces los elementos de C_1 conmutarán con los de A_1, luego:

$$(A_1 \cap C_2)C_1 = C_1(A_1 \cap C_2)$$
$$(A_1 \cap A_2)C_1 = C_1(A_1 \cap A_2)$$

Por lo que ambos serán subgrupos de G. Además, como $C_2 < A_2$, tenemos ya que:

$$(A_1 \cap C_2)C_1 < (A_1 \cap A_2)C_1$$

Para ver la normalidad, sean $x \in (A_1 \cap A_2)C_1, y \in (A_1 \cap C_2)C_1$, entonces existirán elementos $a \in A_1 \cap A_2, b \in A_1 \cap C_2, c, c' \in C_1$ de forma que:

$$x = ac \qquad y = bc'$$

[2]Esta demostración se hizo en clase de otra forma usando resultados previos. Si alguien hace esta demostración de forma más sencilla que se ponga en contacto con nosotros.

Si calculamos:

$$xyx^{-1} = acbc'c^{-1}a^{-1} = (aca^{-1})(aba^{-1})(ac'a^{-1})(ac^{-1}a^{-1})$$

Veamos dónde está este elemento:

- Como $c \in C_1$, $a \in A_1 \cap A_2$ y $C_1 \lhd A_1$, $aca^{-1} \in C_1$.
- Como $b \in A_1 \cap C_2 \subseteq C_2$ y $a \in A_1 \cap A_2 \subseteq A_2$ con $C_2 \lhd A_2$, entonces $aba^{-1} \in A_1 \cap C_2$.
- Como $c', c \in C_1$, $a \in A_1 \cap A_2$ y $C_1 \lhd A_1$, $ac'a^{-1}, ac^{-1}a^{-1} \in C_1$.

En definitva:

$$xyx^{-1} \in C_1(A_1 \cap C_2)C_1C_1 = (A_1 \cap C_2)C_1C_1C_1 = (A_1 \cap C_2)C_1$$

Y concluimos que $(A_1 \cap C_2)C_1 \lhd (A_1 \cap A_2)C_1$.

ii) Es análogo, cambiando los papeles de C_1 y C_2.

iii) Para el primer isomorfismo, si tomamos:

$$\begin{aligned} G_1 &= A_1 \\ A &= A_1 \cap A_2 \\ B &= A_1 \cap C_2 \\ C &= C_1 \end{aligned}$$

Nos encontramos en las Hipótesis del Lema 3.13, ya que $A, B, C < G_1$ y $B \lhd A$, por ser $C_2 \lhd A_2$. Como además $C \lhd G_1$ por hipótesis, concluimos que:

$$AC/BC \cong A/B(A\cap C)$$

Que en nuestro caso significa:

$$(A_1\cap A_2)C_1/(A_1\cap C_2)C_1 \cong A_1\cap A_2/(A_1\cap C_2)(A_1\cap A_2\cap C_1) = A_1\cap A_2/(A_1\cap C_2)(A_2\cap C_1)$$

Para el segundo, hemos de tomar:

$$\begin{aligned} G_2 &= A_2 \\ A &= A_1 \cap A_2 \\ B &= A_1 \cap C_2 \\ C &= C_2 \end{aligned}$$

□

3.4. Producto directo

En un ejemplo del Capítulo 1 vimos que dados dos grupos H y G podíamos definir de forma sencilla una operación en $H \times G$ en función de las operaciones de H y G, que nos dotaba a $H \times G$ de estructura de grupo. A este grupo lo llamábamos grupo directo de G y H, grupo que volveremos a definir a partir de ahora y en el que nos centraremos durante esta sección.

Definición 3.4 (Producto directo)**.** Sean H y G dos grupos, definimos en el producto cartesiano $H \times G$ la operación

$$\begin{array}{rrcl} \cdot: & (H \times G) \times (H \times G) & \longrightarrow & H \times G \\ & (h,k)(h',k') & \longmapsto & (hh',kk') \end{array}$$

Se verifica que $H \times G$ junto con esta operación es un grupo:

- Es claro que la operación es asociativa, por ser las respectivas operaciones de H y G asociativas.
- El elemento $(1,1) \in H \times G$ es el elemento neutro para la operación.
- Dado un elemento $(h,k) \in H \times G$, tenemos que:
$$(h,k)(h^{-1},k^{-1}) = (hh^{-1},kk^{-1}) = (1,1)$$

Este grupo que hemos definido en $H \times G$ recibirá el nombre de producto directo de H y G.

Algunos autores llaman al producto directo que hemos definido producto directo externo, para diferenciarlo del producto directo interno, que luego definiremos. Sin embargo, nosotros lo llamaremos simplemente producto directo.

Proposición 3.15. *Si H y K son dos grupos finitos, entonces:*

i) $|H \times K| = |H||K|$.

ii) $O(h,k) = \text{mcm}(O(h),O(k)) \ \forall (h,k) \in H \times K$.

Demostración. Veamos las dos propiedades:

i) Se vió en Álgebra I.

ii) Como H y K son finitos, también lo será $H \times K$ y como ya vimos en la Proposición 1.9, los órdenes de los elementos son finitos, por lo que el enunciado tiene todo el sentido.

Llamando $m(h,k) = \text{mcm}(O(h),O(k))$, en primer lugar vemos que:
$$(h,k)^{m(h,k)} = \left(h^{m(h,k)},k^{m(h,k)}\right) = (1,1)$$
Donde en la primera igualdad hemos usado la definición del producto directo de H y K y en la segunda hemos usado que $O(h) \mid m(h,k)$ y que $O(k) \mid m(h,k)$.

Ahora, sea $t \in \mathbb{N} \setminus \{0\}$ de forma que $(h,k)^t = (1,1)$, tenemos entonces que $h^t = 1$ y $k^t = 1$, con lo que $O(h) \mid t$ y $O(k) \mid t$, de donde deducimos que (por definición de mínimo común múltiplo) $m(h,k) \mid t$. □

Definición 3.5 (Proyecciones e inyecciones)**.** Dados H y G dos grupos, en el producto directo de H y G podemos definir 4 aplicaciones que nos serán útiles:

1. La proyección en la primera coordenada, $p_1 : H \times G \to H$, dada por:
$$p_1(h, k) = h \qquad \forall (h, k) \in H \times G$$
2. La proyección en la segunda coordenada, $p_2 : H \times G \to G$, dada por:
$$p_2(h, k) = k \qquad \forall (h, k) \in H \times G$$
3. La inyección en la primera coordenada, $i_1 : H \to H \times G$, dada por:
$$i_1(h) = (h, 1) \qquad \forall h \in H$$
4. La inyección en la segunda coordenada, $i_2 : G \to H \times G$, dada por:
$$i_2(k) = (1, k) \qquad \forall k \in G$$

Aplicaciones que podremos recordar fácilmente observando la Figura 3.7.

$$\begin{tikzcd} H \arrow[r, shift left, "i_1"] & H \times G \arrow[l, shift left, "p_1"] \arrow[r, shift right, "p_2"'] & G \arrow[l, shift right, "i_2"'] \end{tikzcd}$$

Figura 3.7: Diagrama de las proyecciones y las inyecciones.

Proposición 3.16. *Se verifica que:*

1. *Las proyecciones y las inyecciones son homomorfismos de grupos.*
2. $p_1 i_1 = id = p_2 i_2$ *y las aplicaciones* $p_1 i_2$ *y* $p_2 i_1$ *son la aplicación constantemente igual a* 1*.*
3. *Las proyecciones son sobreyectivas y las inyecciones son inyectivas.*
4. *Si tomamos* $H' = \{(h, 1) \mid h \in H\}$*, tenemos que:*
$$Im(i_1) = \ker(p_2) = H' \lhd H \times G$$
Además, $H' \cong H$*.*
5. *De la misma forma, si tomamos* $G' = \{(1, k) \mid k \in G\}$*, tenemos:*
$$Im(i_2) = \ker(p_1) = G' \lhd H \times G$$
Además, $G' \cong G$*.*
6. $H' \cap G' = \{1\}$*.*
7. $xy = yx$ *para todo* $x \in H'$*,* $y \in G'$*.*

Demostración. Veamos cada apartado:

1. Tenemos 4 casos:

   - Para p_1, vemos que:

     $$p_1((h,k)(h',k')) = p_1(hh',kk') = hh' = p_1(h,k)p_1(h',k') \qquad \forall (h,k),(h',k') \in H \times G$$

     Y la demostración para p_2 es análoga.

   - Para i_1, vemos que:

     $$i_1(hh') = (hh',1) = (h,1)(h',1) = i_1(h)i_1(h') \qquad \forall h,h' \in H$$

     Y la demostración es análoga para i_2.

2. Si los índices coinciden, tenemos que:

   $$\begin{array}{ll} (p_1 \circ i_1)(h) = p_1(i_1(h)) = p_1(h,1) = h & \forall h \in H \\ (p_2 \circ i_2)(k) = p_2(i_2(k)) = p_2(1,k) = k & \forall k \in G \end{array}$$

   Y si no coinciden, tenemos:

   $$\begin{array}{ll} (p_1 \circ i_2)(k) = p_1(i_2(k)) = p_1(1,k) = 1 & \forall k \in G \\ (p_2 \circ i_1)(h) = p_2(i_1(h)) = p_2(h,1) = 1 & \forall h \in H \end{array}$$

3. Para comprobar que p_1 es sobreyectiva, vemos que dada $h \in H$, tenemos que $p_1(h,1) = h$ y para ver que p_2 es sobreyectiva, dado $k \in G$, tenemos que $p_2(1,k) = k$.

   Para ver la inyectividad de i_1, si dados $h,h' \in H$ de forma que:

   $$(h,1) = i_1(h) = i_1(h') = (h',1)$$

   De donde deducimos que $h = h'$, por lo que i_1 es inyectiva. La demostración para i_2 es análoga.

4. En primer lugar:

   $$\begin{aligned} Im(i_1) &= \{i_1(h) \mid h \in H\} = \{(h,1) \mid h \in H\} \\ \ker(p_2) &= \{(h,k) \in H \times G \mid p_2(h,k) = 1\} = \{(h,k) \in H \times G \mid k = 1\} \\ &= \{(h,1) \in H \times G\} = \{(h,1) \mid h \in H\} \end{aligned}$$

   Además, la igualdad $H' = \ker(p_2)$ nos dice que $H' \lhd H \times G$, gracias a la Proposición 3.7.

   Para ver que $H' \cong H$, en el apartado 1 vimos que i_1 era un homomorfismo y aplicando 3 tenemos que, de hecho, es un monomorfismo. Como $Im(i_1) = H'$, la restricción al codominio de i_1 a su imagen nos da un isomorfismo entre H y H', con lo que $H' \cong H$.

5. Vemos que:

$$\begin{aligned} Im(i_2) &= \{i_2(k) \mid k \in G\} = \{(1,k) \mid k \in G\} \\ \ker(p_1) &= \{(h,k) \in H \times G \mid p_1(h,k) = 1\} = \{(h,k) \in H \times G \mid h = 1\} \\ &= \{(1,k) \in H \times G\} = \{(1,k) \mid k \in G\} \end{aligned}$$

   La igualdad $G' = \ker(p_1)$ nos vuelve a decir que $G' \lhd H \times G$.

   Y finalmente, para ver que $G' \cong G$, tenemos que i_2 es un monomorfismo, por lo que la restricción en codominio a su imagen, $Im(i_2) = G'$ nos da un isomorfismo entre G y G'.

6. La igualdad se tiene porque:

$$H' \cap G' = \{(h,k) \in H \times G \mid k = 1 \ \wedge \ h = 1\} = \{(1,1)\} = \{1\}$$

7. Sean $x \in H'$ y $y \in G'$, entonces $\exists h \in H$ y $k \in G$ de forma que $x = (h,1)$ y $y = (1,k)$, de donde:

$$xy = (h,1)(1,k) = (h,k) = (1,k)(h,1) = yx$$

□

Proposición 3.17. *Sean A y B dos grupos, se cumple que:*

$$\frac{A \times B}{\{1\} \times B} \cong A \qquad \frac{A \times B}{A \times \{1\}} \cong B$$

Demostración. En la Proposición superior ya vimos que $\{1\}\times B, A\times\{1\}\lhd A\times B$, por lo que los cocientes del enunciado tienen todo el sentido. Para el primer isomorfismo, si consideramos la proyección en primera coordenada, $p_1 : A \times B \to A$ dada por:

$$p_1(x,y) = x \qquad \forall (x,y) \in A \times B$$

Y la proyección al cociente $p : A \times B \to (A \times B)/(\{1\} \times B)$ dada por:

$$p(z) = z(\{1\} \times B) \qquad \forall z \in A \times B$$

Observando el siguiente diagrama:

$$\begin{tikzcd} A \times B \arrow[r, "p"] \arrow[dr, "p_1"'] & \dfrac{A \times B}{\{1\} \times B} \arrow[d, dashed, "\varphi"] \\ & A \end{tikzcd}$$

Por la Propiedad Universal del grupo cociente, obtenemos que existe un homomorfismo $\varphi : (A \times B)/(\{1\} \times B) \to A$.

- p_1 es sobreyectiva, por ser una proyección, por lo que φ será sobreyectiva.
- Como $\ker(p_1) = \{1\} \times B$, tenemos que φ es inyectiva.

En definitiva, obtenemos el isomorfismo buscado. Para el segundo, basta considerar la proyección al cociente $(A \times B)/(A \times \{1\})$ y la aplicación p_2. □

3.4.1. Caracterización del grupo directo por isomorfismo

Teorema 3.18 (Propiedad universal del producto directo)**.** *Sea G un grupo y sean $f_1 : G \to H$, $f_2 : G \to K$ dos homomorfismos de grupos, entonces existe un único homomorfismo de grupos $f : G \to H \times K$ tal que $p_1 f = f_1$ y $p_2 f = f_2$.*
Es decir, existe un único homomorfismo f que hace conmutar el siguiente diagrama:

$$\begin{tikzcd}
 & G \arrow[dl, "f_1"'] \arrow[d, dashed, "f"] \arrow[dr, "f_2"] & \\
H & H \times K \arrow[l, "p_1"] \arrow[r, "p_2"'] & K
\end{tikzcd}$$

Demostración. Definimos $f : G \to H \times K$ dada por:

$$f(x) = (f_1(x), f_2(x)) \qquad \forall x \in G$$

- Vemos las dos igualdades:

$$\begin{aligned}
(p_1 \circ f)(x) &= p_1(f(x)) = p_1(f_1(x), f_2(x)) = f_1(x) \qquad \forall x \in G \\
(p_2 \circ f)(x) &= p_2(f(x)) = p_2(f_1(x), f_2(x)) = f_2(x) \qquad \forall x \in G
\end{aligned}$$

- Para ver que f es un homomorfismo:

$$\begin{aligned}
f(xy) = (f_1(xy), f_2(xy)) &= (f_1(x)f_1(y), f_2(x)f_2(y)) \\
&= (f_1(x), f_2(x))(f_1(y), f_2(y)) = f(x)f(y) \qquad \forall x, y \in G
\end{aligned}$$

- Sea $g : G \to H \times K$ un homomorfismo de grupos de forma que $p_1 g = f_1$ y $p_2 g = f_2$, entonces:

$$g(x) = (p_1(g(x)), p_2(g(x))) = (f_1(x), f_2(x)) = f(x) \qquad \forall x \in G$$

  Por lo que $g = f$.

□

El producto directo es único salvo isomorfismos. Es decir, si hay otro grupo que verifica la propiedad universal de grupo directo, este debe ser isomorfo al grupo directo.

Teorema 3.19. *Sea L un grupo y sean $l_1 : L \to H$, $l_2 : L \to K$ dos homomorfismos de grupos de forma que L cumple la propiedad universal del producto directo para estos homomorfismos, es decir, que si G es un grupo, entonces para cada par de homomorfismos $f_1 : G \to H$ y $f_2 : G \to K$ puede encontrarse un único homomorfismo $f : G \to L$ de forma que $l_1 f = f_1$ y $l_2 f = f_2$; entonces, tendremos que:*

$$L \cong H \times K$$

La situación es la descrita en el siguiente diagrama:

$$\begin{tikzcd}
& L \arrow[dl, "l_1"'] \arrow[dr, "l_2"] & \\
H & & K \\
& G \arrow[ul, "f_1"] \arrow[ur, "f_2"'] \arrow[uu, dashed, "f"] &
\end{tikzcd}$$

Demostración. En primer lugar, como $l_1 : L \to H$ y $l_2 : L \to K$ son dos homomorfismos, verifican las hipótesis de la propiedad universal del producto directo, por lo que existe un único homomorfismo $l : L \to H \times K$ de forma que:

$$p_1 l = l_1$$
$$p_2 l = l_2$$

$$\begin{tikzcd}
& L \arrow[dl, "l_1"'] \arrow[d, dashed, "l"] \arrow[dr, "l_2"] & \\
H & H \times K \arrow[l, "p_1"] \arrow[r, "p_2"'] & K
\end{tikzcd}$$

Ahora, si tomamos $G = H \times K$ y consideramos $p_1 : H \times K \to H$ y $p_2 : H \times K \to K$, tenemos dos homomorfismos que por hipótesis pueden factorizarse pasando por L, es decir, existe un único homomorfismo $p : H \times K \to L$ de forma que:

$$l_1 p = p_1$$
$$l_2 p = p_2$$

$$\begin{tikzcd}
& L \arrow[dl, bend right, "l_1"'] \arrow[d, dashed, bend left, "l"] \arrow[dr, bend left, "l_2"] & \\
H & H \times K \arrow[l, "p_1"] \arrow[r, "p_2"'] \arrow[u, dashed, bend left, "p"] & K
\end{tikzcd}$$

Para terminar la demostración, basta ver que p y l son inversos el uno del otro. Para ello, observamos que:

$$l_1 = p_1 l = l_1 p l \Longrightarrow pl = id_L$$
$$p_1 = l_1 p = p_1 l p \Longrightarrow lp = id_{H\times K}$$

Concluimos que $p^{-1} = l$, con lo que p y l son isomorfismos y $L \cong H \times K$. $\square$

Notemos que tanto en la propiedad universal del producto directo como en su unicidad por isomorfismo solo hemos usado las proyecciones p_1 y p_2. Si consideramos resultados análogos para las inyecciones i_1 y i_2, estos seguirán siendo ciertos, teniendo que añadir una hipótesis extra:

Teorema 3.20 (Propiedad universal del producto directo 2)**.** *Sea G un grupo y $f_1 : H \to G$, $f_2 : K \to G$ dos homomorfismos de grupos verificando que:*

$$f_1(h)f_2(k) = f_2(k)f_1(h) \qquad \forall h \in H, k \in K$$

Entonces, existe un único homomorfismo de grupos $f : H \times K \to G$ tal que $fi_1 = f_1$, $fi_2 = f_2$.

$$\begin{tikzcd}
 & G & \\
H \arrow[ur, "f_1"] \arrow[r, "i_1"'] & H \times K \arrow[u, dashed, "f"'] & K \arrow[ul, "f_2"'] \arrow[l, "i_2"]
\end{tikzcd}$$

Demostración. Definimos $f : H \times K \to G$ dada por:

$$f(h,k) = f_1(h)f_2(k) \qquad \forall (h,k) \in H \times K$$

- Vemos que verifica las dos igualdades:

$$\begin{aligned}
(f \circ i_1)(h) &= f(i_1(h)) = f(h,1) = f_1(h)f_2(1) = f_1(h) \qquad \forall h \in H \\
(f \circ i_2)(k) &= f(i_2(k)) = f(1,k) = f_1(1)f_2(k) = f_2(k) \qquad \forall k \in K
\end{aligned}$$

- Vemos que f es un homomorfismo, ya que dados $(h,k),(h',k') \in H \times K$:

$$\begin{aligned}
f((h,k)(h',k')) = f(hh',kk') = f_1(hh')f_2(kk') &= f_1(h)f_1(h')f_2(k)f_2(k') \\
&= f_1(h)f_2(k)f_1(h')f_2(k') = f(h,k)f(h',k')
\end{aligned}$$

- Sea $g : H \times K \to G$ otro homomorfismo de grupos de forma que $gi_1 = f_1$ y $gi_2 = f_2$, entonces dado $(h,k) \in H \times K$:

$$g(h,k) = g((h,1)(1,k)) = g(h,1)g(1,k) = g(i_1(h))g(i_2(k)) = f_1(h)f_2(k) = f(h,k)$$

□

Teorema 3.21. *Sea L un grupo y $l_1 : H \to L$, $l_2 : K \to L$ dos homomorfismos de grupos que verifican que*

$$l_1(h)l_2(k) = l_2(k)l_1(h) \qquad \forall h \in H, k \in K$$

Si L cumple la propiedad universal del producto directo para estos homomorfismos, es decir, que si G es un grupo, entonces para cada par de homomorfismos $f_1 : H \to G$ y $f_2 : K \to G$ tales que

$$f_1(h)f_2(k) = f_2(k)f_1(h) \qquad \forall h \in H, k \in K$$

puede encontrarse un único homomorfismo $f : G \to L$ de forma que $fl_i = f_1$ y $fl_2 = f_2$; entonces:

$$L \cong H \times K$$

$$\begin{tikzcd}
 & L \arrow[dd, dashed, "f"] & \\
H \arrow[ur, "l_1"] \arrow[dr, "f_1"'] & & K \arrow[ul, "l_2"'] \arrow[dl, "f_2"] \\
 & G &
\end{tikzcd}$$

Demostración. En primer lugar, por ser $l_1 : H \to L$ y $l_2 : K \to L$ dos homomorfismos de forma que $l_1(h)l_2(k) = l_2(k)l_1(h)$ $\forall h \in H, k \in K$, tenemos que existe un único homomorfismo $l : H \times K \to L$ de forma que:

$$li_1 = l_1$$
$$li_2 = l_2$$

$$\begin{tikzcd}
 & L & \\
H \arrow[ur, "l_1"] \arrow[r, "i_1"'] & H \times K \arrow[u, dashed, "l"'] & K \arrow[ul, "l_2"'] \arrow[l, "i_2"]
\end{tikzcd}$$

Ahora, si tomamos $G = H \times K$ y consideramos $i_1 : H \to H \times K$ y $i_2 : K \to H \times K$, tenemos por la Proposición 3.16 que $i_1(h)i_2(k) = i_2(k)i_1(h)$ para todo $h \in H$ y para todo $k \in K$, por lo que por hipótesis tenemos que existe un único homomorfismo $i : L \to H \times K$ de forma que:

$$il_1 = i_1$$
$$il_2 = i_2$$

$$\begin{tikzcd}
 & L \arrow[d, dashed, bend right, "i"'] & \\
H \arrow[ur, bend left, "l_1"] \arrow[r, "i_1"'] & H \times K \arrow[u, dashed, bend right, "l"'] & K \arrow[ul, bend right, "l_2"'] \arrow[l, "i_2"]
\end{tikzcd}$$

Basta ver que i y l son inversos el uno del otro. Para ello, observamos que:

$$l_1 = li_1 = lil_1 \Longrightarrow li = id_{H\times K}$$
$$i_2 = il_2 = ili_2 \Longrightarrow il = id_L$$

Concluimos que $i^{-1} = l$, con lo que i y l son isomorfismos y $L \cong H \times K$. $\square$

3.4.2. Producto directo de una familia de grupos

Los resultados vistos para el producto directo de dos grupos G y H puede generalizarse para el conjunto cartesiano obtenido de multiplicar una familia arbitraria de grupos. Para estudiar este caso, fijaremos la notación en un inicio: sea Λ un conjunto arbitrariamente grande, si tenemos una familia de tantos grupos como elementos hay en Λ:

$$\{G_\lambda \mid \lambda \in \Lambda\}$$

Podemos considerar el producto cartesiano de todos ellos, que denotaremos por G:

$$G = \prod\{G_\lambda \mid \lambda \in \Lambda\} = \prod_{\lambda\in\Lambda} G_\lambda$$

Proposición 3.22. *Si $\{G_\lambda \mid \lambda \in \Lambda\}$ es una familia de grupos, definimos en su producto cartesiano $G = \prod_{\lambda\in\Lambda} G_\lambda$ la operación $\cdot : G \times G \to G$ dada por:*

$$x \cdot y = z$$

De forma que la $\lambda-$ésima coordenada de z es el producto de la $\lambda-$ésima coordenadas de x por la $\lambda-$ésima coordenada de y. Se verifica que G con esta operación es un grupo.

Notación. Si $\Lambda = \{1, \ldots, n\}$, notaremos:

$$G = \prod_{\lambda\in\Lambda} G_\lambda = G_1 \times G_2 \times \ldots \times G_n$$

Si por otra parte se tiene que $G_\lambda = H$ para todo $\lambda \in \Lambda$, entonces notaremos:

$$G = \prod_{\lambda\in\Lambda} G_\lambda = H^\Lambda$$

En el caso de que Λ sea finito y tenga n elementos, notaremos H^n.

Definición 3.6 (Proyecciones e inyecciones)**.** Fijado $\lambda \in \Lambda$, definimos:

- La proyección en la $\lambda-$ésima coordenada, $p_\lambda : G \to G_\lambda$ dada por:

  $$p_\lambda(g) = g_\lambda \qquad \forall g \in G$$

  Siendo g_λ la $\lambda-$ésima coordenada de g.

- La inyección en la $\lambda-$ésima coordenada, $i_\lambda : G_\lambda \to G$ dada por:

  $$i_\lambda(x) = g \qquad \forall x \in G_\lambda$$

  Donde $g_\mu = 1$ $\forall \mu \in \Lambda \setminus \{\lambda\}$ y $g_\lambda = x$.

Proposición 3.23. *Sea $\{G_\lambda \mid \lambda \in \Lambda\}$ una familia de grupos y sea $G = \prod_{\lambda\in\Lambda} G_\lambda$, se verifica:*

1. *p_λ y i_λ son homomorfismos de grupos, $\forall \lambda \in \Lambda$.*
2. *Las proyecciones son epimorfismos y las inyecciones son monomorfismos.*
3. *$p_\lambda i_\lambda = id_{G_\lambda}$ y $(p_\lambda i_\mu)(x) = 1$ para todo $x \in G_\mu$, $\forall \lambda \in \Lambda, \mu \in \Lambda \setminus \{\lambda\}$.*
4. *$G'_\lambda = Im(i_\lambda) \cong G_\lambda$ y es un subgrupo normal de G.*

Teorema 3.24 (Propiedad universal del producto directo)**.** *Sea $\{G_\lambda \mid \lambda \in \Lambda\} \cup \{H\}$ una familia de grupos y $G = \prod_{\lambda\in\Lambda} G_\lambda$, si tenemos una familia de homomorfismos para cada coordenada $\{f_\lambda : H \to G_\lambda \mid \lambda \in \Lambda\}$, entonces existe un único homomorfismo $f : H \to G$ de forma que $f_\lambda = p_\lambda f$, $\forall \lambda \in \Lambda$. Además, cualquier otro grupo que verifique esta propiedad será isomorfo a G.*

$$\begin{tikzcd}
H \arrow[d, dashed, "f"] \arrow[dr, "f_\lambda"] & \\
G \arrow[r, "p_\lambda"] & G_\lambda
\end{tikzcd}$$

3.4.3. Producto directo de una familia finita de grupos

Teorema 3.25 (Ley asociativa general)**.** *Tenemos que:*

1. *Si G_1, G_2, G_3 son tres grupos, entonces:*

$$(G_1 \times G_2) \times G_3 \cong G_1 \times G_2 \times G_3 \cong G_1 \times (G_2 \times G_3)$$

2. *Si $G_1, G_2, \ldots, G_n$ son n grupos, entonces si $k \in \{1, \ldots, n-1\}$, se tiene:*

$$\left(\prod_{j=1}^{k} G_j\right) \times \left(\prod_{j=k+1}^{n} G_j\right) \cong \prod_{j=1}^{n} G_j$$

Teorema 3.26. *Sean $G_1, G_2, \ldots, G_n$ n grupos y $G = G_1 \times G_2 \times \ldots \times G_n$:*

1. *$|G| = |G_1||G_2| \cdots |G_n|$. En particular, G es finito si y solo si G_k es finito, para todo $k \in \{1, \ldots, n\}$.*

2. *$O(g_1, \ldots, g_n) = \operatorname{mcm}(O(g_1), \ldots, O(g_n))$, $\forall (g_1, \ldots, g_n) \in G$.*

3.5. Producto directo interno

El caso que nos interesará ahora será fijado un grupo G, consideramos dos subgrupos suyos, $H, K < G$ y trataremos de caracterizar cuándo $H \times K \cong G$. En cuyo caso, diremos que G es producto directo interno de H y de K.

Definición 3.7 (Conmutador)**.** Sea G un grupo, definimos sobre G la operación conmutador $[\cdot, \cdot] : G \times G \to G$ dada por:

$$[h, k] = hk(kh)^{-1} = hkh^{-1}k^{-1} \qquad \forall h, k \in G$$

Esta operación viene a decirnos cómo de abelianos son los elementos h y k que estemos considerando.

Proposición 3.27. *Sea G un grupo y $h, k \in G$:*

$$hk = kh \Longleftrightarrow [h, k] = 1$$

Demostración. Basta observar que:

$$hk = kh \Longleftrightarrow (hk)^{-1} = (kh)^{-1} \Longleftrightarrow [h, k] = hk(kh)^{-1} = 1$$

□

Aunque el siguiente Teorema no nos caracteriza el hecho de que el producto de dos subgrupos de un grupo sea producto directo interno, es el resultado al que comúnmente se le conoce como caracterización del producto directo interno, puesto que viene a decirnos cuándo $H \times K \cong G$ bajo un isomorfismo que se obtiene de una forma muy natural.

Por tanto, diremos que $H \times K$ con $H, K < G$ es producto directo interno de G cuando $H \times K \cong G$ bajo el isomorfismo del siguiente Teorema:

Teorema 3.28 (Caracterización del producto directo interno)**.** *Sea G un grupo, $H, K < G$, equivalen:*

i) *La aplicación $\phi : H \times K \to G$ dada por $\phi(h,k) = hk$ es un isomorfismo.*

ii) *$H, K \lhd G$, $HK = G$ y $H \cap K = \{1\}$.*

iii) *$hk = kh \quad \forall h \in H, k \in K$, $H \vee K = G$ y $H \cap K = \{1\}$.*

iv) *$hk = kh \quad \forall h \in H, k \in K$ y para todo $g \in G$, $\exists_1 h \in H, \exists_1 k \in K$ de forma que $g = hk$.*

Demostración. Veamos las implicaciones:

$i) \Longrightarrow ii)$ Veamos las tres propiedades:

- Primero que $HK = G$:
  - $\subseteq$) $HK \subseteq G$ por definición de HK.
  - $\supseteq$) Como ϕ es sobreyectiva, dado $g \in G$, existen $h \in H$, $k \in K$ de forma que $g = \phi(h,k) = hk$, lo que nos dice que $G \subseteq HK$.
- Sea $g \in H \cap K$, entonces $g = \phi(g,1) = \phi(1,g) = g$, pero por ser ϕ inyectiva, tenemos que $(g,1) = (1,g)$, de donde $g = 1$.
- Finalmente, para ver que $H, K \lhd G$, basta observar que:

$$\begin{tikzcd} & G \arrow[d, bend left, "\phi^{-1}"] & \\ H & H \times K \arrow[l, "p_1"] \arrow[r, "p_2"] \arrow[u, bend left, "\phi"] & K \end{tikzcd}$$

  Para deducir:

$$\ker(p_2\phi^{-1}) = \{hk \in G \mid k = 1\} = H$$
$$\ker(p_1\phi^{-1}) = \{hk \in G \mid h = 1\} = K$$

  De donde tenemos que $H, K \lhd G$ (ya que $p_2\phi^{-1}$ y $p_1\phi^{-1}$ son homomorfismos y H y K conciden con sus respectivos núcleos, ver la Proposición 3.7).

$ii) \Longrightarrow iii)$ Dados $h \in H$ y $k \in K$, veamos que $[h,k] = 1$, de donde deducimos que $hk = kh$:

$$[h,k] = hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$$

- Por un lado, como K es normal, tendremos que $hkh^{-1} \in K$, de donde $[h,k] = (hkh^{-1})k^{-1} \in K$.
- Por otro lado, como H es normal, tendremos también que $kh^{-1}k^{-1} \in H$, de donde $[h,k] = h(kh^{-1}k^{-1}) \in H$.

En definitiva:

$$[h,k] \in H \cap K = \{1\} \Longrightarrow hk = kh$$

Para la segunda propiedad, basta ver que:

$$G = HK \subseteq H \vee K \subseteq G$$

iii) $\Longrightarrow$ *iv*) Sea $g \in G$, veamos que se expresa como producto de un elemento de H por otro elemento de K. Para ello, como $G = H \vee K$, existirán elementos $\alpha_1, \ldots, \alpha_n \in H \cup K$ de forma que:

$$g = \alpha_1 \ldots \alpha_n$$

Pero como $hk = kh$ para todo $k \in K$ y $h \in H$, podremos conmutar los elementos de forma que lleguemos a:

$$g = (h_1 \ldots h_m)(k_{m+1} \ldots k_n) = hk \in HK$$

Para ciertos $h \in H$, $k \in K$. Para la unicidad, si $g = h_1k_1 = h_2k_2$, tenemos que:

$$h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{1\} \Longrightarrow h_2 = h_1 \wedge k_1 = k_2$$

iv) $\Longrightarrow$ *i*) Tenemos para $(h_1, k_1), (h_2, k_2) \in H \times K$ arbitrarios que:

$$\phi((h_1, k_1)(h_2, k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1, k_1)\phi(h_2, k_2)$$

De donde ϕ es un homomorfismo. La biyectividad de ϕ se debe a que dado $g \in G$, existen unos únicos $h \in H$, $k \in K$ de forma que $g = hk = \phi(h, k)$. □

Ejemplo. Veamos si los siguientes ejemplos son o no un producto interno directo, bajo el isomorfismo natural del Teorema anterior:

1. En $G = \mathbb{R}^*$, consideramos $H = \{\pm 1\}$ y $K = \{x \in \mathbb{R} \mid x > 0\}$.

   Sí es producto interno directo, ya que se verifican:

   - $G = HK$.
   - G es abeliano, luego $H, K \lhd G$.
   - $H \cap K = \{1\}$.

   Y podemos aplicar el Teorema 3.28.

2. Sean:

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \right\}$$
$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \right\}$$
$$K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \right\}$$

   Dado un elemento de G, podemos escribirlo como un elemento de HK:

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ab \\ 0 & c \end{pmatrix}$$

   Luego $G = HK$. Sin embargo, $hk \neq kh$ para $h \in H$ y $k \in K$, ya que:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & bc \\ 0 & c \end{pmatrix} \neq \begin{pmatrix} a & ab \\ 0 & c \end{pmatrix}$$

   Por lo que G no es producto directo interno de H y de K.

3. Sea $G = \mathbb{C}^*$, consideramos $H = \{z \in \mathbb{C} \mid |z| = 1\}$ y $K = \mathbb{R}^+$. Por la forma polar de los números complejos, tenemos que $G = HK$:

$$z = \frac{z}{|z|}|z| \in HK$$

Y como G es abeliano, tenemos que $H, K \lhd G$. Además:

$$H \cap K = \{1\}$$

Veamos ahora cómo se comportan los subgrupos con el producto directo:

Proposición 3.29. *Sea G un grupo, $H, K < G$, si $H_1 < H$ y $K_1 < K$, entonces:*

1. *$H_1 \times K_1 < H \times K$.*
2. *Existe un monomorfismo $Aut(H) \times Aut(K) \to Aut(H \times K)$.*

Demostración. Veamos que los dos se cumplen:

1. $H_1 \times K_1 \subseteq H \times K$. Además, como $H_1 < H$ y $K_1 < K$, $H_1 \times K_1$ va a ser cerrado para el producto, el producto será asociativo, tendrá al elemento $(1, 1)$ como neutro y fijado un elemento $(x, y) \in H_1 \times K_1$, tendremos que $(x, y)^{-1} = (x^{-1}, y^{-1}) \in H_1 \times K_1$, de donde concluimos que $H_1 \times K_1 < H \times K$.

2. Consideramos:

$$\begin{array}{rrcl} \psi : & Aut(H) \times Aut(K) & \longrightarrow & Aut(H \times K) \\ & (\alpha, \beta) & \longmapsto & \psi(\alpha, \beta) \end{array}$$

   Donde $\psi(\alpha, \beta) : H \times K \to H \times K$ viene dada por:

$$\psi(\alpha, \beta)(h, k) = (\alpha(h), \beta(k)) \qquad \forall (h, k) \in H \times K$$

   Veamos en primer lugar que la aplicación ψ está bien definida, es decir, que $\psi(\alpha, \beta)$ es un automorfismo siempre que $\alpha \in Aut(H)$ y $\beta \in Aut(K)$:

   - Para ver que $\psi(\alpha, \beta)$ es un homomorfismo, dados $(h, k), (h', k') \in H \times K$:

$$\psi(\alpha, \beta)((h, k)(h', k')) = \psi(\alpha, \beta)(hh', kk') = (\alpha(hh'), \beta(kk'))$$
$$= (\alpha(h)\alpha(h'), \beta(k)\beta(k')) = (\alpha(h), \beta(k))(\alpha(h'), \beta(k')) = \psi(\alpha, \beta)(h, k)\psi(\alpha, \beta)(h', k')$$

   - Para la sobreyectividad, dado $(h, k) \in H \times K$, como $\alpha \in Aut(H)$ y $\beta \in Aut(K)$ son sobreyectivas, existirán $h' \in H$, $k' \in K$ de forma que:

$$\alpha(h') = h \qquad \beta(k') = k$$

     Por lo que:

$$\psi(\alpha, \beta)(h', k') = (\alpha(h'), \beta(k')) = (h, k)$$

- Para la inyectividad, sean $(h, k), (h', k') \in H \times K$ de forma que:

$$(\alpha(h), \beta(k)) = \psi(\alpha, \beta)(h, k) = \psi(\alpha, \beta)(h', k') = (\alpha(h'), \beta(k'))$$

De donde deducimos que:

$$\alpha(h) = \alpha(h') \qquad \beta(k) = \beta(k')$$

Pero como α y β son inyectivas, tenemos que $h = h'$ y $k = k'$, de donde $(h, k) = (h', k')$.

Finalmente, veamos que ψ es un monomorfismo:

- Para ver que es un homomorfismo, dadas $(\alpha, \beta), (\alpha', \beta') \in Aut(H) \times Aut(K)$:

$$\psi((\alpha, \beta)(\alpha', \beta')) = \psi(\alpha\alpha', \beta\beta') \overset{(*)}{=} \psi(\alpha, \beta)\psi(\alpha', \beta')$$

Donde en $(*)$ se da la igualdad funcional, ya que para $(h, k) \in H \times K$:

$$\begin{aligned}\psi(\alpha\alpha', \beta\beta')(h, k) &= ((\alpha \circ \alpha')(h), (\beta \circ \beta')(k)) = (\alpha(\alpha'(h)), \beta(\beta'(k)))\\ (\psi(\alpha, \beta)\psi(\alpha', \beta'))(h, k) &= \psi(\alpha, \beta)(\alpha'(h), \beta'(k)) = (\alpha(\alpha'(h)), \beta(\beta'(k)))\end{aligned}$$

- Para ver que ψ es inyectiva, sean $(\alpha, \beta), (\alpha', \beta') \in Aut(H) \times Aut(K)$ de forma que:

$$\psi(\alpha, \beta) = \psi(\alpha', \beta')$$

Entonces:

$$(\alpha(h), \beta(k)) = \psi(\alpha, \beta)(h, k) = \psi(\alpha', \beta')(h, k) = (\alpha'(h), \beta'(k)) \quad \forall (h, k) \in H \times K$$

De donde deducimos que $\alpha = \alpha'$ y que $\beta = \beta'$, por lo que ψ es inyectiva.

□

Teorema 3.30. *Sean H, K dos grupos finitos tales que* $\text{mcd}(|H|, |K|) = 1$, *entonces:*

1. *$\forall L < H \times K$, $\exists_1 H_1 < H, K_1 < K$ de forma que:*

$$L = H_1 \times K_1$$

Es decir, todo subgrupo de $H \times K$ se descompone de forma única como un subgrupo de H por un subgrupo de K.

2. *La aplicación $\psi : Aut(H) \times Aut(K) \to Aut(H \times K)$ de la Proposición 3.29 es un isomorfismo.*

Demostración. Veamos los dos resultados:

1. Sea $L < H \times K$, consideramos:

$$H_1 = p_1(L) < H \qquad K_1 = p_2(L) < K$$

Por la Proposición 3.29, tenemos que $H_1 \times K_1 < H \times K$, y por la definición de L que $L < H_1 \times K_1$, ya que si $(h, k) \in L$:

$$h = p_1(h, k) \in H_1$$
$$k = p_2(h, k) \in K_1$$

Basta ver que $H_1 \times K_1 < L$.

$$\begin{tikzcd} H \arrow[r, leftarrow, "p_1"'] \arrow[d, dash] & H \times K \arrow[r, "p_2"'] \arrow[d, dash] & K \arrow[d, dash] \\ H_1 & L & K_1 \end{tikzcd}$$

Para ello, si notamos $n = |H|$ y $m = |K|$, por el Teorema de Bezout $\exists r, s \in \mathbb{Z}$ de forma que:

$$nr + ms = 1$$

- En primer lugar, si $h \in H_1$, por su definición y la sobreyectividad de p_1, existirá $(h, k) \in L$ de forma que $p_1(h, k) = h$, de donde:

  $$L \ni (h, k)^{ms} = (h^{ms}, k^{ms}) = \left(h^{1-nr}, 1\right) = (h, 1)$$

  Por lo que: $\{(h, 1) \mid h \in H_1\} \subseteq L$.
- Ahora, si $k \in K_1$, por su definición y la sobreyectividad de p_2, existirán $(h, k) \in L$ de forma que $p_2(h, k) = k$, de donde:

  $$K \ni (h, k)^{nr} = (h^{nr}, k^{nr}) = (1, k^{1-ms}) = (1, k)$$

  Por lo que: $\{(1, k) \mid k \in K_1\} \subseteq L$.

Sea ahora $(h, k) \in H_1 \times K_1$, tenemos que:

$$(h, k) = (h, 1)(1, k) \in L$$

De donde $H_1 \times K_1 < L$. Finalmente, la construcción que hemos realizado nos da la unicidad, pues si existen otros subconjuntos $H_2 < H$ y $K_2 < K$ de forma que $L = H_2 \times K_2$, tendríamos que:

$$H_2 = p_1(L) = H_1 \qquad K_2 = p_2(L) = K_1$$

2. Basta ver que $\psi : Aut(H) \times Aut(K) \to Aut(H \times K)$ es sobreyectiva, es decir, que dada $\varphi \in Aut(H \times K)$, podemos encontrar $\alpha \in Aut(H)$ y $\beta \in Aut(K)$ de forma que $\varphi = \psi(\alpha, \beta)$. Para ello, mostraremos el proceso para encontrar α y el proceso para encontrar β es análogo.

   En primer lugar, lo que hacemos es estudiar la imagen por φ del conjunto $H \times \{1\} < H \times K$. Como φ es un homomorfismo, sabemos que la imagen de $H \times \{1\}$ por φ será un subgrupo de $H \times K$, a quien llamaremos G_1:

   $$G_1 = \varphi(H \times \{1\}) < H \times K$$

Por el apartado 1, sabemos que podemos encontrar únicos $H_1 < H$ y $K_1 < K$ de forma que $G_1 = H_1 \times K_1$. Además, por ser φ biyectiva, tendremos que:

$$|H| = |H \times \{1\}| = |H_1 \times K_1| = |H_1||K_1|$$

Veamos que $|K_1| = 1$. Para ello, si $m = |K_1| \in \mathbb{N}$:

- De la igualdad $|H| = |H_1|m$ deducimos que m divide a $|H|$.
- Como $m = |K_1|$ y $K_1 < K$, por el Teorema de Lagrange tenemos también que m divide a $|K|$.

Por la definición del máximo común divisor, concluimos que m divide a $\text{mcd}(|H|, |K|) = 1$, de donde $m = 1$ y $K_1 = \{1\}$.

Finalmente, de la igualdad $|H| = |H_1|$ concluimos que $H = H_1$. Hemos probado que:

$$\varphi(H \times \{1\}) = H \times \{1\}$$

Definimos ahora $\alpha : H \to H$ dada por:

$$\alpha(h) = p_1(\varphi(i_1(h))) \qquad \forall h \in H$$

Está claro que α es un homomorfismo, como composición de homomorfismos.

- Para la sobreyectividad de α, como $\varphi(H \times \{1\}) = H \times \{1\}$, tenemos que:

  $$\alpha(H) = p_1(\varphi(i_1(H))) = p_1(\varphi(H \times \{1\})) = p_1(H \times \{1\}) = H$$

- Para la inyectividad, sean $h_1, h_2 \in H$ de forma que:

  $$p_1(\varphi(h_1, 1)) = \alpha(h_1) = \alpha(h_2) = p_2(\varphi(h_2, 1))$$

  Como $\varphi(H \times \{1\}) = H \times \{1\}$, sabemos que existirán $h_1', h_2' \in H$ de forma que:

  $$\varphi(h_1, 1) = (h_1', 1) \qquad \varphi(h_2, 1) = (h_2', 1)$$

  Por lo que:

  $$h_1' = p_1(h_1', 1) = p_1(\varphi(h_1, 1)) = p_1(\varphi(h_2, 1)) = p_1(h_2', 1) = h_2'$$

  De donde concluimos que α es inyectiva.

De forma análoga a lo que hicimos anteriormente, puede probarse que:

$$\varphi(\{1\} \times K) = \{1\} \times K$$

Y definiendo $\beta : H \times K \to H \times K$ dada por:

$$\beta(k) = p_2(\varphi(i_2(k))) \qquad \forall k \in K$$

Tenemos que $\beta \in Aut(K)$.

Con estos dos automorfismos, veamos que $\psi(\alpha, \beta) = \varphi$:

$$\psi(\alpha,\beta)(h,k) = (\alpha(h), \beta(k)) = (p_1(\varphi(h,1)), p_2(\varphi(1,k))) \stackrel{(*)}{=} \varphi(h,k) \qquad \forall (h,k) \in H \times K$$

Donde en $(*)$ hemos usado que existirán $h' \in H$ y $k' \in K$ de forma que:

$$\varphi(h,1) = (h',1) \qquad \varphi(1,k) = (1,k')$$

Por lo que:

$$\begin{aligned}(p_1(\varphi(h,1)), p_2(\varphi(1,k))) &= (p_1(h',1), p_2(1,k')) = (h',k') \\ &= (h',1)(1,k') = \varphi(h,1)\varphi(1,k) = \varphi(h,k)\end{aligned}$$

□

El punto 2 de este último Teorema será un resultado que usemos en numerosos ejercicios, sin considerar de forma explícita la aplicación ψ pero usando el isomorfismo $Aut(H) \times Aut(K) \cong Aut(H \times K)$ bajo las hipótesis apropiadas.

3.5.1. Producto directo interno de una familia de subgrupos

Teorema 3.31. *Sea $\{G_\lambda \mid \lambda \in \Lambda\}$ una familia de grupos de forma que para cada $\lambda \in \Lambda$ tenemos $H_\lambda < G_\lambda$, entonces:*

$$\prod_{\lambda \in \Lambda} H_\lambda < \prod_{\lambda \in \Lambda} G_\lambda$$

Teorema 3.32. *Sea $\{G_\lambda \mid \lambda \in \Lambda\}$, entonces existe un monomorfismo*

$$\prod_{\lambda \in \Lambda} Aut(G_\lambda) \longrightarrow Aut\left(\prod_{\lambda \in \Lambda} G_\lambda\right)$$

3.5.2. Producto directo interno de una familia finita de subgrupos

Teorema 3.33. *Sea G un grupo y $G_1, \ldots, G_n < G$ n subgrupos de G, definimos la aplicación $\phi : G_1 \times \ldots \times G_n \to G$ dada por:*

$$\phi(g_1, \ldots, g_n) = g_1 \cdot \ldots \cdot g_n \qquad \forall (g_1, \ldots, g_n) \in G_1 \times \ldots \times G_n$$

Son equivalentes:

i) *ϕ es un isomorfismo.*

ii) *$G_k \lhd G$ $\forall k \in \{1, \ldots, n\}$, $G_1 \ldots G_n = G$ y $(G_1 \ldots G_{k-1}) \cap G_k = \{1\}$ para todo $k \in \{2, \ldots, n\}$.*

iii) *$g_k g_h = g_h g_k$ para todo $g_h \in G_h$, $g_k \in G_k$ con $k \neq h$, $G = G_1 \vee \ldots \vee G_n$ y $(G_1 \ldots G_{k-1}) \cap G_k = \{1\}$ para todo $k \in \{2, \ldots, n\}$.*

iv) $g_k g_h = g_h g_k$ *para todo* $g_h \in G_h$, $g_k \in G_k$ *con* $k \neq h$, *y todo elemento* $g \in G$ *se expresa de manera única como* $g = g_1 \dots g_n$ *con* $g_k \in G_k$ *para todo* $k \in \{1, \dots, n\}$.

Teorema 3.34. *Sean* $G_1, \dots, G_n$ *n grupos de forma que sus órdenes son primos relativos dos a dos, si* $G = G_1 \times \dots \times G_n$, *entonces:*

1. $\exists_1 H_k < G_k$ *tal que* $L = H_1 \times \dots \times H_n$ *para todo* $L < G$.
2. $Aut(G_1) \times \dots \times Aut(G_n) \cong Aut(G)$.

3.6. Producto directo de grupos cíclicos

Notación. Cuando hablemos del producto directo de dos grupos cíclicos, en vez de usar $\times$, usaremos como notación $\oplus$, ya que normalmente usamos la notación aditiva al trabajar con grupos cíclicos.

Ejemplo. En primer lugar, hemos de tener en cuenta que el producto directo de dos grupos cíclicos no tiene por qué ser en general un grupo cíclico. Veamos varios ejemplos de que no se cumple:

1. Supongamos que $\mathbb{Z} \oplus \mathbb{Z}$ es cíclico. En cuyo caso, tenemos que $\exists (r, s) \in \mathbb{Z} \oplus \mathbb{Z}$ de forma que:
$$\mathbb{Z} \oplus \mathbb{Z} = \langle (r, s) \rangle$$
De donde para $(1, 0) \in \mathbb{Z} \oplus \mathbb{Z}$ $\exists n \in \mathbb{Z}$ de forma que:
$$(1,0) = n(r,s) \Longrightarrow \left\{ \begin{array}{l} nr = 1 \\ ns = 0 \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} n, r \in \{\pm 1\} \\ s = 0 \end{array} \right. \Longrightarrow (r,s) = \left\{ \begin{array}{l} (-1,0) \\ (1,0) \end{array} \right.$$
Sin embargo, $(0, 1) \in \mathbb{Z} \oplus \mathbb{Z}$, por lo que $\exists m \in \mathbb{Z}$ de forma que:
$$(0,1) = m(1,0) \Longrightarrow \left\{ \begin{array}{l} m = 0 \\ 1 = 0 \end{array} \right.$$
Contradicción, por lo que $\mathbb{Z} \oplus \mathbb{Z}$ no es cíclico.

2. Ahora, supongamos que $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ es cíclico, con lo que de la misma forma, $\exists (r, s) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$ de modo que:
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \langle (\overline{r}, \overline{s}) \rangle$$
Sin embargo:
$$O(\overline{r}, \overline{s}) = \text{mcm}(O(\overline{r}), O(\overline{s})) = \left\{ \begin{array}{l} 1 \Longleftrightarrow \overline{r} = \overline{s} = 0 \\ 2 \Longleftrightarrow \overline{r} \neq 0 \vee \overline{s} \neq 0 \end{array} \right.$$
En $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ no hay elementos de orden 4, pero:
$$|\mathbb{Z}_2 \oplus \mathbb{Z}_2| = 4$$
Un grupo de orden 4 que no tiene elementos de orden 4 nunca puede ser cíclico. De hecho, tendremos que $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong V$.

3. Un ejemplo de dos grupos cíclicos cuyo producto directo es cíclico es:

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3$$

Que tiene orden $|\mathbb{Z}_2 \oplus \mathbb{Z}_3| = |\mathbb{Z}_2||\mathbb{Z}_3| = 6$. Si consideramos $(\overline{1}, \overline{1})$, tenemos que:

$$O(\overline{1}, \overline{1}) = \text{mcm}(O(\overline{1}_2), O(\overline{1}_3)) = \text{mcm}(2, 3) = 6$$

Por lo que $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle (\overline{1}, \overline{1}) \rangle$. Notemos que el motivo de que esto haya sucedido es porque 2 y 3 son primos relativos.

Proposición 3.35. *Si G y H son grupos cíclicos finitos, entonces:*

$$G \oplus H \text{ es cíclico } \Longleftrightarrow \text{mcd}(|G|, |H|) = 1$$

Demostración. Veamos las dos implicaciones. Para ello, supongamos que:

$$G = \langle x \rangle, \quad O(x) = n, \quad H = \langle y \rangle, \quad O(y) = m$$

Para ciertos $x \in G$ y $y \in H$.

$\Longleftarrow$) Si $\text{mcd}(n, m) = 1$, entonces $\text{mcm}(n, m) = nm$, de donde:

$$O(x, y) = \text{mcm}(O(x), O(y)) = nm = |G||H| = |G \times H|$$

Tenemos un grupo de orden nm que contiene a un elemento de orden nm, luego $G \times H = \langle (x, y) \rangle$.

$\Longrightarrow$) Si $G \oplus H = \langle (a, b) \rangle$, entonces:

$$O(a, b) = \text{mcm}(O(a), O(b)) = nm = |G||H| = |G \times H|$$

Como $O(a) \mid n$ y $O(b) \mid m$, llegamos a que $O(a) = n$ y $O(b) = m$. Finalmente:

$$\text{mcd}(n, m) = \frac{nm}{\text{mcm}(n, m)} = \frac{nm}{nm} = 1$$

□

Corolario 3.35.1. *Si $G_1, G_2, \ldots, G_n$ son n grupos cíclicos finitos, entonces:*

$$\bigoplus_{k=1}^{n} G_k \text{ cíclico} \Longleftrightarrow \text{mcd}(|G_i|, |G_j|) = 1 \quad \forall i, j \in \{1, \ldots, n\}, i \neq j$$

Ejemplo. Aplicando esta última proposición:

- $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{30}$.
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ no es cíclico.

Ejemplo. Podemos demostrar que S_3 no es producto directo interno de subgrupos propios. Por reducción al absurdo, si fuera producto directo, como $|S_3| = 6$, tendría un subgrupo de orden 2 y otro de orden 3, ambos isomorfos a C_2 y C_3. Si tuviera dos subgrupos propios cuyo producto propio fuera él mismo, tendríamos:

$$S_3 \cong C_2 \oplus C_3 \cong C_6$$

Pero S_3 no es cíclico, hemos llegado a una contradicción.

4. Grupos resolubles

Este Capítulo trata sobre los grupos resolubles, propiedad interesante de un grupo que tendrá numerosas aplicaciones, como por ejemplo en la solución de ecuaciones con radicales. Sin embargo, la definición de grupo resoluble ha de esperar, pues primero tenemos que hacer un estudio de las "series de un grupo".

4.1. Series de un grupo

Definición 4.1 (Serie de un grupo)**.** Sea G un grupo, una serie de G es una cadena de subgrupos $G_0, G_1, \ldots, G_r$ de forma que:

$$G = G_0 > G_1 > G_2 > \ldots > G_r = \{1\}$$

En dicho caso, diremos que la serie tiene longitud r.

Ejemplo. En S_3, podemos considerar la serie:

$$S_3 > A_3 > \{1\}$$

Definición 4.2 (Refinamiento)**.** Sea G un grupo, si consideramos sobre él dos series:

$$G = H_0 > H_1 > \ldots > H_s = \{1\} \tag{4.1}$$

$$G = G_0 > G_1 > G_2 > \ldots > G_r = \{1\} \tag{4.2}$$

Diremos que (4.2) es un refinamiento de (4.1) si todo grupo que aparece en (4.1) también aparece en (4.2). Ha de ser por tanto $r \geqslant s$.

Decimos que (4.2) es un refinamiento propio de (4.1) si en (4.2) hay grupos que no aparecen en (4.1). En dicho caso, ha de ser $r > s$.

Ejemplo. En A_4, podemos considerar la serie:

$$A_4 > V > \{1\}$$

Un refinamiento propio de la misma es:

$$A_4 > V > \langle (1\ 2)(3\ 4) \rangle > \{1\}$$

Definición 4.3 (Series propia y normal)**.** Sea G un grupo, si consideramos una serie de G:

$$G = G_0 > G_1 > \ldots > G_r = \{1\}$$

- Decimos que es una serie propia si todas las inclusiones entre los subgrupos son propias, es decir, si $G_{k+1} \subsetneq G_k$, para todo $k \in \{0, \ldots, r-1\}$.
- Decimos que es una serie normal si todas las relaciones de subgrupo que aparecen son de subgrupo normal, es decir, si $G_k \rhd G_{k+1}$, para todo $k \in \{0, \ldots, r-1\}$.

  En dicho caso, lo notaremos como:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$

Ejemplo. Todas las series anteriores eran series normales propias:

$$S_3 \rhd A_3 \rhd \{1\}$$
$$A_4 \rhd V \rhd \{1\}$$
$$A_4 \rhd V \rhd \langle (1\ 2)(3\ 4) \rangle \rhd \{1\}$$

Definición 4.4 (Índices y factores de una serie)**.**
Dada una serie normal de un grupo G:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$

- Llamamos factores de la serie a los grupos cocientes:

$$G_{k-1}/G_k \qquad \forall k \in \{1, \ldots, r\}$$

- Llamamos índices de la serie a los correspondientes órdenes de los factores.

  Si $i_k = [G_{k-1} : G_k]$ para todo $k \in \{1, \ldots, r\}$, entonces notaremos:

$$G = G_0 \overset{i_1}{\rhd} G_1 \overset{i_2}{\rhd} \ldots \overset{i_r}{\rhd} G_r = \{1\}$$

Ejemplo. Por ejemplo, en la serie:

$$S_3 \rhd A_3 \rhd \{1\}$$

Tenemos los factores:

$$S_3/A_3 \cong C_2 \qquad A_3/\{1\} \cong A_3$$

Y los índices:

$$S_3 \overset{2}{\rhd} A_3 \overset{3}{\rhd} \{1\}$$

Si consideramos ahora la serie:

$$A_4 \overset{3}{\rhd} V \overset{2}{\rhd} \langle (1\ 2)(3\ 4) \rangle \overset{2}{\rhd} \{1\}$$

Los factores que obtenemos son:

$$A_4/V \qquad V/\langle (1\ 2)(3\ 4) \rangle \qquad \langle (1\ 2)(3\ 4) \rangle/\{1\}$$

Definición 4.5. Sea G un grupo, si tenemos dos series normales de G:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$
$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_s = \{1\}$$

Se dice que son isomorfas si $r = s$ y existe $\sigma \in S_r$ de forma que:

$$G_{k-1}/G_k \cong H_{\sigma(k)-1}/H_{\sigma(k)} \qquad \forall k \in \{1, \ldots, r\}$$

Ejemplo. En $\mathbb{Z}/24\mathbb{Z}$ consideramos las series:

$$\mathbb{Z}/24\mathbb{Z} \rhd 2\mathbb{Z}/24\mathbb{Z} \rhd 4\mathbb{Z}/24\mathbb{Z} \rhd 8\mathbb{Z}/24\mathbb{Z} \rhd 24\mathbb{Z}/24\mathbb{Z} = \{0\}$$
$$\mathbb{Z}/24\mathbb{Z} \rhd 3\mathbb{Z}/24\mathbb{Z} \rhd 6\mathbb{Z}/24\mathbb{Z} \rhd 12\mathbb{Z}/24\mathbb{Z} \rhd 24\mathbb{Z}/24\mathbb{Z} = \{0\}$$

Que son dos series isomorfas, para la permutación $\sigma = (1\ 2\ 3\ 4)$, ya que:

$$\mathbb{Z}/24\mathbb{Z} \overset{2}{\rhd} 2\mathbb{Z}/24\mathbb{Z} \overset{2}{\rhd} 4\mathbb{Z}/24\mathbb{Z} \overset{2}{\rhd} 8\mathbb{Z}/24\mathbb{Z} \overset{3}{\rhd} 24\mathbb{Z}/24\mathbb{Z} = \{0\}$$
$$\mathbb{Z}/24\mathbb{Z} \overset{3}{\rhd} 3\mathbb{Z}/24\mathbb{Z} \overset{2}{\rhd} 6\mathbb{Z}/24\mathbb{Z} \overset{2}{\rhd} 12\mathbb{Z}/24\mathbb{Z} \overset{2}{\rhd} 24\mathbb{Z}/24\mathbb{Z} = \{0\}$$

4.1.1. Series de composición

Pasamos ya al estudio de las series que nos interesarán, que son las series de composición.

Definición 4.6 (Serie de composición)**.** Una serie de G se dice que es una serie de composición de G si es una serie normal sin refinamientos normales propios.
En una serie de composición, será usual referirnos a los factores como factores de composición, y a los índices como índices de composición.

Ejemplo. Ejemplos de series de composición son:

- Las dos series anteriores sobre $\mathbb{Z}/24\mathbb{Z}$ son series de composición, ya que los índices no permiten introducir más subgrupos a la serie.
- Anteriormente vimos que la serie $A_4 \rhd V \rhd \{1\}$ no era de composición, ya que podíamos refinarla más: $A_4 \rhd V \rhd \langle(1\ 2)(3\ 4)\rangle \rhd \{1\}$, aunque ya esta última sí que es de composición.

Por ahora, para estudiar si una serie es o no de composición, no nos queda otra que realizar un análisis exhaustivo del retículo de subgrupos del grupo que consideremos, analizando solo las inclusiones de subgrupos que sean normales, algo que mostraremos en los siguientes ejemplos.

Ejemplo. Sea $\mathbb{K}$ un cuerpo, sobre $\mathrm{GL}_2(\mathbb{K})$ consideramos las matrices triangulares superiores:

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{K}^*, b \in \mathbb{K} \right\}$$

Que tiene infinitos elementos y no es un grupo abeliano, ya que:

$$\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \qquad \forall d \neq 1$$

Si consideramos ahora:

$$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{K} \right\}$$

Tenemos que $T \rhd U \rhd \{1\}$ es una serie de composición.

Notemos que:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$$

Si ahora para $n > 2$ cogemos como T el conjunto de las matrices triangulares superiores y luego cogemos:

$$N = \{\text{matrices triangulares superiores con diagonal de ceros}\}$$
$$U_r = I + N^r$$

Tomando potencias los elementos van subiendo en la diagonal. Podemos considerar:

$$T \rhd U_1 \rhd U_2 \rhd \ldots \rhd U_n = I$$

Ejemplo. Tratamos de buscar cuántas series de composición hay en los siguientes grupos:

- En S_3, recordamos que el retículo de subgrupos que teníamos era:

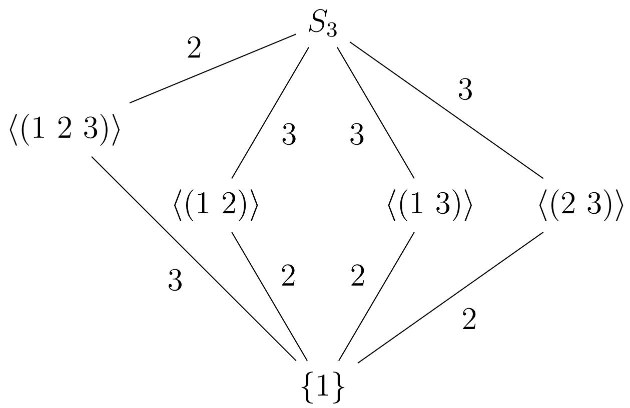


Figura 4.1: Diagrama de Hasse para los subgrupos de S_3.

Como $A_3 = \langle(1\ 2\ 3)\rangle \lhd S_3$ (por tener índice 2) y ningún otro subgrupo de S_3 es normal salvo el trivial (compruébese), la única serie de composición de S_3 es:

$$S_3 \rhd A_3 \rhd \{1\}$$

- En D_4:

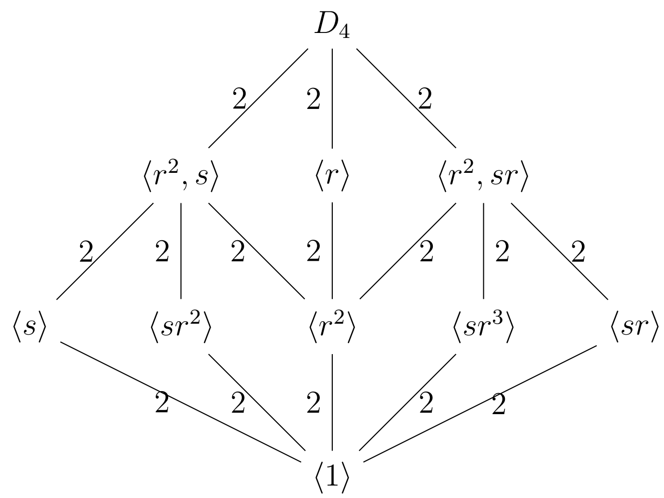
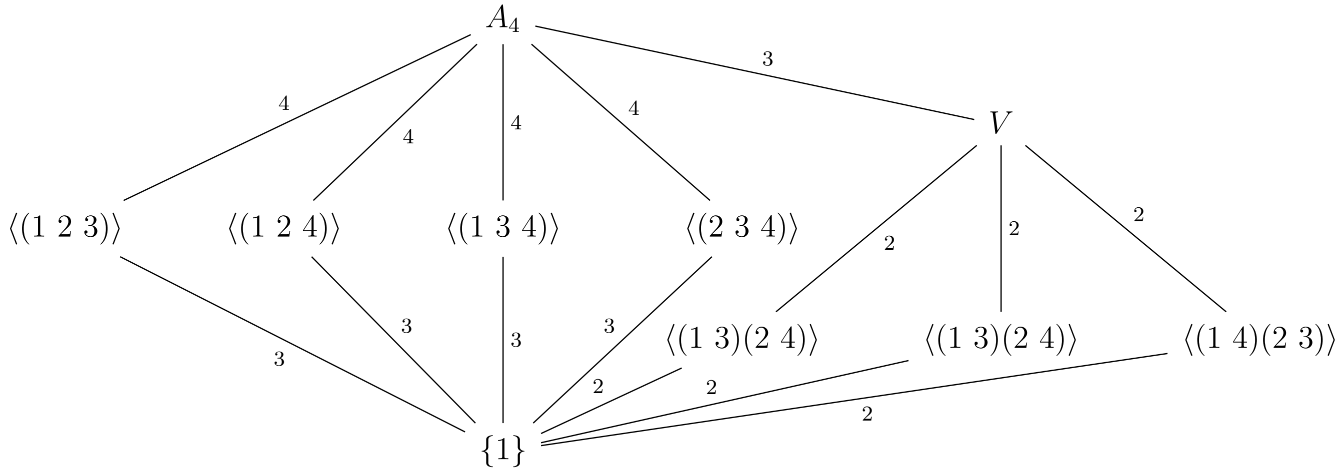


Figura 4.2: Diagrama de Hasse para los subgrupos de D_4.

Como todos los índices del grafo son 2, todas las relaciones de inclusión mostradas en el grafo en realidad son relaciones de normalidad ($\lhd$), por lo que tenemos 7 series de composición distintas (una por cada forma que tengamos de llegar desde D_4 hasta $\{1\}$ en el grafo mediante caminos descendientes):

$$\begin{gathered}
D_4 \rhd \langle r^2, s\rangle \rhd \langle s\rangle \rhd \{1\} \\
D_4 \rhd \langle r^2, s\rangle \rhd \langle sr^2\rangle \rhd \{1\} \\
D_4 \rhd \langle r^2, s\rangle \rhd \langle r^2\rangle \rhd \{1\} \\
D_4 \rhd \langle r^2, sr\rangle \rhd \langle r^2\rangle \rhd \{1\} \\
D_4 \rhd \langle r^2, sr\rangle \rhd \langle sr\rangle \rhd \{1\} \\
D_4 \rhd \langle r^2, sr\rangle \rhd \langle sr^3\rangle \rhd \{1\} \\
D_4 \rhd \langle r\rangle \rhd \langle r^2\rangle \rhd \{1\}
\end{gathered}$$

- Para A_4:

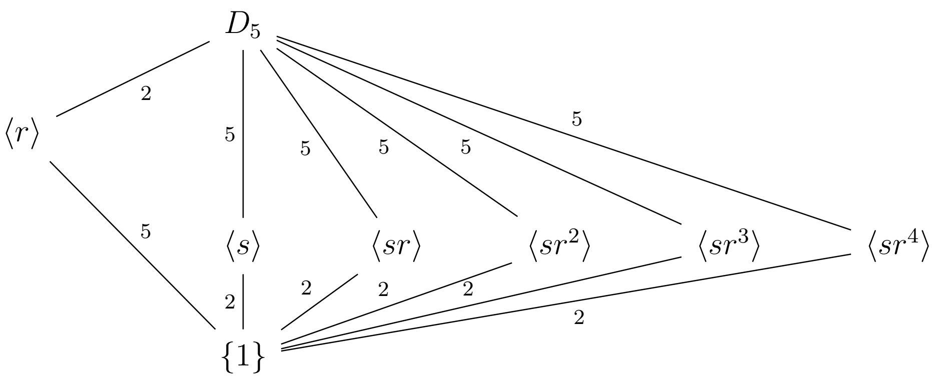


Como $V \lhd A_4$, tenemos como series de composición:

$$A_4 \rhd V \rhd \langle (1\ 2)(3\ 4) \rangle \rhd \{1\}$$
$$A_4 \rhd V \rhd \langle (1\ 3)(2\ 4) \rangle \rhd \{1\}$$
$$A_4 \rhd V \rhd \langle (2\ 3)(2\ 3) \rangle \rhd \{1\}$$

Además, como ninguna de las relaciones $\langle (i\ j\ k) \rangle < A_4$ es normal, no tenemos más series de composición.

- En $D_5 = \langle r, s \mid r^5 = s^2 = 1, sr = r^4 s \rangle$ tenemos:



Solo tenemos la serie de composición:

$$D_5 \rhd \langle r \rangle \rhd \{1\}$$

Ya que D_5 no tiene más subgrupos normales, a parte del trivial.

- En el grupo de los cuaternios:

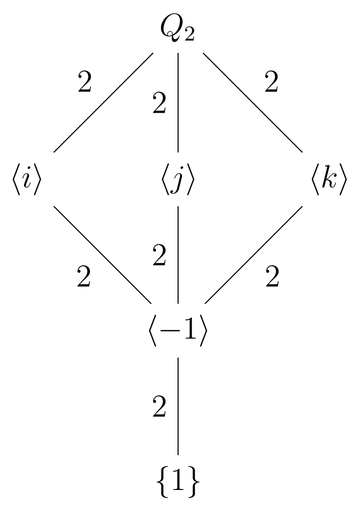


Figura 4.3: Diagrama de Hasse para los subgrupos del grupo de los cuaternios.

Como todas las aristas del grafo están numeradas con índice 2, todas las relaciones de subgrupo son normales, por lo que tenemos 3 series de composición, una por cada camino posible:

$$\begin{gathered}
Q_2 \rhd \langle i \rangle \rhd \langle -1 \rangle \rhd \{1\} \\
Q_2 \rhd \langle j \rangle \rhd \langle -1 \rangle \rhd \{1\} \\
Q_2 \rhd \langle k \rangle \rhd \langle -1 \rangle \rhd \{1\}
\end{gathered}$$

- El retículo de S_5 se deja como ejercicio.
- En $S_3 \times \mathbb{Z}_2$: Por una parte, en S_3 teníamos una única serie de composición:

$$S_3 \rhd A_3 \rhd \{1\}$$

Y en $\mathbb{Z}_2$ la única opción a considerar es $\mathbb{Z}_2 \rhd \{0\}$. Podemos considerar ahora las series de composición resultantes de considerar todas las combinaciones:

$$\begin{gathered}
S_3 \times \mathbb{Z}_2 \rhd S_3 \times \{0\} \rhd A_3 \times \{0\} \rhd \{(1,0)\} \\
S_3 \times \mathbb{Z}_2 \rhd A_3 \times \mathbb{Z}_2 \rhd A_3 \times \{0\} \rhd \{(1,0)\} \\
S_3 \times \mathbb{Z}_2 \rhd A_3 \times \mathbb{Z}_2 \rhd \{1\} \times \mathbb{Z}_2 \rhd \{(1,0)\}
\end{gathered}$$

Que obtenemos primero variando algunos y luego otras. Esto es posible ya que el producto de subgrupos es subgrupo del producto, como vimos en la Proposición 3.29; y además si $A \lhd B$ y $C \lhd D$, entonces $A \times C \lhd B \times D$ (compruébese).

Sin embargo, como $\text{mcd}(6, 2) = 2 \neq 1$, el Teorema 3.30 no puede asegurarnos que todos los subgrupos de $S_3 \times \mathbb{Z}_2$ sean producto de subgrupos, y de hecho vamos a tener que hay subgrupos del producto que no son producto de subgrupos de cada coordenada, por lo que tendremos otra serie de composición, que tendrá la forma:

$$S_3 \times \mathbb{Z}_2 \overset{2}{\rhd} H_1 \overset{2}{\rhd} H_2 \overset{3}{\rhd} \{1\}$$

Con $H_1, H_2 < S_3 \times \mathbb{Z}_2$ que no especificaremos pero diremos que $H_1 \cong S_3$ y $H_2 \cong A_3$.

Definición 4.7 (Grupo simple)**.** Un grupo G se dice simple si no es trivial y no tiene subgrupos normales propios.

Ejemplo. $\mathbb{Z}_3$ es un grupo simple, ya que su retículo de subgrupos es:

$$\begin{tikzcd}
\mathbb{Z}_3 \arrow[d, dash] \\
\{0\}
\end{tikzcd}$$

Un resultado que veremos luego (el Teorema de Abel) nos dirá que los grupos A_n para $n \geqslant 5$ son grupos simples.

4.1.2. Resultados sobre series de composición

Proposición 4.1 (Caracterización de los grupos abelianos simples)**.**
Un grupo es abeliano y simple si y solo si es de orden primo.

Demostración. Por doble implicación:

$\Longleftarrow$) Si G es un grupo de orden p primo, vimos en la Proposición 2.14 que entonces es cíclico, luego abeliano. Además, por ser de orden primo, no tendrá subgrupos propios (ya que sus órdenes serían distintos de p y de 1 y dividirían a p), por lo que también será simple.

$\Longrightarrow$) Si G es abeliano, entonces todos sus subgrupos serán normales. Si es simple, no tendrá subgrupos propios (ya que si no serían normales, luego no sería simple). Sea $1 \neq x \in G$, sabemos que $\langle x \rangle < G$, de donde ($\{1\} \neq \langle x \rangle$ y G no tiene subgrupos propios) $G = \langle x \rangle$, por lo que G es cíclico.

Veamos ahora que G es finito: como vimos en el Teorema 2.16, G ha de ser isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}_n$ para algún $n \in \mathbb{N}$. Supongamos que G no es finito, con lo que $G \cong \mathbb{Z}$, pero G es simple (por hipótesis) y $\mathbb{Z}$ no, pues tiene subgrupos propios (por ejemplo, $2\mathbb{Z}$). Como la propiedad de "ser simple" se preserva por isomorfismos, G no puede ser isomorfo a $\mathbb{Z}$, luego tendremos que $G \cong \mathbb{Z}_n$ para algún $n \in \mathbb{N}$, por lo que G es finito.

Veamos ahora que $|G|$ es primo. Si no lo fuese, tendríamos $|G| = nm$. Entonces $\{1\} \neq \langle x^m \rangle < G$, por lo que G tendría subgrupos propios, luego no sería simple. Por tanto, $|G|$ ha de ser primo.

□

Ejemplo. Estudiando un poco el caso de grupos cíclicos infinitos, $\mathbb{Z}$ no es simple, ya que tiene subgrupos propios (que además son normales, por ser $\mathbb{Z}$ abeliano).

Proposición 4.2 (Caracterización de series de composición)**.** *Sea G un grupo, una serie normal es de composición si y solo si sus factores son grupos simples.*

Demostración. Consideramos una serie normal de longitud r:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$

Y demostraremos que la serie no es de composición si y solo si tiene un factor que no es un grupo simple:

$\Longrightarrow$) Si la serie no es de composición, podemos encontrar $H < G$ de forma que la serie:

$$G = G_0 \rhd \ldots \rhd G_{k-1} \rhd H \rhd G_k \rhd \ldots \rhd G_r = \{1\}$$

Sea un refinamiento normal propio de la serie de partida. Si consideramos la proyección al cociente $p_k : G_{k-1} \to G_{k-1}/G_k$ de los grupos:

$$G_{k-1} \rhd H \rhd G_k$$

Llegamos por el Tercer Teorema de Isomorfía a que:

$$p_*(G_{k-1}) = G_{k-1}/G_k \rhd p_*(H) = H/G_k \rhd p_*(G_k) = \{G_k\}$$

Y ninguna de estas inclusiones es una igualdad, ya que (como los subgrupos de G_{k-1} que contienen a G_k son biyectivos con los subgrupos de G_{k-1}/G_k):

- Si $G_{k-1}/G_k = H/G_k$, entonces $G_{k-1} = H$ y el refinamiento anterior no era propio.
- Si $H/G_k = \{G_k\}$, entonces $H = G_k$ y el refinamiento anterior no era propio.

En definitiva, hemos encontrado un subgrupo normal propio de G_{k-1}/G_k, por lo que este factor no es un grupo simple.

$\Longleftarrow$) Si existe $k \in \{1, \ldots, r\}$ de forma que G_{k-1}/G_k no es un grupo simple, entonces dicho grupo tendrá un subgrupo propio normal suyo:

$$\{G_k\} = \{1\} \neq H \lhd G_{k-1}/G_k$$

Si usamos el Tercer Teorema de Isomorfía considerando la proyección al cociente $p_k : G_{k-1} \to G_{k-1}/G_k$, tenemos que:

$$p_k^*(H) \lhd G_{k-1}$$

Además, como $H < G_{k-1}/G_k$, tendremos que $G_k \in H$, luego:

$$G_k = \ker(p_k) = p_k^*(\{G_k\}) \subseteq p_k^*(H) \lhd G_{k-1}$$

Y por ser $G_k \lhd G_{k-1}$, deducimos que también $G_k \lhd p_k^*(H)$. Hemos encontrado un subgrupo normal de G que estaría entre G_k y G_{k-1}:

$$G = G_0 \rhd \ldots \rhd G_{k-1} \rhd p_k^*(H) \rhd G_k \rhd \ldots \rhd G_r = \{1\}$$

Además, este refinamiento de la serie normal es propio, ya que (como p_k^* es una biyección):

- Si fuese $p_k^*(H) = G_k$, tendríamos que $H = \{G_k\}$.
- Si fuese $p_k^*(H) = G_{k-1}$, tendríamos que $H = G_{k-1}/G_k$.

Ambos casos son imposibles, puesto que H era un subgrupo propio de G_{k-1}/G_k. Hemos encontrado un refinamiento normal propio de la serie de partida, por lo que esta no era de composición.

□

Proposición 4.3. *Todo grupo finito tiene una serie de composición.*

Demostración. Sea G un grupo finito, distinguimos casos:

- Si G es simple o trivial, entonces no tiene subgrupos normales propios, por lo que tiene una única serie de composición:

$$G \rhd \{1\}$$

- Si $|G| = p$ primo, la Proposición 4.1 nos dice que G es simple, por lo que estamos en el caso anterior.

- Si $|G|$ no es primo y G no es simple, por inducción sobre $n = |G|$, suponemos que es cierto para todo grupo H con $|H| < |G|$ (observemos que el punto anterior nos sirve como caso base).

  Como G es finito, tiene un número finito de subgrupos, entre los que podemos encontrar (por ser G no simple) G_1, un subgrupo normal propio maximal[1] de G. Como $|G_1| < |G|$ (G_1 es subgrupo propio), por hipótesis de inducción tenemos una serie de composición para G_1:

$$G_1 \rhd G_2 \rhd \ldots \rhd G_r = \{1\}$$

  Además, como G_1 era el subgrupo normal maximal de G, sabemos que no existe $H \lhd G$ con $G_1 \lhd H \lhd G$, por lo que la serie:

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_r = \{1\}$$

  Es de composición. □

Teorema 4.4 (de Refinamiento de Schreier)**.** *Sea G un grupo, dos series normales de G tienen refinamientos isomorfos.*

Demostración. Consideramos dos series normales de G:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_{i-1} \rhd G_i \rhd \ldots \rhd G_r = \{1\} \tag{4.3}$$

$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_{j-1} \rhd H_j \rhd \ldots \rhd H_s = \{1\} \tag{4.4}$$

Fijado $i \in \{1, \ldots, r\}$, tenemos $G_i \lhd G_{i-1} < G$, y para todo $j \in \{1, \ldots, s\}$ tenemos $H_j \lhd H_{j-1} < G$, donde podemos aplicar el primer apartado del Cuarto Teorema de Isomorfía, obteniendo la siguiente relación entre los grupos:

$$G_{ij} = G_i(H_j \cap G_{i-1}) \lhd G_i(H_{j-1} \cap G_{i-1}) = G_{ij-1} \qquad \forall j \in \{1, \ldots, s\}$$

En los casos extremos (es decir, en $j = 0$ y $j = s$), tendremos:

$$\begin{aligned} G_{i0} &= G_i(H_0 \cap G_{i-1}) = G_iG_{i-1} = G_{i-1} \\ G_{is} &= G_i(H_s \cap G_{i-1}) = G_i\{1\} = G_i \end{aligned}$$

De esta forma, tenemos para todo $i \in \{1, \ldots, r\}$ que:

$$G_{i-1} = G_{i0} \rhd G_{i1} \rhd \ldots \rhd G_{is-1} \rhd G_{is} = G_i$$

Que podemos meter en todos los eslabones de la serie (4.3):

$$\begin{aligned} G = G_0 = G_{10} \rhd G_{11} \rhd \ldots \rhd G_{1s} = G_1 = G_{20} \rhd G_{21} \rhd \ldots \rhd G_{2s} = G_2 = G_{30} \rhd \ldots \\ \ldots \rhd G_{r-1s} = G_{r-1} = G_{r0} \rhd \ldots \rhd G_{rs} = G_r = \{1\} \end{aligned}$$

Obteniendo un refinamiento de longitud $r(s + 1) - (r - 1) = rs + 1$:
En cada eslabón (teníamos r) hemos metido $s + 1$ eslabones, de los que se repetían ($G_{is} = G_{i+1,0}$, para $i \in \{0, \ldots, r - 1\}$) $r - 1$ eslabones.

[1]Es decir, que no existe $G_1 \neq K \lhd G$ con $G_1 \lhd K$.

Si repetimos el procedimiento para la serie (4.4), fijado $j \in \{1, \ldots, s\}$, para todo $i \in \{0, \ldots, r\}$ podemos aplicar el primer apartado del Cuarto Teorema de Isomorfía, obteniendo que:

$$H_{ij} = H_j(G_i \cap H_{j-1}) \lhd H_j(G_{i-1} \cap H_{j-1}) = H_{i-1j} \qquad \forall i \in \{1, \ldots, r\}$$

En los casos extremos tendremos:

$$\begin{aligned} H_{0j} &= H_{j-1} \\ H_{rj} &= H_j \end{aligned}$$

Por lo que para todo $j \in \{1, \ldots, s\}$, tenemos:

$$H_{j-1} = H_{0j} \rhd H_{1j} \rhd \ldots \rhd H_{r-1j} \rhd H_{rj} = H_j$$

Y podemos obtener un refinamiento de (4.4) al igual que hicimos antes, metiendo la cadena superior entre cada uno de los eslabones de la serie original:

$$\begin{aligned} G = H_0 = H_{01} \rhd H_{11} \rhd \ldots \rhd H_{r1} = H_1 = H_{02} \rhd H_{12} \rhd \ldots \rhd H_{r2} = G_2 = H_{03} \rhd \ldots \\ \ldots \rhd H_{rs-1} = H_{s-1} = H_{0s} \rhd H_{1s} \rhd \ldots \rhd H_{rs} = H_s = \{1\} \end{aligned}$$

Que tiene longitud $s(r+1) - (s-1) = rs + 1$, al igual que antes.

Ahora, por la segunda parte del Cuarto Teorema de Isomorfía, tenemos que:

$$\frac{G_{ij-1}}{G_{ij}} = \frac{G_i(H_j \cap G_{i-1})}{G_i(H_j \cap G_{i-1})} \cong \frac{H_j(G_{i-1} \cap H_{j-1})}{H_j(G_i \cap H_{j-1})} = \frac{H_{i-1j}}{H_{ij}}$$

Por lo que los dos refinamientos encontrados son isomorfos. □

Ejercicio. Se pide calcular un refinamiento isomorfo aplicando el método de Schreier a las dos siguientes series normales:

$$\begin{aligned} G &= G_0 \rhd G_1 \rhd G_2 \rhd G_3 = \{1\} \\ G &= H_0 \rhd H_1 \rhd H_2 = \{1\} \end{aligned}$$

Teorema 4.5 (Jordan-Holder)**.** *Si un grupo G admite una serie de composición, cualquier serie normal puede refinarse a una serie de composición.*

Además, dos series de composición de un mismo grupo son isomorfas siempre.

Demostración. Tomamos una serie de composición de G:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$

Y también una serie normal de G:

$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_s = \{1\}$$

Por el Teorema de Schreier (la serie de composición es normal), existe un refinamiento de ambos isomorfo. Sin embargo, como la primera serie de de composición, no podrá tener un refinamiento propio, por lo que el refinamiento obtenido es impropio (es decir, o tenemos la misma serie o hemos añadido repeticiones de un grupo que aparece como eslabón de la serie, en este caso podemos simplemente eliminar las repeticiones que aparezcan tanto en esta serie como en la otra). Para la segunda serie, obtendremos un refinamiento isomorfo a la primera:

$$G = \overline{G_0} \rhd \overline{G_1} \rhd \ldots \rhd \overline{G_r} = \{1\}$$

Por tanto, tendremos que $\exists \sigma \in S_r$ de forma que:

$$G_k/G_{k+1} \cong \overline{G}_{\sigma(k)}/\overline{G}_{\sigma(k)+1} \qquad \forall k \in \{0, \ldots, r-1\}$$

Como la primera serie era de composición, los factores G_k/G_{k+1} son simples, y como esta propiedad se conserva por isomorfismos (compruébese), los factores $\overline{G}_k/\overline{G}_{k+1}$ también serán simples, de donde deducimos que el refinamiento de la serie normal que hemos encontrado es de composición. □

Con este último Teorema de Jordan-Holder se tiene claro ya el interés en las series de composición, ya que cada grupo admite un única (salvo isomorfismos) serie de composición.

Podemos pensar en calcular series de composición de un grupo conocida una serie de composición en un grupo isomorfo, resultado que podemos esperar que sea cierto (y que de hecho vamos a probar a continuación); sin embargo, el recíproco no es cierto en general: si tenemos dos series de composición isomorfas, una de un grupo G y otra de otro grupo K, en general G y K no van a ser isomorfos.

Ejemplo. Por ejemplo, anteriormente vimos en un ejemplo que la única serie de composición que podemos considerar en S_3 es:

$$S_3 \overset{2}{\rhd} A_3 \overset{3}{\rhd} \{1\}$$

En $\mathbb{Z}_6$, que no es isomorfo a S_3 por ser abeliano, si observamos su retículo:

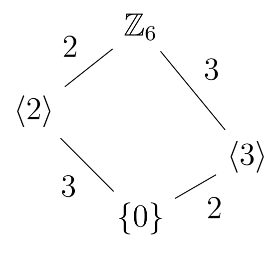


Figura 4.4: Diagrama de Hasse para los subgrupos de $\mathbb{Z}_6$.

Vemos que una serie de composición de $\mathbb{Z}_6$ es:

$$\mathbb{Z}_6 \overset{2}{\rhd} \langle 2 \rangle \overset{3}{\rhd} \{0\}$$

Además, sabemos ahora por el Teorema de Jordan-Holder que toda serie de composición de $\mathbb{Z}_6$ ha de ser isomorfa a esta. Otra posibilidad a contemplar podría haber sido (como estamos en un grupo abeliano, cualquier grupo es normal):

$$\mathbb{Z}_6 \overset{3}{\rhd} \langle 3 \rangle \overset{2}{\rhd} \{0\}$$

Y como vemos por los índices, es isomorfa a la otra serie. Vemos finalmente que las series:

$$S_3 \overset{2}{\rhd} A_3 \overset{3}{\rhd} \{1\}$$
$$\mathbb{Z}_6 \overset{2}{\rhd} \langle 2 \rangle \overset{3}{\rhd} \{0\}$$

son isomorfas. Para ello, basta ver que:

$$S_3/A_3 \cong \mathbb{Z}_2 \cong Z_6/\langle 2 \rangle$$
$$A_3/\{1\} \cong A_3 \cong \mathbb{Z}_3 \cong \langle 2 \rangle \cong \langle 2 \rangle/\{0\}$$

Veamos ahora que dos grupos isomorfos siempre tienen una serie de composición isomorfa. Sin embargo, antes de ello, hemos de destacar un resultado que no vimos en el Capítulo anterior pero que puede demostrarse fácilmente con las herramientas introducidas en el mismo.

Lema 4.6. *Sean G y K dos grupos, $f : G \to K$ un isomorfismo de grupos y $H \lhd G$, entonces:*

$$G/H \cong K/f_*(H)$$

Demostración. En primer lugar, hemos de demostrar que $f_*(H) \lhd K$. Para ello:

- Como $H < G$ y f es un homomorfismo, por la Proposición 2.3, tenemos que $f_*(H) < K$.
- Ahora, si $y \in K$ y $h' \in f(H)$, existirán $x \in G$ y $h \in H$ de forma que:

  $$f(x) = y \qquad f(h) = h'$$

  En cuyo caso:

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

  Ya que por ser $H \lhd G$, tenemos que $xhx^{-1} \in H$.

Ahora, podemos considerar los grupos cocientes G/H y $K/f_*(H)$, junto con las proyecciones $p_G : G \to G/H$ y $p_K : K \to K/f_*(H)$. Si definimos $g : G \to K/f_*(H)$ como $g = p_K \circ f$:

$$g(x) = p_K(f(x)) = f(x)f_*(H) \qquad \forall x \in G$$

Es un homomorfismo, como composición de homomorfismos. Si observamos el siguiente diagrama:

$$\begin{tikzcd}
G \arrow[r, "p_G"] \arrow[d, "f"'] \arrow[dr, "g"] & G/H \arrow[d, dashed, "\varphi"] \\
K \arrow[r, "p_K"] & K/f_*(H)
\end{tikzcd}$$

Figura 4.5: Situación de los grupos.

Podemos aplicar la Propiedad Universal del grupo cociente sobre g, obteniendo que existe un único homomorfismo $\varphi : G/H \to K/f_*(H)$ que hace que el diagrama conmute. Como vimos en el Teorema 3.8:

- Como g es sobreyectiva por ser composición de aplicaciones sobreyectivas, tenemos que φ es sobreyectiva.

- Calculemos $\ker(g)$, sea $x \in \ker(g)$:

$$f(x)f_*(H) = p_K(f(x)) = g(x) = f_*(H)$$

Entonces, $f(x) \in f_*(H)$, de donde $x \in H$. La inclusión $H \subseteq \ker(g)$ es clara, por lo que $H = \ker(g)$, de donde deducimos que φ es inyectiva.

□

Proposición 4.7. *Sean G y K dos grupos isomorfos, entonces todas las series de composición de G son isomorfas a todas las series de composición de K.*

Demostración. Como todas las series de composición de G son isomorfas entre sí y todas las series de composición de K también (por el Teorema de Jordan-Holder), basta ver que hay una serie de composición de G que es isomorfa a una serie de composición de K. Para ello, como $G \cong K$, ha de existir un isomorfismo de grupos $f : G \to K$. Sea

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$

una serie de composición de G, si denotamos:

$$H_k = f_*(G_k) \qquad \forall k \in \{0, \ldots, r\}$$

Tendremos entonces una serie normal en K:

$$K = H_0 \rhd H_1 \rhd \ldots \rhd H_r = \{1\}$$

Por el Lema anterior, tenemos que:

$$G_k/G_{k+1} \cong H_k/H_{k+1} \qquad \forall k \in \{0, \ldots, r-1\}$$

Además, como la serie de G era de composición, sus factores serán grupos simples, de donde los factores H_k/H_{k+1} serán también grupos simples, por lo que la serie obtenida en K es de composición, y son series isomorfas. □

El objetivo principal de esta asignatura es clasificar los grupos finitos. Como estos grupos van a tener series de composición cuyos factores serán grupos simples, nos centraremos en clasificar los grupos simples, para luego clasificar los grupos finitos.

La teoría de clasificación de grupos simples comenzó en 1960 y fue completada en 2004, con una demostración de 15000 páginas en lo que se conoce como el "Teorema enorme". En la demostración intervinieron matemáticos como Gorestein (1923 - 1992). Esta clasificación de los grupos simples se hizo en:

- 18 familias infinitas de grupos simples.

- 26 grupos simples, llamados grupos esporádicos.

  Como curiosidad, el grupo esporádico más pequeño tiene orden 7920 y el más grande, 10^{54}.

Cualquier grupo finito simple pertenece a una de estas 18 familias, o es isomorfo a alguno de los 26 grupos esporádicos.

Entre las 18 familias de grupos simples destacamos 2, que son las que nos interesan por ahora:

- Los grupos cíclicos de orden primo, que ya hemos demostrado que se tratan de grupos simples.
- Los grupos alternados A_n con $n \geqslant 5$.

Veremos ahora este segundo resultado, en el ya prometido Teorema de Abel.

Teorema 4.8 (de Abel)**.** *A_n es simple, para $n \geqslant 5$.*

Demostración. Sea $\{1\} \neq N \lhd A_n$, veamos que ha de ser $N = A_n$. En la Proposición 1.20 vimos que dado[2] $j \in X_n \setminus \{1, 2\}$, teníamos que:

$$A_n = \langle (1\ 2\ j) \rangle$$

Y la demostración terminará viendo que N contiene a un elemento de esta forma. Bajo estas hipótesis, sabemos que va a existir (por ser N finito) $1 \neq \sigma \in N$, la permutación de N que mueve menos elementos. Por ser σ par (estamos en A_n), ha de mover más de dos elementos. Veamos que mueve exactamente 3:

1. Si σ es producto de ciclos disjuntos de longitud 2: supongamos que σ mueve, al menos, los elementos x_1, x_2, x_3 (distintos entre sí), con lo que podemos escribir:

   $$\sigma = (x_1\ x_2)(x_3\ x_4)\dots$$

   Sea $\tau = (x_3\ x_4\ x_5)$ para ciertos $x_4, x_5 \in X_n$ distintos de x_1, x_2, x_3 y distintos entre sí, definimos:

   $$\sigma_1 = (x_3\ x_4\ x_5)\sigma(x_3\ x_4\ x_5)^{-1} \in N$$

   σ_1 está en N por ser $N \lhd A_n$. Si consideramos:

   $$[\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1} = \sigma_1\sigma^{-1} \in N$$

   - Supongamos que σ mueve a x_5, en cuyo caso:

     $$\begin{aligned} \sigma &= (x_1\ x_2)(x_3\ x_4)(x_5\ \sigma(x_5))\dots \\ \sigma_1 &= (x_1\ x_2)(x_3\ \sigma(x_5))(x_4\ x_5)\dots \end{aligned}$$

     Con lo que:

     $$[\tau, \sigma] = (x_3\ \sigma(x_5))(x_4\ x_5)(x_3\ x_4)(x_5\ \sigma(x_5))$$

     Luego $[\tau, \sigma]$ deja fijos a x_1 y x_2 y mueve a los mismos que movía σ. Por ello, $[\tau, \sigma] \in N$ y $[\tau, \sigma]$ mueve menos elementos que σ, contradicción, que viene de suponer que σ mueve a x_5.

[2] Donde $X_n = \{1, 2, \dots, n\}$.

- Si suponemos que σ no mueve a x_5:

$$\sigma_1 = (x_1\ x_2)(x_4\ x_5)$$

Tenemos:

$$[\tau, \sigma] = (x_3\ x_5\ x_4)$$

Que mueve menos elementos que σ, contradicción.

Por tanto, σ no puede ser producto de transposiciones, ya que llegamos a contradicciones.

2. Si σ tiene un ciclo de longitud mayor o igual que 3 en el que mueve a x_1, x_2 y x_3, si definimos:

$$\tau = (x_3\ x_4\ x_5)$$
$$\sigma_1 = \tau\sigma\tau^{-1} \in N$$

Supongamos que σ mueve más de 3 elementos, por lo que mueve al menos (por ser una permutación par) 5. En dicho caso:

$$\sigma_1 = (x_1\ x_2\ x_4\ \ldots) \neq \sigma$$

Por lo que:

$$[\tau, \sigma] = \sigma_1\sigma^{-1} \in N$$

Y $[\tau, \sigma]$ deja fijos a los mismos que σ y a x_2. En dicho caso, tenemos que $[\tau, \sigma]$ mueve menos que σ.

En definitiva, concluimos que σ contiene a un ciclo de longitud 3, a saber: $(i\ j\ k)$, todos ellos elementos distintos.

- Si $i, j, k, 1, 2$ son todos distintos:

$$(1\ i)(2\ j)(i\ j\ k)(1\ i)(2\ j) = (1\ 2\ k) \in N$$

- Si $i = 1$ y $j, k, 2$ fueran distintos, $\exists h$ distinto de los anteriores de forma que:

$$(2\ j)(k\ h)(1\ j\ k)(2\ j)(k\ h) = (1\ 2\ h) \in N$$

- Si $i = 2$ y $j, k, 1$ fueran distintos, $\exists h$ distinto de los anteriores de forma que:

$$(1\ j)(k\ h)(j\ 2\ k)(1\ j)(k\ h) = (1\ 2\ h) \in N$$

En definitiva, N contiene al generador de A_n, de donde:

$$A_n = \langle (1\ 2\ j) \rangle \subseteq N$$

□

4.2. Grupos resolubles

Antes de pasar con la definición de grupos resolubles, hemos de repasar ciertos conceptos relacionados con la operación de conmutador que ya definimos sobre los elementos de G, recordamos que era la aplicación $[\cdot,\cdot] : G \times G \to G$ dada por:

$$[x,y] = xy(yx)^{-1} = xyx^{-1}y^{-1} \qquad \forall x,y \in G$$

4.2.1. Preliminares

Sobre el conmutador solo vimos la Proposición 3.27, que nos decía que dados dos elementos h,k de un grupo G:

$$hk = kh \iff [h,k] = 1$$

Proposición 4.9. *Sea G un grupo y $x,y \in G$, se verifican:*

i) $[x,y]^{-1} = [y,x]$.

ii) $z[x,y]z^{-1} = [zxz^{-1}, zyz^{-1}]$, $\forall z \in G$.

Demostración. Veamos cada apartado:

i) Basta con ver:

$$[x,y][y,x] = xy(yx)^{-1}yx(xy)^{-1} = xy(xy)^{-1} = 1$$

ii) Sea $z \in G$, basta aplicar la definición del conmutador:

$$\begin{aligned} z[x,y]z^{-1} &= zxy(yx)^{-1}z^{-1} = zxy(x^{-1}y^{-1}z^{-1}) \\ [zxz^{-1}, zyz^{-1}] &= zxz^{-1}zyz^{-1}(zyz^{-1}zxz^{-1})^{-1} = zxyz^{-1}(zx^{-1}y^{-1}z^{-1}) \\ &= zxy(x^{-1}y^{-1}z^{-1}) \end{aligned}$$

□

Proposición 4.10. *Sea G un grupo, el conjunto:*

$$\langle [x,y] \mid x,y \in G \rangle$$

es un subgrupo normal de G.

Demostración. Llamando Λ a dicho conjunto, por la definición de subgrupo generado por un subconjunto, es claro que $\Lambda < G$. Para ver la normalidad, sea $\lambda \in \Lambda$ y $z \in G$, existirán $x_1,\ldots,x_n,y_1,\ldots,y_n \in G$ y $\gamma_1,\ldots,\gamma_n \in \{\pm 1\}$ de forma que:

$$\lambda = ([x_1,y_1])^{\gamma_1} \ldots ([x_n,y_n])^{\gamma_n}$$

Por lo que:

$$\begin{aligned} z\lambda z^{-1} = z([x_1,y_1])^{\gamma_1} \ldots ([x_n,y_n])^{\gamma_n} z^{-1} &= z([x_1,y_1])^{\gamma_1} z^{-1}z \ldots z^{-1}z([x_n,y_n])^{\gamma_n} z^{-1} \\ &= ([zx_1z^{-1}, zy_1z^{-1}])^{\gamma_1} \ldots ([zx_nz^{-1}, zy_nz^{-1}])^{\gamma_n} \end{aligned}$$

Ya que para los γ_k positivos tendremos que:

$$z([x_k, y_k])^{\gamma_k} z^{-1} = [zx_k z^{-1}, zy_k z^{-1}] = ([zx_k z^{-1}, zy_k z^{-1}])^{\gamma_k}$$

Y para los γ_k negativos tendremos:

$$z([x_k, y_k])^{\gamma_k} z^{-1} = [zy_k z^{-1}, zx_k z^{-1}] = ([zx_k z^{-1}, zy_k z^{-1}])^{\gamma_k}$$

□

Definición 4.8 (Subgrupo conmutador)**.** Sea G un grupo, llamamos subgrupo conmutador de G al subgrupo:

$$[G, G] = \langle [x, y] \mid x, y \in G\rangle$$

Observemos que como $hk = kh \iff [h, k] = 1$, este grupo está generado por los conmutadores de los elementos que no conmutan entre sí:

$$[G, G] = \langle [x, y] \mid xy \neq yx\rangle$$

Proposición 4.11. *Sea G un grupo, $G/[G, G]$ es abeliano. Más aún, es el menor subgrupo normal de G que hace que el cociente sea abeliano. Es decir, si $N \lhd G$:*

$$G/N \text{ es abeliano} \iff [G, G] < N$$

$G/[G, G]$ recibe el nombre de grupo abelianizado de G.

Demostración. Si demostramos la doble implicación, como $[G, G] < [G, G]$, tendremos que $G/[G, G]$ es abeliano, por lo que solo tenemos que probar esto:

$\Longrightarrow$) Si consideramos la proyección al cociente $p : G \to G/N$, sean $x, y \in G$, observemos que:

$$\begin{aligned} p([x, y]) = p\left(xy(yx)^{-1}\right) &= p(xy)p\left((yx)^{-1}\right) = p(x)p(y)(p(yx))^{-1} \\ &= p(x)p(y)(p(y)p(x))^{-1} \overset{(*)}{=} p(x)p(y)(p(y))^{-1}(p(x))^{-1} = 1 \end{aligned}$$

Donde en $(*)$ hemos usado que G/N es abeliano. De esta forma, vemos que $[x, y] \in \ker(p) = N$, para todo $x, y \in G$, de donde $[G, G] < N$.

$\Longleftarrow$) Sean $x, y \in G$, entonces:

$$xy(yx)^{-1} = [x, y] \in [G, G] < N$$

Por lo que $xy(yx)^{-1}N = N$, y si multiplicamos por yxN a la derecha obtenemos que:

$$(xN)(yN) = xyN = yxN = (yN)(xN)$$

Como x e y eran arbitrarios, concluimos que G/N es abeliano.

□

Corolario 4.11.1. *Si G es un grupo:*

$$G \text{ abeliano} \iff [G, G] = \{1\}$$

Demostración. Como $G \cong G/\{1\}$:

$$G \text{ abeliano} \iff G/\{1\} \text{ abeliano} \iff [G,G] < \{1\} \iff [G,G] = \{1\}$$

□

Lema 4.12. *Sea B un grupo y $A < B$, entonces $[A,A] < [B,B]$.*

Demostración. Por la definición del subgrupo conmutador, si definimos:

$$S_A = \{[x,y] \mid x,y \in A\}$$
$$S_B = \{[x,y] \mid x,y \in B\}$$

De la relación $A \subseteq B$ tenemos que $S_A \subseteq S_B$, y como:

$$[A,A] = \langle S_A \rangle \qquad [B,B] = \langle S_B \rangle$$

Tendremos que $[A,A] \subseteq [B,B]$, de donde $[A,A] < [B,B]$. □

4.2.2. Definición

Definición 4.9 (Serie derivada)**.** La serie derivada de un grupo G es la cadena de subgrupos normales:

$$G = G^0 \rhd G' \rhd G'' \rhd \ldots \rhd G^{(k)} \rhd \ldots$$

Donde:

$$G^{(k+1)} = [G^{(k)}, G^{(k)}] \qquad \forall k \in \mathbb{N}$$

De esta forma, el subgrupo $G' = [G,G]$ recibe el nombre de subgrupo derivado de G, o primer derivado de G.

Un grupo G se dice <u>resoluble</u> si existe un índice k de forma que $G^{(k)} = \{1\}$. Es decir, la serie derivada de G alcanza el $\{1\}$.

Ejemplo. Veamos algunos ejemplos de conmutadores de ciertos grupos, los cuales usaremos a lo largo de este capítulo:

- $[A_3, A_3] = \{1\}$.

  Como A_3 es abeliano (de hecho es cíclico), tenemos por el Corolario 4.11.1 que $[A_3, A_3] = \{1\}$.

- $[A_4, A_4] = V$.

  Si observamos el retículo de subgrupos de A_4, veremos que los únicos subgrupos normales de A_4 son $\{1\}$, V y A_4, y como el conmutador es el menor subgrupo que hace que el cociente sea abeliano:

  - $A_4/\{1\} \cong A_4$, que no es abeliano.
  - $A_4/V \cong \mathbb{Z}_3$, que es abeliano.

  Concluimos que $[A_4, A_4] = V$.

- $[S_n, S_n] = A_n$ para $n \geqslant 3$.

  $\subseteq$) Como $S_n/A_n \cong \mathbb{Z}_2$ es abeliano, tenemos por la Proposición 4.11 que $[S_n, S_n] < A_n$.

  $\supseteq$) Como $A_n = \langle\{(x\ y\ z)\}\rangle$, para ver esta inclusión basta ver que los generadores están en $[S_n, S_n]$. Para ello, basta observar que:

  $$[(x\ z), (z\ y)] = (x\ z)(z\ y)(x\ z)(z\ y) = (x\ y\ z)$$

  Por lo que todos los 3−ciclos están en $[S_n, S_n]$, luego $A_n < [S_n, S_n]$.

Ejemplo. Veamos ejemplos de grupos que son resolubles, y de algunos que no lo son.

- Si G es abeliano, entonces G es resoluble, ya que:

  $$G' = [G, G] = \{1\}$$

  Por lo que la serie derivada de cualquier grupo abeliano G es:

  $$G \rhd G' = \{1\}$$

- S_3 es resoluble, ya que:

  $$S_3' = [S_3, S_3] = A_3$$
  $$S_3'' = A_3' = [A_3, A_3] = \{1\}$$

  Y la serie derivada es:

  $$S_3 \rhd A_3 \rhd \{1\}$$

- A_4 es resoluble:

  $$A_4' = [A_4, A_4] = V$$
  $$A_4'' = V' = [V, V] = \{1\}$$

  Y la serie derivada es:

  $$A_4 \rhd V \rhd \{1\}$$

- S_4 es resoluble, ya que $S_4' = [S_4, S_4] = A_4$ y ya tenemos la serie de A_4:

  $$S_4 \rhd A_4 \rhd V \rhd \{1\}$$

  En general, si G es un grupo de forma que su $k-$ésimo grupo derivado es resoluble para cierto $k \in \mathbb{N}$, entonces G será resoluble.

- A_5 no es resoluble:

  $$A_5' = [A_5, A_5] \neq \{1\}$$

  Ya que A_5 no es abeliano, pero como A_5 es simple, no tiene subgrupos normales propios, con lo que ha de ser $A_5' = A_5$. La serie derivada será por tanto:

  $$A_5 \rhd A_5 \rhd A_5 \rhd \dots$$

  En general, ningún grupo no abeliano y simple es resoluble.

- S_n no es resoluble para $n \geqslant 5$, ya que:

$$[S_n, S_n] = A_n \qquad \forall n \geqslant 3$$

Y como ya vimos lo que le pasa a A_n para $n \geqslant 5$ (ya que por el Teorema de Abel todos ellos son simples), la serie derivada de S_n será:

$$S_n \rhd A_n \rhd A_n \rhd \ldots$$

Teorema 4.13 (Caracterización de grupos resolubles para grupos finitos)**.**
Si G es un grupo finito, son equivalentes:

i) *G es resoluble.*

ii) *G tiene una serie normal con factores abelianos.*

iii) *Los factores de composición de G son cíclicos de orden primo.*

iv) *G tiene una serie normal con factores cíclicos.*

Demostración. Veamos todas las implicaciones:

i) $\Longrightarrow$ *ii)* Si G es resoluble, la serie derivada será de la forma:

$$G = G^0 \rhd G' \rhd \ldots \rhd G^{(r)} = \{1\}$$

Que es una serie normal con factores abelianos, ya que los factores son de la forma:

$$G^{(k-1)}/G^{(k)} = G^{(k-1)}/\left[G^{(k-1)}, G^{(k-1)}\right]$$

Que ya vimos en la Proposición 4.11 que siempre era un grupo abeliano.

ii) $\Longrightarrow$ *iii)* Si tenemos una serie normal con factores abelianos:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_s = \{1\}$$

Por el Teorema de Jordan-Holder, podemos refinarla a una serie de composición, donde nos fijaremos ahora en lo que pasa entre dos eslabones de la serie original:

$$\ldots \rhd G_r \rhd H_{r1} \rhd H_{r2} \rhd \ldots \rhd H_{rs} \rhd G_{r+1} \rhd \ldots$$

Por hipótesis los factores son abelianos, es decir, los grupos:

$$G_{k-1}/G_k \qquad \forall k \in \{1, \ldots, s\}$$

son abelianos. Por consiguiente, como todo subgrupo de un grupo abeliano también es abeliano, tenemos que los siguientes cocientes también son abelianos:

$$H_{r1}/G_{r+1} \quad H_{r2}/G_{r+1} \quad \cdots \quad H_{rs}/G_{r+1} \quad < \quad G_r/G_{r+1}$$

Por tanto, los factores:

$$\begin{aligned}
G_r/H_{r1} &\cong \frac{G_r/G_{r+1}}{H_{r1}/G_{r+1}} \\
H_{r1}/H_{r2} &\cong \frac{H_{r1}/G_{r+1}}{H_{r2}/G_{r+1}} \\
&\vdots \\
H_{rs-1}/H_{rs} &\cong \frac{H_{rs-1}/G_{r+1}}{H_{rs}/G_{r+1}}
\end{aligned}$$

Son abelianos, por ser isomorfos a un cociente de un grupo abeliano. En definitiva, todos los factores de composición son abelianos, finitos y simples (por ser factores de composición), luego son cíclicos de orden primo, por la Proposición 4.1.

iii) $\Longrightarrow$ *iv)* Como las series de composición son, en particular, series normales, cualquier[3] serie de composición de G será normal con factores cíclicos.

iv) $\Longrightarrow$ *i)* Consideramos una serie normal con factores cíclicos:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$

Donde los grupos G_k/G_{k+1} son cíclicos, para todo $k \in \{0, \ldots, r-1\}$, luego abelianos. Veamos que $G^{(k)} < G_k$, para todo $k \in \{1, \ldots, r\}$:

- Para $k = 1$: como el cociente G/G_1 es abeliano, tenemos por la Proposición 4.11 que $G' = [G, G] < G_1$.
- Supuesto que $G^{(k)} < G_k$, veámoslo para $k + 1$: Como tenemos por hipótesis que $G^{(k)} < G_k$, si consideramos el grupo derivado a ambos lados gracias al Lema 4.12, tendremos que:

  $$G^{(k+1)} = (G^{(k)})' < G'_k = [G_k, G_k]$$

  Y finalmente, como el cociente G_k/G_{k+1} es abeliano, deducimos por la Proposición anterior que $G'_k = [G_k, G_k] < G_{k+1}$. En definitiva, tenemos $G^{(k+1)} < G_{k+1}$.

Una vez probado esto, en particular, tenemos que:

$$G^{(r)} < G_r = \{1\}$$

De donde deducimos que el $r-$ésimo grupo derivado de G es trivial, con lo que G es resoluble.

□

Observación. Notemos que en el Teorema superior podríamos haber demostrado que *i)* $\Longleftrightarrow$ *ii)* para cualquier grupo G (no necesariamente finito):

[3] Gracias al Teorema de Jordan-Holder.

- En la demostración $i) \Longrightarrow ii)$ no se usó que G era finito.
- En la demostración $iv) \Longrightarrow i)$ en realidad no se usó que G tuviera una serie normal con factores cíclicos, sino que las hipótesis pueden relajarse a que G tenga una serie normal con factores abelianos. Además, en esta tampoco usamos que G era finito.

Ejemplo. Aplicaciones del Teorema son:

- Vimos ya que S_4 era resoluble, veámoslo de otra forma:
$$S_4 \rhd A_4 \rhd V \rhd \{1\}$$
Es una serie normal con factores abelianos:
$$S_4/A_4 \cong \mathbb{Z}_2 \qquad A_4/V \cong \mathbb{Z}_3 \qquad V/\{1\} \cong V \text{ abeliano}$$
- En D_n:
$$D_n \rhd \langle r \rangle \rhd \{1\}$$
Es una serie normal con factores abelianos, luego D_n es resoluble.

Proposición 4.14. *Sea G un grupo resoluble y $f : G \to H$ un homomorfismo, entonces $f(G)$ es resoluble.*

Demostración. Como G es resoluble, entonces tendrá una serie normal con factores abelianos:
$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{1\}$$
Como la imagen de grupos normales por homomorfismos conservan la normalidad (compruébese), tenemos:
$$f(G) = f(G_0) \rhd f(G_1) \rhd f(G_2) \rhd \cdots \rhd f(G_n) = f(\{1\}) = \{1\}$$
Veamos ahora que $f(G_k)/f(G_{k+1})$ es abeliano para todo $k \in \{0, \ldots, n-1\}$. Como G_k/G_{k+1} es abeliano, para cada par $x_1, x_2 \in G_k$ se tiene que:
$$\begin{aligned}
x_1x_2G_{k+1} = x_2x_1G_{k+1} &\Longrightarrow x_1x_2(x_2x_1)^{-1} \in G_{k+1} \\
&\Longrightarrow f(x_1x_2(x_2x_1)^{-1}) = f(x_1x_2)f(x_2x_1)^{-1} \in f(G_{k+1}) \\
&\Longrightarrow f(x_1x_2)f(G_{k+1}) = f(x_2x_1)f(G_{k+1}) \\
&\Longrightarrow f(x_1)f(x_2)f(G_{k+1}) = f(x_2)f(x_1)f(G_{k+1})
\end{aligned}$$
Por tanto, $f(G)$ es resoluble. □

Una estrategia muy usada a la hora de comprobar si un grupo es resoluble o no es buscar si nuestro grupo tiene un subgrupo normal resoluble que haga que el cociente sea resoluble, con lo que podemos aplicar el tercer apartado de la siguiente Proposición, para la cual hemos de introducir dos Lemas previos.

Lema 4.15. *Sea G un grupo, $H < G$ y $N \lhd G$, entonces:*
$$\left[\frac{HN}{N}, \frac{HN}{N}\right] = \frac{[H,H]N}{N}$$

Lema 4.16. *Sea G un grupo y $N \lhd G$, entonces:*

$$\left(\frac{G}{N}\right)^{(k)} = \frac{G^{(k)}N}{N} \qquad \forall k \in \mathbb{N}$$

Demostración. Por inducción sobre $k \in \mathbb{N}$:

- Para $k = 0$, como $G = GN$ y $G = G^{(0)}$, tendremos que:

$$\frac{G}{N} = \frac{GN}{N}$$

- Supuesto para k, para $k + 1$:

$$\left(\frac{G}{N}\right)^{(k+1)} = \left(\left(\frac{G}{N}\right)^{(k)}\right)' = \left[\left(\frac{G}{N}\right)^{(k)}, \left(\frac{G}{N}\right)^{(k)}\right] \overset{(*)}{=} \left[\frac{G^{(k)}N}{N}, \frac{G^{(k)}N}{N}\right]$$
$$\overset{(**)}{=} \frac{[G^{(k)}, G^{(k)}]N}{N} = \frac{G^{(k+1)}N}{N}$$

Donde en $(*)$ usamos la hipótesis de inducción y en $(**)$ el Lema anterior. □

Proposición 4.17. *Se verifica que:*

i) *Todo subgrupo de un grupo resoluble es resoluble.*

ii) *Todo cociente de un grupo resoluble es resoluble.*

iii) *Si $N \lhd G$ y N y G/N son resolubles, entonces G es resoluble.*

Demostración. Veamos cada una:

i) Supongamos que la serie derivada de G es:

$$G = G^0 \rhd G' \rhd G'' \rhd \ldots \rhd G^{(r)} = \{1\}$$

Si $H < G$, entonces $H^{(k)} < G^{(k)}$ para todo $k \in \{1, \ldots, r\}$, gracias al Lema 4.12. Como tenemos que $G^{(r)} = \{1\}$, tendremos que $H^{(r)} = \{1\}$, por lo que H es resoluble.

ii) Supuesto que G es resoluble, y dado un subgrupo normal $N \lhd G$, consideramos el cociente G/N. Por la Proposición 4.14, como G es resoluble y la proyección al cociente es un epimorfismo, tenemos que G/N es resoluble.

iii) Por ser G/N resoluble, sabemos que $\exists s \in \mathbb{N}$ de forma que:

$$\frac{G^{(s)}N}{N} = (G/N)^{(s)} = \{1\}$$

Por lo que tendremos $G^{(s)} < N$. Por ser N resoluble, $\exists t \in \mathbb{N}$ de forma que $N^{(t)} = \{1\}$. En dicho caso, tendremos que, aplicando el Lema 4.12:

$$G^{(s+t)} < N^{(t)} = \{1\}$$

Por lo que G es resoluble. □

Para concluir los resultados sobre grupos resolubles, veamos qué pasa con el producto de grupos resolubles:

Corolario 4.17.1. *Cualquier producto finito de grupos resolubles es resoluble.*

Demostración. Suponiendo que G_1 y G_2 son dos grupos resolubles, si consideramos:

$$\{1\} \times G_2 < G_1 \times G_2$$

Tenemos que $\{1\} \times G_2$ es resoluble, por ser $\{1\} \times G_2 \cong G_2$. Si observamos el cociente:

$$\frac{G_1 \times G_2}{\{1\} \times G_2} \cong G_1$$

es resoluble, por ser G_1 resoluble. Por la Proposición anterior, concluimos que $G_1 \times G_2$ es resoluble. Por una sencilla inducción, lo demostramos para productos finitos de grupos resolubles. □

Por último lugar, cabe mencionar que para ciertos grupos podemos razonar si son resolubles simplemente mirando sus órdenes. Tras leer el siguiente Capítulo (que versa de $p-$grupos), estaremos en condiciones de probar que:

- Todo grupo de orden p^n con p primo y $n \in \mathbb{N}$ es resoluble.
- Todo grupo de orden pq con p, q primos es resoluble.
- Todo grupo de orden p^2q con p, q primos es resoluble.
- Todo grupo de orden $p_1p_2p_3$ con p_1, p_2, p_3 primos y $p_3 > p_1p_2$ es resoluble.

Estos resultados están demostrados al final de la relación correspondiente a este tema.

5. $G-$conjuntos y p-grupos

Definición 5.1. Sea G un grupo y X un conjunto no vacío, una acción[1] de G sobre X es una aplicación:

$$\begin{array}{rrcl} ac: & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & ac(g,x) \end{array}$$

Que verifica:

i) $ac(1,x) = x \quad \forall x \in X$.

ii) $ac(g, ac(h,x)) = ac(gh, x) \quad \forall x \in X, \quad \forall g,h \in G$.

En dicho caso, diremos que G actúa[2] (o que opera) sobre X.

Si G actúa sobre X, diremos que este conjunto X es un $G-$conjunto a izquierda. A la aplicación ac se le llama aplicación de la $G-$estructura.

Notación. Si $ac : G \times X \to X$ es una acción de G sobre X, es común denotar:

$$ac(g,x) = {}^g x = g \cdot x = g * x$$

En este documento, usaremos la notación $ac(g,x) = {}^g x$. Con esta, las propiedades que ha de cumplir una aplicación $ac : G \times X \to X$ para ser una acción son:

i) ${}^1 x = x \ \forall x \in X$.

ii) ${}^g({}^h x) = {}^{gh} x \ \forall x \in X, \forall g \in G$.

Ejemplo. Si G es un grupo y X es un conjunto no vacío, ejemplos de acciones de G sobre X son:

1. La acción trivial:

$$\begin{array}{rrcl} ac: & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & x \end{array}$$

2. Si tenemos una acción $ac : G \times X \to X$ y $H < G$, podemos considerar la acción por restricción $ac : H \times X \to X$, dada por:

$$ac(h,x) = ac(i(h), x) \qquad \forall h \in H, x \in X$$

   Donde consideramos la aplicación inclusión $i : H \to G$ dada por $i(h) = h$, para todo $h \in H$.

[1]En realidad esta es la definición de acción por la izquierda, pero no vamos a trabajar con las acciones por la derecha, por lo que hablaremos simplemente de acciones.

[2]En realidad deberíamos decir que "G actúa por la izquierda sobre X".

3. Dado $n \in \mathbb{N}$, si $X = \{1, \ldots, n\}$ y $G = S_n$, la acción natural de S_n sobre X será la acción $ac : S_n \times X \to X$ dada por:

$$ac(\sigma, k) = {}^{\sigma}k = \sigma(k) \qquad \forall \sigma \in S_n, k \in X$$

Proposición 5.1. *Sea G un grupo y X un conjunto no vacío, dar una acción de G sobre X equivale a dar un homomorfismo de grupos de G en* $\mathrm{Perm}(X)$.

Demostración. Veamos que es posible:

- Por una parte, dada una acción de G sobre X, $ac : G \times X \to X$, podemos definir la aplicación:

$$\begin{array}{rccc} \phi: & G & \longrightarrow & \mathrm{Perm}(X) \\ & g & \longmapsto & \phi(g) \end{array}$$

  Donde $\phi(g)$ es una aplicación $\phi(g) : X \longrightarrow X$ dada por:

$$\phi(g)(x) = {}^{g}x \qquad \forall x \in X$$

  Veamos en primer lugar que ϕ está bien definida, es decir, que $\phi(g) \in \mathrm{Perm}(X)$ para cada $g \in G$. Para ello, veamos antes que ϕ cumple:

  - $\phi(1) = id_X$, ya que la aplicación $x \mapsto ac(1, x)$ es la aplicación identidad en X, por ser ac una acción de G sobre X.
  - $\phi(g)\phi(h) = \phi(gh)$, ya que al evaluar en cualquier $x \in G$:

$$(\phi(g)\phi(h))(x) = \phi(g)(\phi(h)(x)) = \phi(g)({}^{h}x) = {}^{g}({}^{h}x) \overset{(*)}{=} {}^{gh}x = \phi(gh)(x)$$

    Donde en $(*)$ hemos usado que ac es una acción de G sobre X.

  Ahora, veamos que dado $g \in G$, la aplicación $\phi(g)$ es biyectiva (es decir, está en $\mathrm{Perm}(X)$), ya que su aplicación inversa es $\phi(g^{-1})$:

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(1) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$$

  Y anteriormente vimos que $\phi(1) = id_X$, por lo que $\phi(g) \in \mathrm{Perm}(X)$, para todo $g \in G$ y la aplicación ϕ está bien definida.

  Además, por las dos propiedades anteriores, tenemos que ϕ es un homomorfismo de grupos.

- Sea $\phi : G \to \mathrm{Perm}(X)$ un homomorfismo de grupos, definimos la aplicación $ac : G \times X \to X$ dada por:

$$ac(g, x) = \phi(g)(x) \qquad \forall g \in G, x \in X$$

  Veamos que es una acción:

$$\begin{gathered} ac(1, x) = \phi(1)(x) = id_X(x) = x \qquad \forall x \in X \\ ac(g, ac(h, x)) = \phi(g)(\phi(h)(x)) = (\phi(g)\phi(h))(x) = \phi(gh)(x) = ac(gh, x) \\ \forall x \in X, \quad \forall g, h \in G \end{gathered}$$

□

Definición 5.2 (Representación por permutaciones)**.** Sea G un grupo y X un conjunto no vacío, si tenemos una acción de G sobre X, el homomorfismo ϕ dado por esta acción según la Proposición 5.1 recibirá el nombre de representación de G por permutaciones.

Además, llamaremos a $\ker(\phi)$ núcleo de la acción, ya que:

$$\ker(\phi) = \{g \in G \mid \phi(g) = id_X\} = \{g \in G \mid {}^g x = x \quad \forall x \in X\}$$

En el caso de que $\ker(\phi) = \{1\}$, diremos que la acción es fiel.

Ejemplo. A continuación, dados varios ejemplos de acciones, consideraremos en cada caso su representación por permutaciones:

1. La representación por permutaciones de la acción trivial es el homomorfismo $\phi : G \to Perm(X)$ dado por:

$$\phi(g) = id_X \qquad \forall g \in G$$

2. Si tenemos un conjunto no vacío X y una acción $ac : G \times X \to X$ sobre un grupo G que tiene asociada una representación por permutaciones ϕ, entonces la acción por restricción $ac : H \times X \to X$ tendrá asociada como representación por permutaciones el homomorfismo $\phi_H : H \to Perm(X)$ dado por:

$$\phi_H = \phi \circ i$$

   Siendo $i : H \to G$ la aplicación inclusión.

3. En el caso de la acción natural de S_n sobre $X = \{1, \ldots, n\}$, tenemos que la representación por permutaciones es el homomorfismo $\phi : S_n \to S_n$ dado por:

$$\phi(\sigma) = \sigma \qquad \forall \sigma \in S_n$$

   Es decir, $\phi = id_{S_n}$.

4. Sea G un grupo, podemos definir la acción por traslación como:

$$\begin{array}{rccc} ac: & G \times G & \longrightarrow & G \\ & (g,h) & \longmapsto & gh \end{array}$$

   Y el homomorfismo asociado a la acción como representación por permutaciones será $\phi : G \to \mathrm{Perm}(G)$ dado por:

$$\phi(g)(h) = gh \qquad \forall g, h \in G$$

   Como además:

$$\ker(\phi) = \{g \in G \mid gh = h \quad \forall h \in G\} = \{1\}$$

   Tenemos que es una acción fiel.

Teorema 5.2 (Cayley)**.** *Todo grupo es isomorfo a un subgrupo de un grupo de permutaciones.*

Demostración. Sea G un grupo, consideramos la acción por traslación:

$$\begin{array}{rccc} ac: & G\times G & \longrightarrow & G \\ & (g,h) & \longmapsto & gh \end{array}$$

Y su representación por permutaciones, $\phi : G \to \text{Perm}(G)$ dado por:

$$\phi(g)(h) = gh \qquad \forall g \in G, \forall h \in G$$

Como la acción por traslación es una acción fiel, tendremos que $\ker(\phi) = \{1\}$ y aplicando el Primer Teorema de Isomorfía sobre ϕ, obtenemos que:

$$G \cong G/\{1\} \cong Im(\phi)$$

Donde $Im(\phi) = \phi_*(G)$, que en la Proposición 2.3 vimos que es un subgrupo de $\text{Perm}(G)$. □

Ejemplo. Podemos considerar las traslaciones de G sobre conjuntos especiales:

- La acción por traslación de G sobre $\mathcal{P}(G)$ será $ac : G \times \mathcal{P}(G) \to \mathcal{P}(G)$ dada por:
$$ac(g, A) = gA = \{ga \mid a \in A\} \subseteq G \qquad \forall A \in \mathcal{P}(G)$$
- Podemos también considerar la acción por traslación en el cociente por las clases laterales por la izquierda[3]: si $H < G$, consideramos el cociente de G sobre H por la izquierda y la acción $ac : G \times G/_{H}\!\sim\, \to G/_{H}\!\sim$ dada por:
$$ac(g, xH) = {}^g(xH) = gxH = \{gxh \mid h \in H\}$$

6. La <u>acción por conjugación</u> se define como $ac : G \times G \to G$ dada por:

$$ac(g, h) = {}^gh = ghg^{-1}$$

Que es una acción, ya que:

$$\begin{array}{c} {}^1h = 1h1^{-1} = h \qquad \forall h \in G \\ {}^g({}^hl) = g\,{}^hlg^{-1} = ghlh^{-1}g^{-1} = ghl(gh)^{-1} = {}^{gh}l \qquad \forall g, h, l \in G \end{array}$$

El homomorfismo asociado es:

$$\begin{array}{c} \phi : G \to \text{Perm}(G) \\ \phi(g)(h) = ghg^{-1} \qquad \forall g, h \in G \end{array}$$

El núcleo en este caso es:

$$\ker(\phi) = \{g \in G \mid ghg^{-1} = h \quad \forall h \in G\} = \{g \in G \mid gh = hg \quad \forall h \in G\} = Z(G)$$

7. La <u>acción por conjugación en partes de G</u> se define como la aplicación $ac : G \times \mathcal{P}(G) \to \mathcal{P}(G)$ dada por:

$$ac(g, A) = {}^gA = gAg^{-1} = \{gag^{-1} \mid a \in A\} \subseteq G \qquad \forall A \in \mathcal{P}(G)$$

[3]No es necesario considerar $H \lhd G$, ya que solo consideramos conjuntos no vacíos, por lo que no es necesario que el cociente tenga estructura de grupo.

8. Podemos definir la acción por conjugación de G también sobre $Subg(G)$:

$$Subg(G) = \{H \subseteq G \mid H < G\}$$

Como la aplicación $ac : G \times Subg(G) \to Subg(G)$ dada por:

$$ac(g, H) = {}^gH = gHg^{-1} < G$$

Ya que en la Proposición 3.1 vimos que gHg^{-1} era un subgrupo de G, al que llamaremos subgrupo conjugado de G.

5.1. Órbitas de un elemento

Definición 5.3 (Órbita)**.** Sea G un grupo y X un $G-$conjunto, definimos en X una relación de equivalencia $\sim$ (se comprueba a continuación) dada por:

$$y \sim x \Longleftrightarrow \exists g \in G \mid y = {}^gx$$

La clase de equivalencia de cada $x \in X$ se llama órbita de x, denotada por:

$$Orb(x) = \{y \in X \mid \exists g \in G \text{ con } y = {}^gx\}$$

Como estamos considerando una acción, será equivalente escribir (gracias a la propiedad simétrica):

$$Orb(x) = \{y \in X \mid \exists g \in G \text{ con } {}^gy = x\}$$

Tenemos de esta forma que el conjunto cociente $X/\sim$ es el conjunto formado por las órbitas de todos los elementos de X:

$$X/\sim = \{Orb(x) \mid x \in X\}$$

Proposición 5.3. *La relación $\sim$ de la definición anterior es una relación de equivalencia en X.*

Demostración. Comprobamos la reflexividad, simetría y transitividad de $\sim$:

i) Reflexividad: sea $x \in X$, entonces ${}^1x = x$, por lo que $x \sim x$.

ii) Simetría: sean $x, y \in X$ tales que $y \sim x$, entonces $\exists g \in G$ de forma que $y = {}^gx$. Como G es un grupo, consideramos $g^{-1} \in G$, de forma que:

$$^{g^{-1}}y = {}^{g^{-1}}({}^gx) = {}^{g^{-1}g}x = {}^1x = x$$

Por lo que $x \sim y$.

iii) Transitividad: sean $x, y, z \in X$ tales que $x \sim y$ e $y \sim z$, entonces $\exists g, h \in G$ de forma que:

$$y = {}^gx \qquad\qquad z = {}^hy$$

Entonces, tenemos que:

$$z = {}^h({}^gx) = {}^{hg}x$$

Como $hg \in G$, tenemos que $z \sim x$. $\square$

Ejemplo. Sobre $X = \{1, 2, 3, 4\}$: En S_4 consideramos $ac : S_4 \times X \to X$, la acción natural de S_4 sobre X:

$$ac(\sigma, k) = {}^{\sigma}k = \sigma(k)$$

- Si tenemos $H = \langle (1\ 2\ 3) \rangle$, queremos calcular las órbitas de los elementos de X. Recordamos que:

  $$Orb(x) = \{y \in X \mid \exists \sigma \in H \text{ con } \sigma(y) = x\}$$

  Es decir, pensamos en $Orb(x)$ como en los elementos de X desde los que podemos llegar a x con una permutación de H (o también como en aquellos elementos de X a los que podemos llegar desde x a través de una permutación de H). De esta forma:

  $$\begin{aligned} Orb(1) &= \{1, 2, 3\} \\ Orb(2) &= \{1, 2, 3\} \\ Orb(3) &= \{1, 2, 3\} \\ Orb(4) &= \{4\} \end{aligned}$$

- En A_4:

  $$A_4 = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1\,2\,3), (1\,2\,4), (1\,3\,4), (2\,3\,4), (1\,3\,2), (1\ 4\ 2), (1\ 4\ 3), (2\ 4\ 3)\}$$

  Como tenemos todos los $3-$ciclos:

  $$Orb(1) = X$$

  Y también tendremos que $Orb(k) = X$, para $k \in X$.

- En V, que contiene a todos los $2-$ciclos, la situación será la misma:

  $$Orb(k) = X \qquad \forall k \in X$$

- En $H = \langle (1\ 2\ 3\ 4) \rangle$ sucede lo mismo:

  $$Orb(k) = X \qquad \forall k \in X$$

Definición 5.4. Si el conjunto de órbitas $X/\sim$ es unitario, decimos que la acción es transitiva.

Este nombre se debe a que dados $x, y \in X$, siempre $\exists g \in G$ de forma que:

$$y = {}^{g}x$$

Definición 5.5 (Estabilizador)**.** Sea G un grupo y X un $G-$conjunto, definimos el grupo de estabilizadores de $x \in X$ en G como:

$$Stab_G(x) = \{g \in G \mid {}^{g}x = x\}$$

También se le llama grupo de isotropía.

Para justificar por qué a $Stab_G(x)$ le llamábamos grupo de estabilizadores de x en G, es necesaria la siguiente Proposición:

Proposición 5.4. *Sea G un grupo y X un $G-$conjunto:*

$$Stab_G(x) < G \qquad \forall x \in X$$

Demostración. Fijado $x \in X$, es claro que $Stab_G(x) \subseteq G$. Vemos que:

- $1 \in Stab_G(x)$, ya que ${}^1x = x$ por definición de acción.
- Si $g \in Stab_G(x)$, supongamos que $g^{-1} \notin Stab_G(x)$, con lo que ${}^{g^{-1}}x = y \in X$ con $y \neq x$. En dicho caso:

  $$x = {}^1x = {}^{g^{-1}g}x = {}^{g^{-1}}({}^gx) = {}^{g^{-1}}x = y$$

  Llegamos a una contradicción, luego $g^{-1} \in Stab_G(x)$ para todo $g \in Stab_G(x)$.
- Finalmente, si $g, h \in Stab_G(x)$, entonces:

  $${}^{gh}x = {}^g({}^hx) = {}^gx = x$$

  Por lo que $gh \in Stab_G(x)$.

$\square$

Ejemplo. Si nuevamente sobre $X = \{1, 2, 3, 4\}$ volvemos a considerar la acción natural de S_4 sobre X:

- En $H = \langle(1\ 2\ 3)\rangle$, recordamos que:

  $$Stab_H(x) = \{\sigma \in H \mid \sigma(x) = x\}$$

  Es decir, el grupo de estabilizadores de x en H son los elementos de H que dejan fijo el elemento x. De esta forma:

  $$\begin{aligned} Stab_H(1) &= \{1\} \\ Stab_H(2) &= \{1\} \\ Stab_H(3) &= \{1\} \\ Stab_H(4) &= H \end{aligned}$$

- En A_4:

  $$\begin{aligned} Stab_{A_4}(1) &= \{1, (2\ 3\ 4), (2\ 4\ 3)\} = \langle(2\ 3\ 4)\rangle \\ Stab_{A_4}(2) &= \langle(1\ 3\ 4)\rangle \\ Stab_{A_4}(3) &= \langle(1\ 2\ 4)\rangle \\ Stab_{A_4}(4) &= \langle(1\ 2\ 3)\rangle \end{aligned}$$

- En V:

  $$Stab_V(k) = \{1\} \qquad \forall k \in X$$

- En $H = \langle(1\ 2\ 3\ 4)\rangle$:
$$Stab_H(k) = \{1\} \qquad \forall k \in X$$

Vamos a poder establecer una relación entre el órden de las órbitas y del conjunto cociente.

Proposición 5.5. *Sea G un grupo finito que actúa sobre X, entonces para cada $x \in X$, $Orb(x)$ es un conjunto finito y:*

$$|Orb(x)| = [G : Stab_G(x)]$$

En particular, el cardinal de la órbita es un divisor del orden de G.

Demostración. Fijado $x \in X$, si consideramos $Stab_G(x) < G$ y las clases laterales por la izquierda[4], $G/_{Stab_G(x)}\sim$, definimos la aplicación $\phi : G/_{Stab_G(x)}\sim \longrightarrow Orb(x)$ dada por:
$$\phi(gStab_G(x)) = {}^gx \qquad \forall gStab_G(x) \in G/_{Stab_G(x)}\sim$$

- Veamos que está bien definida. Para ello, sean $g, g' \in G$ de forma que:
$$gStab_G(x) = g'Stab_G(x)$$
Entonces, existirá $h \in Stab_G(x)$ de forma que $g = g'h$. En dicho caso:
$$\phi(gStab_G(x)) = {}^gx = {}^{g'h}x = {}^{g'}({}^hx) = {}^{g'}x = \phi(g'Stab_G(x))$$

- Veamos que es sobreyectiva: sea $y \in Orb(x)$, entonces $\exists g \in G$ de forma que:
$$y = {}^gx$$
Por lo que $y = \phi(gStab_G(x))$.

- Para la inyectividad, sean $g, g' \in G$ de forma que:
$${}^gx = \phi(gStab_G(x)) = \phi(g'Stab_G(x)) = {}^{g'}x$$
Entonces, podemos escribir:
$$x = {}^{g^{-1}}({}^gx) = {}^{g^{-1}}({}^{g'}x) = {}^{g^{-1}g'}x$$
De donde concluimos que $g^{-1}g' \in Stab_G(x)$, por lo que $gStab_G(x) = g'Stab_G(x)$.

En definitiva, acabamos de probar que $Orb(x)$ es biyectivo con $G/_{Stab_G(x)}\sim$, por lo que tienen el mismo cardinal. Además:

- Por ser G finito y $Stab_G(x) < G$, tenemos que:
$$|Orb(x)| = [G : Stab_G(x)] = \frac{|G|}{|Stab_G(x)|}$$
Por lo que $Orb(x)$ es un conjunto finito.

[4]No consideramos el conjunto cociente porque no sabemos si $Stab_G(x)$ es un subgrupo normal en G o no.

- Despejando de la igualdad superior, tenemos que:

$$|Orb(x)||Stab_G(x)| = |G|$$

Por lo que $|Orb(x)|$ es un divisor de $|G|$.

□

Observación. La demostración es cierta sin suponer que G sea un grupo finito, pero entonces solo podemos poner como tesis que $Orb(x)$ es biyectivo con $G/_{Stab_G(x)}\sim$, para todo $x \in X$.

Proposición 5.6. *Sea G un grupo que actúa sobre X, si $x, y \in X$ están en la misma órbita, entonces $Stab_G(x)$ y $Stab_G(y)$ son subgrupos conjugados.*

Demostración. Si x e y están en la misma órbita, entonces $Orb(x) = Orb(y)$, por lo que $\exists g \in G$ de forma que $y = {}^g x$. En dicho caso, también tenemos que $x = {}^{g^{-1}} y$. Veamos que:

$$Stab_G(x) = g^{-1} Stab_G(y) g$$

Para ello:

$\subseteq$) Sea $h \in Stab_G(x)$, queremos ver que $h \in g^{-1} Stab_G(y) g$, para lo que bastará ver que $ghg^{-1} \in Stab_G(y)$:

$${}^{ghg^{-1}} y = {}^{gh} x = {}^g x = y$$

$\supseteq$) Sea $h \in Stab_G(y)$, queremos ver que $g^{-1} hg \in Stab_G(x)$:

$${}^{g^{-1}hg} x = {}^{g^{-1}h} y = {}^{g^{-1}} y = x$$

□

Definición 5.6. Sea G un grupo y X un $G-$conjunto, un elemento $x \in X$ se dice que es fijo por la acción si ${}^g x = x$, $\forall g \in G$.

Consideramos el conjunto de todos los elementos que se quedan fijos por todos los elementos de G:

$$Fix(X) = \{x \in X \mid {}^g x = x, \quad \forall g \in G\}$$

Proposición 5.7. *Sea G un grupo y X un $G-$conjunto, si $x \in X$, entonces:*

$$x \in Fix(X) \iff Orb(x) = \{x\} \iff Stab_G(x) = G$$

Demostración. Si recordamos las definiciones de estos tres conjuntos:

$$\begin{aligned} Orb(x) &= \{y \in X \mid \exists g \in G \text{ con } {}^g y = x\} \\ Stab_G(x) &= \{g \in G \mid {}^g x = x\} \\ Fix(X) &= \{x \in X \mid {}^g x = x \quad \forall g \in G\} \end{aligned}$$

Veamos todas las implicaciones:

$x \in Fix(X) \Longrightarrow Orb(x) = \{x\}$

Si $y \in Orb(x)$, entonces $\exists g \in G$ con ${}^g y = x$, por lo que:

$$y = {}^{g^{-1}g}y = {}^{g^{-1}}({}^g y) = {}^{g^{-1}}x \overset{(*)}{=} x$$

Donde en $(*)$ usamos que $x \in Fix(X)$. Concluimos que $Orb(x) = \{x\}$.

$Orb(x) = \{x\} \Longrightarrow Stab_G(x) = G$

Sea $g \in G$, si consideramos $y = {}^g x$, entonces $y \in Orb(x) = \{x\}$, de donde $y = x$ y $g \in Stab_G(x)$.

$Stab_G(x) = G \Longrightarrow x \in Fix(x)$

$${}^g x = x \qquad \forall g \in G$$

De donde deducimos que $x \in Fix(X)$.

□

Observación. Si tenemos un grupo G y un $G-$conjunto X, recordamos que tenemos definida sobre X una relación de equivalencia $\sim$, con la que anteriormente definimos los órbitas de los elementos, que nos da una partición de X en clases de equivalencia. Estaremos especialmente interesados en el caso en el que X sea un conjunto finito, ya que podremos obtener una fórmula del cardinal de X a partir de los cardinales de las órbitas de los elementos de X.

De esta forma, si $\Lambda \subseteq X$ contiene un único elemento de cada clase de equivalencia del conjunto cociente $X/\sim$, obtenemos la igualdad:

$$|X| = \sum_{y \in \Lambda} |Orb(y)|$$

Para simplificarla usando propiedades ya vistas, sabemos que puede haber órbitas unitarias:

$$Orb(x) = \{x\} \Longleftrightarrow x \in Fix(x)$$

Por tanto, podemos simplificar la igualdad superior, eliminando de ella todas las órbitas unitarias. Para ello, si $\Gamma = \Lambda \setminus Fix(X)$:

$$|X| = \sum_{y \in \Lambda} |Orb(y)| = |Fix(X)| + \sum_{y \in \Gamma} |Orb(y)|$$

Y aplicando finalmente la Proposición 5.5, llegamos a que:

$$|X| = \sum_{y \in \Lambda} |Orb(y)| = |Fix(X)| + \sum_{y \in \Gamma} |Orb(y)| = |Fix(X)| + \sum_{y \in \Gamma} [G : Stab_G(y)]$$

En lo que sigue, no diremos de forma explícita quién es este conjunto Γ, debido a lo engorrosas que se volverían las explicaciones. Por tanto, cada vez que veamos esta fórmula debemos pensar en que estamos cogiendo un único representante de cada clase de equivalencia no unitaria, y lo estamos metiendo en Γ.

A continuación, lo que haremos será estudiar los conjuntos $Orb(\cdot)$, $Stab_G(\cdot)$ y $Fix(X)$ para ciertos ejemplos comunes de acciones.

5.1.1. Acción por traslación

Sea G un grupo no trivial, la acción por traslación se define como $ac : G \times G \to G$ dada por:

$$ac(g, h) = {}^g h = gh \qquad \forall g, h \in G$$

De esta forma, tenemos que:

$$Orb(h) = \{k \in G \mid \exists g \in G \text{ con } k = {}^g h = gh\} = G \qquad \forall h \in G$$

Ya que fijado $k \in G$ y dado $h \in G$, siempre podemos tomar $g = kh^{-1} \in G$ para tener que ${}^g h = gh = k$.

$$Stab_G(h) = \{g \in G \mid gh = {}^g h = h\} = \{1\} \qquad \forall h \in G$$
$$Fix(G) = \{h \in G \mid gh = {}^g h = h \quad \forall g \in G\} = \emptyset$$

Observación. Observemos que la acción por traslación cuenta con las mismas cualidades que tiene una traslación entre dos espacios vectoriales, pensando en que primero fijamos un vector $v \in V$ para luego definir una aplicación $t_v : V \to V'$. De esta forma:

- Fijado cualquier vector v, t_v siempre será sobreyectiva. Esto se pone de manifiesto al decir que $Orb(h) = G$ para todo $h \in G$.
- La única traslación que mantiene fijo un punto es la correspondiente al vector 0, que deja fijos todos los puntos, $Stab_G(h) = \{1\}$ $\forall h \in G$.
- Como hay traslaciones que no mantienen fijos ningún punto (todas salvo la trivial), no hay ningún punto que permanezca invariante ante todas ellas, $Fix(G) = \emptyset$.

5.1.2. Acción por conjugación

Sea G un grupo, la acción por conjugación se define como $ac : G \times G \to G$ dada por:

$$ac(g, h) = {}^g h = ghg^{-1} \qquad \forall g, h \in G$$

Preliminares

Antes de estudiar los subconjuntos notables de esta acción, definimos ciertos conjuntos y vemos propiedades de estos que nos ayudarán a entender la acción.

Definición 5.7 (Centralizador)**.** Sea G un grupo y $S \subseteq G$, llamamos centralizador de S en G al conjunto:

$$C_G(S) = \{x \in G \mid xs = sx \quad \forall s \in S\}$$

Definición 5.8 (Normalizador)**.** Sea G un grupo y $S \subseteq G$, llamamos normalizador de S en G al conjunto:

$$N_G(S) = \{x \in G \mid xS = Sx\}$$

Proposición 5.8. *Sea G un grupo y $S \subseteq G$, se verifica:*

i) $N_G(S) < G$.

ii) $C_G(S) \lhd N_G(S)$.

iii) *Si $S < G$, entonces $S \lhd N_G(S)$.*

Demostración. Demostramos cada apartado:

i) Sean $x, y \in N_G(S)$, entonces tendremos que:

$$xS = Sx \Longrightarrow xSx^{-1} = S$$
$$yS = Sy \Longrightarrow S = y^{-1}Sy$$

En dicho caso:

$$(xy^{-1})S(xy^{-1})^{-1} = (xy^{-1})S(yx^{-1}) = x(y^{-1}Sy)x^{-1} = xSx^{-1} = S$$

De donde deducimos que $(xy^{-1})S = S(xy^{-1})$, por lo que $xy^{-1} \in N_G(S)$ y $N_G(S) < G$.

ii) Hemos de ver primero que $C_G(S) < N_G(S)$:

- En primer lugar, si $x \in C_G(S)$:

  $$xS = \{xs \mid s \in S\} = \{sx \mid s \in S\} = Sx$$

  Por lo que $x \in N_G(S)$ y se tiene que $C_G(S) \subseteq N_G(S)$.

- Ahora, si $x, y \in C_G(S)$, entonces:

  $$xs = sx \Longrightarrow xsx^{-1} = s$$
  $$ys = sy \Longrightarrow s = y^{-1}sy \qquad \forall s \in S$$

  Lo que nos permite escribir:

  $$(xy^{-1})s(xy^{-1})^{-1} = x(y^{-1}sy)x^{-1} = xsx^{-1} = s \qquad \forall s \in S$$

  De donde deducimos que $xy^{-1} \in C_G(S)$, por lo que $C_G(S) < N_G(S)$.

Para la normalidad, dado $x \in C_G(S)$ y $g \in N_G(S)$, queremos ver que se cumple $y = gxg^{-1} \in C_G(S)$. Para ello, dado $s \in S$, vemos que:

$$ys = (gxg^{-1})s \overset{(*)}{=} gxs'g^{-1} = gs'xg^{-1} \overset{(**)}{=} s(gxg^{-1}) = sy$$

Donde en $(*)$ usamos que como $g \in N_G(S)$, también tenemos que $g^{-1} \in N_G(S)$, con lo que $\exists s' \in S$ de forma que:

$$g^{-1}s = s'g^{-1}$$

Y en $(**)$ deshacemos este proceso, ya que multiplicando la igualdad superior por derecha e izquierda por g, llegamos a que:

$$g^{-1}s = s'g^{-1} \Longrightarrow gg^{-1}sg = gs'g^{-1}g \Longrightarrow sg = gs'$$

En definitiva, de $ys = sy$ deducimos que $y = gxg^{-1} \in C_G(S)$, para todo $x \in C_G(S)$ y todo $g \in N_G(S)$, de donde $C_G(S) \lhd N_G(S)$.

iii) Si suponemos además que $S < G$, por una parte tenemos que:

$$sS = S = Ss \qquad \forall s \in S$$

De donde deducimos que $S \subseteq N_G(S)$ y por ser $S < G$, tenemos que $S < N_G(S)$. Para la normalidad, si $g \in N_G(S)$, tendremos entonces que:

$$gS = Sg \Longrightarrow gSg^{-1} = S$$

De donde deducimos que $S \lhd N_G(S)$.

□

Proposición 5.9. *Sea G un grupo, $H, K < G$ con $H \subseteq K$, entonces:*

$$H \lhd K \Longleftrightarrow K < N_G(H)$$

De esta forma, el normalizador $N_G(H)$ se caracteriza como el mayor subgrupo de G en el que H es normal.

Demostración. Por ser $H, K < G$ con $H \subseteq K$, tenemos ya que $H < K$. Por una caracterización que vimos de los subgrupos normales:

$$H \lhd K \Longleftrightarrow kHk^{-1} = H \quad \forall k \in K \Longleftrightarrow kH = Hk \quad \forall k \in K \Longleftrightarrow K \subseteq N_G(H)$$

Y por ser $K < G$, $K \subseteq N_G(H) \Longleftrightarrow K < N_G(H)$. □

Ejercicio. Para terminar de comprender las propiedades del centralizador y del normalizador, se pide probar que si G es un grupo y $H < G$:

$$H \lhd G \Longleftrightarrow G = N_G(H)$$
$$H \subseteq Z(G) \Longleftrightarrow G = C_G(H)$$

Subconjuntos notables

Estudiadas ya las propiedades del centralizador y del normalizador, estamos ya en condiciones de estudiar los conjuntos notables de la acción por conjugación:

$$Orb(h) = \{k \in G \mid \exists g \in G \text{ con } k = {}^gh = ghg^{-1}\} = \{ghg^{-1} \mid g \in G\} := Cl_G(h) \qquad \forall h \in G$$

De esta forma, llamaremos a la órbita de h por la acción por conjugación la clase de conjugación de h en G, notada por $Cl_G(h)$.

$$Stab_G(h) = \{g \in G \mid {}^gh = ghg^{-1} = h\} = \{g \in G \mid gh = hg\} = C_G(h)$$

El estabilizador de h en G coincide con el centralizador de h en G, y como la órbita de h coincidía con la clase de conjugación de h en G, por la Proposición 5.5, tenemos que:

$$|Cl_G(h)| = |Orb(h)| = [G : Stab_G(h)] = [G : C_G(h)] \qquad \forall h \in G$$

Y en el caso de que G sea finito:

$$|Cl_G(h)||C_G(h)| = |G|$$

Para los puntos fijos:

$$Fix(G) = \{h \in G \mid ghg^{-1} = {}^gh = h \quad \forall g \in G\} = \{h \in G \mid gh = hg \quad \forall g \in G\} = Z(G)$$

Ejemplo. Calcular las clases de conjugación de los elementos de D_4:

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} = \{s^i r^j \mid i \in \{0,1\}\ j \in \{0,1,2,3\}\}$$

Vemos que:

$$\begin{aligned}
Cl_{D_4}(1) &= \{s^i r^j 1 (s^i r^j)^{-1}\} = \{1\} \\
Cl_{D_4}(r) &= \{s^i r^j r (s^i r^j)^{-1}\} = \{s^i r^j r r^{-j} s^{-i}\} = \{s^i r s^i\} = \{r, srs\} = \{r, r^3\} \\
Cl_{D_4}(r^2) &= \{s^i r^2 s^i\} = \{r^2\} \\
Cl_{D_4}(s) &= \{s, sr^2\} \\
Cl_{D_4}(sr) &= \{sr, sr^3\}
\end{aligned}$$

Fórmula de clases

Podemos particularizar la fórmula anteriormente obtenida:

$$|X| = |Fix(X)| + \sum_{y\in\Gamma} [G : Stab_G(y)]$$

Para la acción por conjugación, obteniendo la **fórmula de clases**:

$$|G| = |Z(G)| + \sum_{y\in\Gamma} [G : C_G(y)]$$

Esta última podemos generalizarla para cualquier subgrupo $H \lhd G$, obteniendo la fórmula de clases general:

$$|H| = |H \cap Z(G)| + \sum_{y\in\Gamma} [G : C_G(y)]$$

Aunque no será de gran relevancia en esta asignatura.

5.1.3. Acción por conjugación sobre subgrupos

Sea G un grupo, la acción por conjugación sobre sus subgrupos viene definida[5] por $ac : G \times Subg(G) \to Subg(G)$ dada por:

$$ac(g, H) = {}^gH = gHg^{-1} \qquad \forall g \in G, \qquad \forall H \in Subg(G)$$

Veamos que:

$$Orb(H) = \{K \in Subg(G) \mid \exists g \in G \text{ con } gHg^{-1} = {}^gH = K\} = \{gHg^{-1} \mid g \in G\}$$

Es decir, la órbita de un subgrupo está formado por todos sus conjugados.

Observación. Sea G un grupo, $H \in Subg(G)$, si consideramos la acción por conjugación sobre subgrupos, tenemos que:

$$Orb(H) = \{H\} \Longleftrightarrow H \lhd G$$

Esto se debe a que:

$$Orb(H) = \{H\} \Longleftrightarrow \{gHg^{-1} \mid g \in G\} = \{H\} \Longleftrightarrow H \lhd G$$

Donde la última equivalencia se tiene gracias a la Proposición 3.2, donde vimos una caracterización de los subgrupos normales.

[5] está bien definida gracias a la Proposición 3.1

El estabilizador:

$$Stab_G(H) = \{g \in G \mid {}^gH = H\} = \{g \in G \mid gH = Hg\} = N_G(H)$$

Vemos finalmente los subgrupos que quedan fijos mediante la acción (resultado que debemos tener claro después de la observación anterior):

$$Fix(Subg(G)) = \{H < G \mid gHg^{-1} = {}^gH = H \quad \forall g \in G\} = \{H < G \mid H \lhd G\}$$

Coincide con el conjunto de subgrupos normales de G.

Y tendremos que:

$$|Orb(H)| = [G : N_G(H)]$$

5.2. $p-$grupos

Definición 5.9 ($p-$grupo)**.** Si p es un número primo, un grupo G se dice que es un $p-$grupo si todo elemento de G distinto del neutro tiene orden una potencia de p. Si G es un grupo, diremos que $H < G$ es un $p-$subgrupo de G si H es un $p-$grupo.

Ejemplo. $\mathbb{Z}_8$ es un ejemplo de $2-$grupo, ya que sus elementos son:

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

Calculamos los órdenes de todos los elementos, sabiendo que (Proposición 2.18):

$$O(x) = \frac{n}{\text{mcd}(x, n)} \qquad \forall x \in \mathbb{Z}_n$$

Por lo que:

$$\begin{array}{llll} O(1) = 8 = 2^3 & O(2) = 4 = 2^2 & O(3) = 8 = 2^3 & O(4) = 2 \\ O(5) = 8 = 2^3 & O(6) = 4 = 2^2 & O(7) = 8 = 2^3 & \end{array}$$

Teorema 5.10 (de Cauchy)**.** *Si G es un grupo finito y p es un primo que divide a $|G|$, entonces G tiene un elemento de orden p, y por tanto tendrá un $p-$subgrupo de orden p.*

Demostración. Si consideramos:

$$X = \{(a_1, a_2, \ldots, a_p) \in G^p \mid a_1 a_2 \ldots a_p = 1\}$$

Si $|G| = n$, entonces $|X| = n^{p-1}$, ya que elegimos libremente las $p - 1$ primeras coordenadas (variación con repetición):

$$a_1, a_2, \ldots, a_{p-1} \in G \quad \text{arbitrarios}$$

Y la última viene condicionada:

$$a_p = (a_1 a_2 \ldots a_{p-1})^{-1}$$

Sea $\sigma = (1\ 2\ \dots\ p) \in S_p$, consideramos $H = \langle\sigma\rangle = \{1, \sigma, \dots, \sigma^{p-1}\} \subseteq S_p$. Consideramos también la acción $ac : H \times X \to X$ dada por (compruébese que es una acción):

$$ac(\sigma^k, (a_1, a_2, \dots, a_p)) = \left(a_{\sigma^k(1)}, a_{\sigma^k(2)}, \dots, a_{\sigma^k(p)}\right) \qquad \forall (a_1, \dots, a_p) \in X, \forall \sigma^k \in H$$

Por la Proposición 5.5, tenemos que:

$$|Orb(z)| = [H : Stab_H(z)] = \frac{|H|}{|Stab_H(z)|} \qquad \forall z \in X$$

De donde tenemos que $|Orb(a_1, \dots, a_p)|$ es un divisor de $|H|$, $\forall (a_1, \dots, a_p) \in X$. En dicho caso, $|Orb(a_1, \dots, a_p)| \in \{1, p\}$, por ser $|H| = p$. Por tanto, las órbitas de un elemento serán unitarias o bien tendrán cardinal p.

Por tanto, sean r el número de órbitas con un elemento y s el número de órbitas con p elementos, entonces ($|\Gamma| = s$):

$$n^{p-1} = |X| = |Fix(X)| + \sum_{y \in \Gamma} |Orb(y)| = r + \sum_{y \in \Gamma} p = r + sp$$

Veamos ahora cómo son los elementos de $Orb(a_1, \dots, a_p)$:

$$\begin{aligned} Orb(a_1, \dots, a_p) &= \left\{{}^{\sigma^k}(a_1, \dots, a_p) \mid k \in \{0, \dots, p-1\}\right\} \\ &= \{(a_1, \dots, a_p), (a_2, \dots, a_p, a_1), \dots, (a_p, a_1, \dots, a_{p-1})\} \end{aligned}$$

Por tanto, la órbita será unitaria si y solo si $a_1 = a_2 = \dots = a_p$. Además, sabemos de la existencia de órbitas con un elemento ($r \geqslant 1$), como $Orb(1, 1, \dots, 1)$. Busquemos más: por hipótesis, $p \mid n$ y además $r = n^{p-1} - sp$, de donde $p \mid r$, por lo que $r \geqslant 2$ (ya que lo divide un primo).

En conclusión, $\exists a \in G \setminus \{1\}$ de forma que $Orb(a, a, \dots a)$ es unitaria, de donde $a^p = 1$, por lo que $O(a) \mid p$ y sabemos que $O(a) \neq 1$. La única posibilidad es que $O(a) = p$.

Finalmente, sea $x \in \langle a\rangle \setminus \{1\}$, tenemos entonces que $1 \neq O(x) \mid p$, por lo que $O(x) = p$ y tenemos que todo elemento del subgrupo $\langle a\rangle$ es de orden p. En definitiva, $\langle a\rangle$ es un $p-$subgrupo de G de orden p. □

Corolario 5.10.1. *Sea G un grupo finito y p un número primo:*

$$G \text{ es un } p-\text{grupo} \iff \exists n \in \mathbb{N} \text{ con } |G| = p^n$$

Demostración. Veamos la doble implicación.

$\Longleftarrow$) Si $|G| = p^n$ para cierto $n \in \mathbb{N}$, entonces tendremos que $O(x) | p^n$ para todo $x \in G$, de donde $O(x) = p^k$ para cierto $k \in \mathbb{N}$, luego G es un $p-$grupo.

$\Longrightarrow$) Suponemos que q es un primo que divide al orden de $|G|$, luego por el Teorema de Cauchy debe existir $x \in G$ de forma que $O(x) = q$. En dicho caso, como G es un $p-$grupo, $q = p^r$ para cierto $r \in \mathbb{N}$, de donde (q y p son primos) $r = 1$ y $q = p$.

De esta forma, el único primo que divide a $|G|$ es p, luego $|G| = p^n$, para algún $n \in \mathbb{N}$. □

Teorema 5.11 (de Burnside)**.** *Si G es un $p-$grupo finito no trivial, entonces $|Z(G)| \geqslant p$, y en particular, $|Z(G)| \neq 1$.*

Demostración. Distinguimos casos:

- Si G es abeliano, $Z(G) = G$ y tenemos que $|Z(G)| = |G| = p^n$ para cierto $n \in \mathbb{N}$, por lo que $|Z(G)| \geqslant p$. En particular, $Z(G) = G$ no es trivial.
- Si G es no abeliano, entonces $Z(G) < G$ y por la fórmula anterior de clases:

$$p^n = |G| = |Z(G)| + \sum_{h\in\Gamma}[G : C_G(h)]$$

Como G es finito, $[G : C_G(h)]$ divide a $|G| = p^n$ para cualquier $h \in \Gamma$ y para cierto $n \in \mathbb{N}$. Es decir:

$$[G : C_G(h)] = p^k \qquad \text{para algún } k \in \mathbb{N}, \quad \forall h \in \Gamma$$

En ningún caso puede ser $k = 0$, ya que diríamos que $C_G(h) = G$ y:

$$C_G(h) = \{g \in G \mid gh = hg\}$$

De donde $h \in Z(G)$, por lo que h no estaría en $\Gamma \subseteq G \setminus Z(G)$.

En dicho caso, $p \mid [G : C_G(h)]$ para todo $h \in \Gamma$, $p \mid |Z(G)|$ (despejar $|Z(G)|$ de la anterior igualdad), de donde $|Z(G)| \geqslant p$.

□

Lema 5.12. *Si G es un grupo y $G/Z(G)$ es cíclico, entonces G es abeliano.*

Demostración. Como $G/Z(G)$ es cíclico, existirá $z \in G$ de forma que:

$$G/Z(G) = \langle zZ(G)\rangle$$

Sean $x, y \in G$, si consideramos su proyección al cociente, tendremos que $\exists n, m \in \mathbb{Z}$ de forma que:

$$xZ(G) = z^n Z(G) \qquad yZ(G) = z^m Z(G)$$

Es decir, $\exists a, b \in Z(G)$ de forma que $x = z^n a$ y $y = z^m b$. Por tanto:

$$xy = z^n a z^m b = z^n z^m ab = z^{n+m} ba = z^m z^n ba = z^m b z^n a = yx$$

□

Corolario 5.12.1. *Si G es un grupo y p es un número primo, si $|G| = p^n$, entonces:*

$$|Z(G)| \neq p^{n-1}$$

En particular, todos los grupos de orden p^2 son abelianos.

Demostración. Supongamos que $|G| = p^n$ y que $|Z(G)| = p^{n-1}$. De esta forma:

$$|G/Z(G)| = p$$

En dicho caso, $G/Z(G)$ es cíclico, luego G es abeliano (por el Lema anterior). Por tanto, G coincide con su centro, $G = Z(G)$, luego $p^n = p^{n-1}$, contradicción.

En particular, si G es un grupo con $|G| = p^2$ con p primo, como $Z(G) < G$, $|Z(G)|$ a de dividir a p^2, luego:

- Si $|Z(G)| = 1$, entonces $Z(G) = 1$, que contradice a Burnside.
- $|Z(G)| = p$ no puede ser, por lo que acabamos de probar.
- La única posibilidad es que $|Z(G)| = p^2$, de donde $Z(G) = G$.

□

Observación. Notemos que ahora sabemos que todos los grupos de orden un primo al cuadrado son resolubles, por ser abelianos.

Teorema 5.13. *Sea G un grupo finito con $|G| = n$ y sea p un número primo, entonces, para toda potencia p^k que divida a n, existe un subgrupo $H < G$ con orden $|H| = p^k$.*

Demostración. Por inducción sobre k:

- Si $k = 1$: tenemos el Teorema de Cauchy.
- Primera hipótesis de inducción: el resultado es cierto para todo $l < k$: si p^l divide a $|G|$, entonces $\exists H < G$ con $|H| = p^l$.
  Veamos qué ocurre con k, es decir, si $|G| = p^k r = n$ para cierto $r \in \mathbb{N}$.

  Por inducción sobre r:

  - Si $r = 1$: tomamos $H = G$.
  - Segunda hipótesis de inducción: si $r > 1$, suponemos el resultado cierto para todo grupo G de orden $p^k m$ con $m < r$, es decir, $\exists H < G$ con $|H| = p^k$, veamos qué ocurre para $|G| = p^k r$:

    Para ello, distinguimos casos:

    - Si existe $K < G$, $K \neq G$ de forma que $p \nmid [G : K]$. En dicho caso: $|G| = [G : K]|K|$ y $p^k \mid |G|$, entonces p^k dividirá a $|K|$, luego $\exists s \in \mathbb{N}$ de forma que $|K| = p^k s$ con $s < r$ (ya que $|K| < |G|$). Usando la Segunda Hipótesis de inducción, tendremos que existe un subgrupo $H < K < G$ de forma que $|H| = p^k$.

- Si para cualquier $K < G$, $K \neq G$ se tiene que $p \mid [G : K]$, entonces usando la fórmula de las clases:

$$|Z(G)| = |G| - \sum_{h \in \Gamma} [G : C_G(h)]$$

Como $G \neq C_G(h) < G$ para cada $h \in \Gamma$ (ya que $C_G(h) = G \iff h \in Z(G)$), tendremos que p divide a $[G : C_G(h)]$ para todo $h \in \Gamma$ (y además p^k divide a $|G|$), concluimos que $p \mid |Z(G)|$. Por el Teorema de Cauchy, podemos encontrar $K < Z(G)$ de forma que $|K| = p$.
Por ser $K \subseteq Z(G)$, entonces $K \lhd G$ (basta pensar en la definición de subgrupo normal) y podemos considerar el conjunto cociente G/K, con orden:

$$|G/K| = \frac{|G|}{|K|} = \frac{|G|}{p} = \frac{p^k r}{p} = p^{k-1} r$$

De donde p^{k-1} divide a $|G/K|$.
Por la Primera Hipótesis de inducción, existe un subgrupo $L < G/K$ con $|L| = p^{k-1}$. Por el Tercer Teorema de Isomorfía, si tomamos $H = p^*(L)$, tenemos que $K \lhd H < G$, con:

$$L = H/K$$

De donde:

$$|H| = |H/K||K| = p^{k-1} p = p^k$$

□

Ejemplo. Por ejemplo, si G es un grupo con orden $|G| = 24 = 2^3 \cdot 3$, sabemos que G tendrá subgrupos de orden 2, 4, 8 y 3.

5.2.1. $p-$subgrupos de Sylow

En 1872, un noruego llamado Peter LM Sylow (1832-1918) definió unos grupos y llegó a unos resultados sobre ellos. En este documento, sus Teoremas no tendrán demostraciones muy elaboradas, como consecuencia de la teoría que venimos ya desarrollando desde el inicio.

Definición 5.10 ($p-$subgrupos de Sylow)**.** Si G es un grupo finito y p un número primo que divide a $|G|$, un $p-$subgrupo de Sylow de G es un $p-$subgrupo de G cuyo orden es la máxima potencia de p que divide a $|G|$.

Es decir, si $|G| = p^k m$ con $\text{mcd}(p, m) = 1$ y p primo, un $p-$subgrupo $H < G$ es de Sylow si $|H| = p^k$.

Corolario 5.13.1 (Primer Teorema de Sylow)**.** *Para todo grupo finito G y todo divisor primo p de su orden, existe al menos un $p-$subgrupo de Sylow de G.*

Demostración. Si p divide a $|G|$, existirán $k \in \mathbb{N}$ y $m \in \mathbb{N}$ con $\text{mcd}(p, m) = 1$ de forma que $|G| = p^k m$, por lo que también p^k divide a $|G|$. El Teorema 5.13 nos dice que $\exists H < G$ con $|H| = p^k$, luego H será un $p-$subgrupo de Sylow de G. □

Ejemplo. Si tenemos un grupo G con $|G| = 24 = 2^3 \cdot 3$, vamos a tener:

- $P < G$ un $2-$subgrupo de Sylow, con $|P| = 8$.
- $Q < G$ un $3-$subgrupo de Sylow, con $|Q| = 3$.

Observación. Si G es un grupo y p es un número primo con:

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

Si $H < G$ y P es un $p-$subgrupo de Sylow con $P < H < G$, entonces usando la fórmula de los índices:

$$[G : P] = [G : H][H : P]$$

En dicho caso, $[H : P] \mid [G : P] = m$. Si suponemos que p divide a $[H : P]$, entonces p dividirá a $[G : P] = m$, pero $\text{mcd}(p, m) = 1$, por lo que p no puede dividir a $[H : P]$.

Es decir, si encontramos un subgrupo H de G que contiene a P como subgrupo, entonces p no dividirá a $[H : P]$.

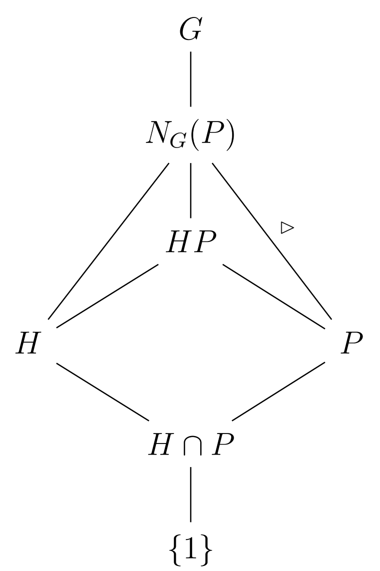
El siguiente Lema también recibe el nombre de Segundo Teorema de Sylow, aunque nos reservamos este nombre para el resultado que se demuestra a partir del Lema.

Lema 5.14. *Si P es un $p-$subgrupo de Sylow de un grupo finito G y H es un $p-$subgrupo de $N_G(P)$, entonces H está contenido en P.*

Es decir, los $p-$subgrupos del normalizador de un $p-$subgrupo de Sylow estarán contenidos en dicho $p-$subgrupo de Sylow.

Demostración. Como $P \lhd N_G(P)$ (gracias a la Proposición 5.8) y $H < N_G(P)$, podemos aplicar el Segundo Teorema de Isomorfía, obteniendo que:

- $HP < N_G(P)$.
- $P \lhd HP$.
- $H \cap P \lhd H$.



Así como que:

$$HP/P \cong H/H \cap P$$

Llamando $r = [HP : P] = [H : H \cap P]$, distinguimos casos:

- Si $r = 1$, entonces $HP = P$, de donde $H < P$, como queríamos demostrar.
- Si $r > 1$, estamos en la situación de la observación anterior:

  $$P < HP < N_G(P) \qquad [N_G(P) : P] = [N_G(P) : HP][HP : P]$$

  Si suponemos que p divide a $[HP : P]$, entonces p dividirá a $[N_G(P) : P]$, contradicción (puesto que P era un $p-$*subgrupo* de Sylow de G, luego lo será de $N_G(P)$, por ser $|N_G(P)| \leqslant |G|$). Tenemos entonces que $p \nmid [HP : P] = r$.

  Por otro lado, como la intersección de $p-$grupos sigue siendo un $p-$grupo (basta aplicar la definición de $p-$grupo) y el cociente de $p-$grupos sigue siendo un $p-$grupo (gracias al Corolario 5.10.1), tendremos que $H/(H \cap P)$ es un $p-$grupo, con $|H/(H \cap P)| = r > 1$, por lo que si $1 \neq x \in H/(H \cap P)$, tendremos que $\exists k \in \mathbb{N}$ de forma que $O(x) = p^k$, con $p^k \mid r$. Por tanto, $\exists m \in \mathbb{N}$ de forma que:

  $$r = p^k m$$

  De donde $p \mid r$, contradicción, ya que habíamos visto antes que $p \nmid r$.

Como vemos, la única posibilidad es $r = 1$. $\square$

Teorema 5.15 (Segundo Teorema de Sylow)**.** *Sea G un grupo finito, p un número primo, supongamos que $|G| = p^k m$ con $\operatorname{mcd}(p, m) = 1$ y n_p denota el número de $p-$subgrupos de Sylow de G, entonces:*

i) *Todo $p-$subgrupo de G está contenido (como subgrupo) en un $p-$subgrupo de Sylow de G.*

ii) *Cualesquiera dos $p-$subgrupos de Sylow de G son conjugados.*

iii) *$n_p \mid m$ y $n_p \equiv 1 \mod p$.*

Demostración. Demostramos cada apartado:

i) Si llamamos $S = Syl_p(G) = \{P \mid P \text{ es un } p\text{−subgrupo de Sylow de } G\}$, consideramos la acción por conjugación $G \times S \to S$ dada por:

$$ac(g, P) = {}^gP = gPg^{-1} \in S$$

Que estará bien definida, ya que:

- Sabemos por la Proposición 3.1 que $gPg^{-1} < G$, para todo $g \in G$.
- Fijado $g \in G$, la aplicación

  $$\begin{array}{rccc} \phi_g: & P & \longrightarrow & gPg^{-1} \\ & x & \longmapsto & gxg^{-1} \end{array}$$

  Es biyectiva:

- Si $gxg^{-1} \in gPg^{-1}$, entonces $\phi_g(x) = gxg^{-1}$, luego ϕ_g es sobreyectiva.
- Si $gxg^{-1} = gyg^{-1}$, entonces $x = y$, por lo que ϕ_g es inyectiva.

Por lo que $|P| = |gPg^{-1}|$, luego gPg^{-1} seguirá siendo un $p-$subgrupo de Sylow de G.

Es evidente que es una acción. Sea $P_1 \in S$, estudiemos su órbita y estabilizador:

$$Orb(P_1) = \{gP_1g^{-1} \mid g \in G\}$$
$$Stab_G(P_1) = \{g \in G \mid gP_1g^{-1} = P_1\} = N_G(P_1)$$

Tenemos:

- $|Orb(P_1)| = [G : N_G(P_1)]$.
- $P_1 \lhd N_G(P_1) < G$.
- $[G : P_1] = [G : N_G(P_1)][N_G(P_1) : P_1]$.

Por lo que $|Orb(P_1)|$ divide a $[G : P_1] = m$, existirá $t \in \mathbb{N}$ de forma que $m = |Orb(P_1)|t$. Además, como $P_1 \in S$, $\text{mcd}(m, p) = 1$. Se tiene por tanto que:

$$\text{mcd}(|Orb(P_1)|t, p) = 1 \Longrightarrow \text{mcd}(|Orb(P_1)|, p) = 1$$

Propiedad que usaremos luego. Ahora, veamos que todo $p-$subgrupo está contenido en un $p-$subgrupo de Sylow. Para ello, sea H un $p-$subgrupo de G, consideramos la acción sobre la órbita de $P_1 \in S$, $ac : H \times Orb(P_1) \to Orb(P_1)$, dada por:

$$ac(h, P) = {}^hP = hPh^{-1} \in Orb(P_1)$$

Que estará bien definida gracias a la definición de $Orb(P_1)$. Si tomamos $P \in Orb(P_1)$, tendremos que:

$$Stab_H(P) = \{h \in H \mid hPh^{-1} = P\} = H \cap N_G(P) < H$$

Además, también tendremos que $H \cap N_G(P) < P$, por ser $H \cap N_G(P) < N_G(P)$ un $p-$subgrupo y aplicar el Lema anterior. En definitiva, $H \cap N_G(P) < H \cap P$ y como tenemos $P \lhd N_G(P)$, llegamos a:

$$Stab_H(P) = H \cap N_G(P) < H \cap P < H \cap N_G(P)$$

De donde tenemos que $H \cap N_G(P) = H \cap P$. Usando la fórmula de clases:

$$|Orb(P_1)| = \sum_{P \in \Gamma} |Orb(P)| = \sum_{P \in \Gamma} [H : Stab_H(P)] = \sum_{P \in \Gamma} [H : H \cap P]$$

Y como cada sumando $[H : H \cap P]$ con $P \in \Gamma$ divide a $|H|$, que es una potencia de p (H era un $p-$subgrupo) y teníamos que $p \nmid |Orb(P_1)|$ (demostramos anteriormente que $\text{mcd}(|Orb(P_1)|, p) = 1$), ha de existir $P \in Orb(P_1) \subseteq S$ de forma que:

$$[H : H \cap P] = 1$$

De donde $H = H \cap P$, por lo que $H < P$.

ii) Veamos ahora que cualesquiera dos $p-$subgrupos de Sylow de G son conjugados. Para ello, sean P_1, P_2 dos $p-$subgrupos de Sylow de G, hemos visto en el apartado anterior que si $H = P_2 < G$ es un $p-$subgrupo de G, entonces H está contenido en un subgrupo de Sylow, por lo que $\exists P$, un $p-$subgrupo de Sylow de G, conjugado de P_1 (por lo que hemos demostrado en el apartado anterior), de forma que $P_2 < P$, pero $|P| = |P_2|$, luego $P_2 = P$ y llegamos a que P_1 y P_2 son conjugados.

iii) Veamos ahora que $n_p \mid m$ y que $n_p \equiv 1 \mod p$.

En el apartado *ii)* hemos visto que $Orb(P_1) = S$, luego:

$$n_p = |S| = |Orb(P_1)| = [G : N_G(P_1)]$$

Y tenemos que:

$$m = [G : P_1] = [G : N_G(P_1)][N_G(P_1) : P_1] = n_p[N_G(P_1) : P_1]$$

Por lo que $n_p \mid m$.

Si en el apartado *i)* tomamos $H = P_1$ (el de la demostración anterior), llegamos a que:

$$n_p = |Orb(P_1)| = \sum_{P \in \Gamma} [P_1 : P_1 \cap P]$$

Y los índices $[P_1 : P_1 \cap P]$ pueden ser múltiplos de p o 1, por ser cociente de $p-$subgrupos:

- Si $[P_1 : P_1 \cap P] = 1$, entonces $P_1 = P_1 \cap P$, por lo que $P < P_1$, pero como $|P| = |P_1|$, tenemos que $P = P_1$.

Por lo que:

$$n_p = 1 + \sum_{P \in \Gamma \setminus \{P_1\}} [P_1 : P_1 \cap P]$$

Con $[P_1 : P_1 \cap P]$ múltiplos de p para todo $P \in \Gamma \setminus \{P_1\}$, por lo que $\exists k \in \mathbb{N}$ de forma que:

$$n_p = 1 + pk$$

Es decir, $n_p \equiv 1 \mod p$.

□

Ejemplo. Vamos a calcular grupos de Sylow:

- En $C_n = \langle x \mid x^n = 1 \rangle$ para $n \in \mathbb{N}$, por el Primer Teorema de Sylow tendremos grupos de Sylow de las potencias máximas de los primos que aparecen en la factorización de n. Es decir, si n se descompone como:

  $$n = p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}$$

  Para cada $k \in \{1, 2, \dots, m\}$, existe un p_k-subgrupo de Sylow, que será cíclico y tendrá orden $p_k^{t_k}$, luego los subgrupos de Sylow serán de la forma: $C_{p_k^{t_k}}$.

- En S_3, como $|S_3| = 6 = 2 \cdot 3$, tendremos $2-$subgrupos de Sylow y $3-$subgrupos de Sylow. Veamos cuántos tenemos a partir del Segundo Teorema de Sylow:

  - $2-$subgrupos de Sylow, es decir, subgrupos de orden 2 de S_3. Como $n_2 \mid 3$ y ha de ser $n_2 \equiv 1 \mod 2$, tendremos que n_2 valdrá 1 o 3.

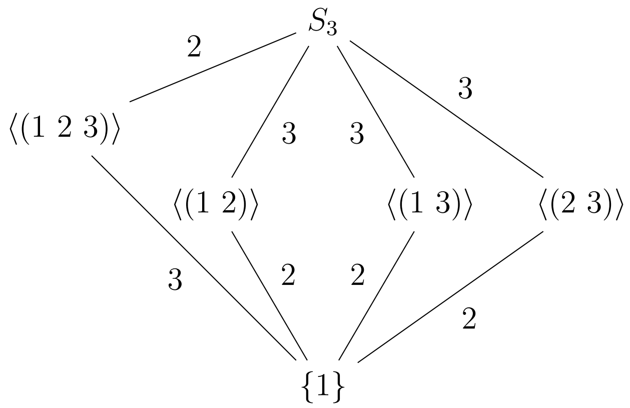


Figura 5.1: Diagrama de Hasse para los subgrupos de S_3.

  Si observamos el retículo de subgrupos de S_3, observamos que hay 3 subgrupos distintos de orden 2, por lo que tendremos que $n_2 = 3$.

  - Los $3-$subgrupos de Sylow será un subgrupo de orden 3 de S_3, que será el único que hay: $\langle(1\ 2\ 3)\rangle = A_3 \lhd S_3$.

    Si queremos verlo por el Segundo Teorema de Sylow:

$$\left.\begin{array}{r} n_3 \mid 2 \\ n_3 \equiv 1 \mod 3 \end{array}\right\} \Longrightarrow n_3 = 1$$

- En A_4, tenemos $|A_4| = 12 = 2^2 \cdot 3$. Tendremos:

  - $2-$subgrupo de Sylow de orden 4. Busquemos por el Segundo Teorema de Sylow:

$$\left.\begin{array}{r} n_2 \mid 3 \\ n_2 \equiv 1 \mod 2 \end{array}\right\} \Longrightarrow n_2 \in \{1, 3\}$$

    Observando el retículo de A_4, concluimos que $n_2 = 1$, ya que el único subgrupo de orden 4 de A_4 es V, que es normal en A_4.

  - $3-$subgrupo de Sylow de orden 3:

$$\left.\begin{array}{r} n_3 \mid 4 \\ n_3 \equiv 1 \mod 3 \end{array}\right\} \Longrightarrow n_3 \in \{1, 4\}$$

    Y observando el retículo de A_4, serán los 4 subgrupos de A_4 generados por los $3-$ciclos:

$$\langle(1\ 2\ 3)\rangle \qquad \langle(1\ 2\ 4)\rangle \qquad \langle(1\ 3\ 4)\rangle \qquad \langle(2\ 3\ 4)\rangle$$

- En S_4, $|S_4| = 24 = 2^3 \cdot 3$:

- Para los $2-$subgrupos:

$$\left.\begin{array}{r} n_2 \mid 3 \\ n_2 \equiv 1 \mod 2 \end{array}\right\} \Longrightarrow n_2 \in \{1, 3\}$$

Si suponemos que $n_2 = 1$, sea $Q < S_4$ un subgrupo con $|Q| = 8$, será el único $2-$subgrupo de Sylow. En dicho caso, todas las trasposiciones de S_4 deben estar contenidas en Q, ya que $\langle(x\ y)\rangle$ es un $2-$grupo (es un grupo de orden 2) y todo $2-$grupo está contenido en un $2-$grupo de Sylow (gracias al Segundo Teorema de Sylow), por lo que Q contiene todas las trasposiciones. Sin embargo, como $S_4 = \langle\{(x\ y) \mid x, y \in \{1, 2, 3, 4\}\}\rangle$, tendremos que $Q = S_4$, contradicción.

Por tanto, tenemos $n_2 = 3$, tenemos tres $2-$subgrupos de Sylow: Q_1, Q_2 y Q_3. El grupo de Klein V es un $2-$subgrupo, por lo que va a estar contenido en algún Q_k (para $k \in \{1, 2, 3\}$). Supongamos que $V < Q_1$. Como todos ellos son conjugados, $\exists \alpha, \beta \in S_4$ de forma que:

$$Q_2 = \alpha Q_1 \alpha^{-1}$$
$$Q_3 = \beta Q_1 \beta^{-1}$$

Y si multiplicamos (como $V \lhd S_4$):

$$V = \alpha V \alpha^{-1} < \alpha Q_1 \alpha^{-1} = Q_2$$
$$V = \beta V \beta^{-1} < \beta Q_1 \beta^{-1} = Q_3$$

De donde deducimos que $V < Q_k$ para todo $k \in \{1, 2, 3\}$. Los Q_k contendrán a V y deben repartirse entre ellos a las trasposiciones. Realizando las cuentas pertinentes, podemos llegar a deducir que:

$$Q_1 = V\langle(1\ 2)\rangle$$
$$Q_2 = V\langle(1\ 3)\rangle$$
$$Q_3 = V\langle(1\ 4)\rangle$$

- Para los $3-$subgrupos de Sylow:

$$\left.\begin{array}{r} n_3 \mid 8 \\ n_3 \equiv 1 \mod 3 \end{array}\right\} \Longrightarrow n_3 \in \{1, 4\}$$

Como sabemos de la existencia de varios elementos de orden 3, los $3-$subgrupos de Sylow de S_4 serán:

$$\langle(1\ 2\ 3)\rangle, \langle(1\ 2\ 4)\rangle, \langle(1\ 3\ 4)\rangle, \langle(2\ 3\ 4)\rangle$$

Corolario 5.15.1. *Sea P un $p-$subgrupo de Sylow de un grupo finito G. Entonces:*

$$P \text{ es el único } p-\text{subgrupo de Sylow} \Longleftrightarrow P \lhd G$$

Demostración. Como en el Segundo Teorema de Sylow vimos que el conjugado de un $p-$subgrupo de Sylow es un $p-$subgrupo de Sylow y que todos los $p-$subgrupos de Sylow son conjugados entre sí, acabamos de justificar $(*)$ en:

$$P \text{ es el único } p-\text{subgrupo de Sylow de } G \overset{(*)}{\Longleftrightarrow} gPg^{-1} = P \quad \forall g \in G \Longleftrightarrow P \lhd G$$

La segunda equivalencia se tiene por una caracterización vista de los subgrupos normales. □

Ejemplo. Todo grupo de orden 35 es resoluble.

Demostración. Sea G un grupo con $|G| = 35 = 5 \cdot 7$, vemos que:

$$\left.\begin{array}{r} n_7 \mid 5 \\ n_7 \equiv 1 \mod 5 \end{array}\right\} \Longrightarrow n_7 = 1$$

En dicho caso, tenemos un único $7-$subgrupo de Sylow $H < G$, que tendrá orden 7 y por el Corolario anterior será normal en G. En dicho caso, sabemos que será isomorfo a $\mathbb{Z}_7$. Como los grupos abelianos son resolubles, tenemos que H es resoluble. Si consideramos el cociente:

$$|G/H| = \frac{|G|}{|H|} = \frac{5 \cdot 7}{7} = 5$$

Por lo que $G/H \cong \mathbb{Z}_5$ y G/H será resoluble por ser isomorfo a un grupo abeliano. Deducimos que G es resoluble, por ser H y G/H resolubles. □

Esta estrategia que hemos seguido para demostrar que cualquier grupo de orden 35 es resoluble puede seguirse de forma análoga para demostrar que otros grupos de cierto orden son siempre resolubles.

Teorema 5.16. *Sea G un grupo finito en el que todos sus subgrupos de Sylow son normales, entonces G es el producto directo interno de sus subgrupos de Sylow:*

$$G \cong \prod_{H \in Syl(G)} H$$

Demostración. En la caracterización de producto directo interno para una cantidad finita de subgrupos (Teorema 3.33), vimos que G era producto directo interno de todos ellos (los llamaremos H_i con $i \in \{1, \ldots, n\}$) si y solo si:

- $H_i \lhd G$ para todo $i \in \{1, \ldots, n\}$.
- $H_1 H_2 \ldots H_n = G$.
- $(H_1 \ldots H_{i-1}) \cap H_i = \{1\}$, para todo $i \in \{2, \ldots, k\}$

Basta pues, demostrar estos 3 puntos. Supuesto que $|G| = p_1^{n_1} \ldots p_k^{n_k}$, llamamos P_i al único p_i-subgrupo de Sylow, para todo $i \in \{1, \ldots, k\}$.

- Por hipótesis, tendremos que $P_i \lhd G$ para todo $i \in \{1, \ldots, k\}$.
- También:
$$|P_1 P_2 \ldots P_K| = |P_1||P_2| \ldots |P_k| = |G|$$
Y como tenemos siempre que $P_1 P_2 \ldots P_k < G$, deducimos que $P_1 P_2 \ldots P_k = G$.
- Fijado $i \in \{2, \ldots, k\}$, veamos que $(P_1 \ldots P_{i-1}) \cap P_i = \{1\}$. Para ello, sea $x \in (P_1 \ldots P_{i-1}) \cap P_i$, tenemos:
$$\left.\begin{array}{l} O(x) \mid |P_1 \ldots P_{i-1}| = p_1^{n_1} \ldots p_{i-1}^{n_{i-1}} \\ O(x) \mid |P_i| = p_i^{n_i} \end{array}\right\} \Longrightarrow O(x) = 1 \Longrightarrow x = 1$$

□

Observación. Notemos que cualquier grupo abeliano finito es producto directo interno de sus subgrupos de Sylow, ya que el Primer Teorema de Sylow nos garantiza su existencia y por ser el grupo abeliano siempre tendremos que dichos subgrupos son normales.

6. Clasificación de grupos abelianos finitos

El objetivo final del tema es demostrar los teoremas de estructura de los grupos abelianos finitos, que permiten clasificar todos los grupos de este tipo según su orden. De esta forma, dado un grupo abeliano finito, la clasificación que realizaremos en este tema nos permitirá encontrar un grupo abeliano finito bien conocido al que el grupo dado sea isomorfo.

6.1. Descomposiciones como producto de grupos cíclicos

Como toma de contacto, serán de especial relevancia dos resultados que ya vimos en Capítulos anteriores, como:

1. En la Proposición 3.35 vimos que:

$$C_n \oplus C_m \cong C_{nm} \Longleftrightarrow \text{mcd}(n, m) = 1$$

2. En el Teorema 5.16 vimos que si G es un grupo finito en el que todos sus subgrupos de Sylow son únicos, entonces G es producto directo interno de todos ellos:

$$G \cong P_1 \oplus P_2 \oplus \ldots \oplus P_k$$

Como trabajaremos con subgrupos abelianos, será usual usar la notación de $\oplus$ en lugar de la de $\times$.

Teorema 6.1 (Estructura de los $p-$grupos abelianos finitos)**.**
Sea A un $p-$grupo abeliano finito con orden $|A| = p^n$ para $n \geqslant 1$, entonces existen enteros $\beta_1 \geqslant \beta_2 \geqslant \ldots \geqslant \beta_t \geqslant 1$ de forma que:

$$\beta_1 + \beta_2 + \ldots + \beta_t = n \quad y \quad A \cong C_{p^{\beta_1}} \oplus C_{p^{\beta_2}} \oplus \ldots \oplus C_{p^{\beta_t}}$$

Además, esta expresión es única, es decir, si existen $\alpha_1 \geqslant \alpha_2 \geqslant \ldots \geqslant \alpha_s \geqslant 1$ de forma que:

$$\alpha_1 + \alpha_2 + \ldots + \alpha_s = n \quad y \quad A \cong C_{p^{\alpha_1}} \oplus C_{p^{\alpha_2}} \oplus \ldots \oplus C_{p^{\alpha_s}}$$

entonces $s = t$ y $\alpha_k = \beta_k$, para todo $k \in \{1, \ldots, t\}$.

Observación. Notemos que lo que estamos haciendo es tomar particiones de n de la forma β_i, y este Teorema nos dice que el $p-$grupo puede escribirse de forma única salvo isomorfismos como producto de ciertos grupos cíclicos.
Es decir, existen tantos $p-$grupos abelianos de orden p^n como particiones tengamos del número n, salvo isomorfismos. Por tanto, conocemos ya cómo son todos los $p-$grupos abelianos finitos.

Ejemplo. Por ejemplo:

- Para saber los grupos abelianos finitos de orden $8 = 2^3$ que hay (salvo isomorfismos), calculamos cada una de las posibles particiones del número 3 (el exponente del 2):

$$\begin{aligned} 3 &\longrightarrow A \cong C_8 \\ 2,1 &\longrightarrow A \cong C_4 \oplus C_2 \\ 1,1,1 &\longrightarrow A \cong C_2 \oplus C_2 \oplus C_2 \end{aligned}$$

- Para saber los grupos abelianos finitos de orden $81 = 3^4$, calculamos cada una de las particiones de 4:

$$\begin{aligned} 4 &\longrightarrow A \cong C_{81} \\ 3,1 &\longrightarrow A \cong C_{27} \oplus C_3 \\ 2,2 &\longrightarrow A \cong C_9 \oplus C_9 \\ 2,1,1 &\longrightarrow A \cong C_9 \oplus C_3 \oplus C_3 \\ 1,1,1,1 &\longrightarrow A \cong C_3 \oplus C_3 \oplus C_3 \oplus C_3 \end{aligned}$$

6.1.1. Descomposición cíclica primaria

Teorema 6.2 (Estructura de los grupos abelianos finitos)**.**
Sea A un grupo abeliano finito con $|A| = p_1^{\gamma_1} \dots p_k^{\gamma_k}$ siendo p_i primo $\forall i \in \{1, \dots, k\}$, entonces existen $t_1, t_2, \dots, t_k \in \mathbb{N}$ de forma que para el $i-$ésimo entero t_i existen

$$n_{i1} \geqslant n_{i2} \geqslant \dots \geqslant n_{it_i} \geqslant 1$$

Con:

$$n_{i1} + n_{i2} + \dots + n_{it_i} = \gamma_i$$

Para dichos n_{ij} con $j \in \{1, \dots, t_i\}$ y $i \in \{1, \dots, k\}$ podremos escribir:

$$A \cong \bigoplus_{i=1}^{k} \left(\bigoplus_{j=1}^{t_i} C_{p_i^{n_{ij}}} \right)$$

Y la descomposición es única.

Demostración. Si A es abeliano y finito, entonces todos sus $p-$subgrupos de Sylow son normales, luego podemos escribir:

$$A = P_1 \oplus P_2 \oplus \dots \oplus P_k$$

Siendo $\{P_1, P_2, \ldots, P_k\}$ el conjunto de todos sus $p-$subgrupos de Sylow, de forma que $|P_i| = p_i^{r_i}$, para todo $i \in \{1, \ldots, k\}$. Como cada P_i es un p_i-subgrupo abeliano finito, aplicando el Teorema 6.1, podemos encontrar:

$$n_{i1} \geqslant n_{i2} \geqslant \ldots \geqslant n_{it_i} \geqslant 1 \qquad n_{i1} + n_{i2} + \ldots + n_{it_i} = \gamma_i$$

De forma que podamos escribir:

$$P_i = \bigoplus_{j=1}^{t_i} C_{p_i^{n_{ij}}} \qquad \forall i \in \{1, \ldots, k\}$$

De donde tenemos la expresión de la tesis. □

Definición 6.1. Sea A un grupo abeliano finito, el Teorema 6.2 motiva las siguientes definiciones:

- La única descomposición obtenida para A en dicho teorema recibirá el nombre de descomposición cíclica primaria de A.
- A las potencias $p_i^{n_{ij}}$ obtenidas (usando la notación del Teorema), las llamaremos divisores elementales de A.
- A cada $p-$subgrupo de Sylow de A lo llamaremos componente $p-$primaria de A.

Ejemplo. Si tenemos un grupo finito abeliano A con $|A| = 360 = 2^3 \cdot 3^2 \cdot 5$, buscamos las posibles descomposiciones cíclicas primarias de A, que obtenemos fácilmente tras combinar todas las particiones posibles de los exponentes de los primos que aparecen en la descomposición de $|A|$, es decir, las particiones de 3, 2 y 1:

Divisores elementales	Descomposición cíclica primaria
$2^3\ 3^2\ 5$	$C_8 \oplus C_9 \oplus C_5$
$2^2\ 2\ 3^2\ 5$	$C_4 \oplus C_2 \oplus C_9 \oplus C_5$
$2\ 2\ 2\ 3^2\ 5$	$C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5$
$2^3\ 3\ 3\ 5$	$C_8 \oplus C_3 \oplus C_3 \oplus C_5$
$2\ 2^2\ 3\ 3\ 5$	$C_2 \oplus C_4 \oplus C_3 \oplus C_3 \oplus C_5$
$2\ 2\ 2\ 3\ 3\ 5$	$C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$

Estas sería todas las descomposiciones cíclicas primarias de A. Es decir, dado cualquier grupo de orden 360, sabemos que será isomorfo a alguno de los grupos que aparecen a la derecha de la tabla.

Sin embargo, si recordamos la Proposición 3.35, podemos escribir (multiplicando aquellos cíclicos de mayor orden que sean primos relativos):

$$C_8 \oplus C_9 \oplus C_5 \cong C_{360}$$
$$C_4 \oplus C_2 \oplus C_9 \oplus C_5 \cong C_{180} \oplus C_2$$
$$C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5 \cong C_{90} \oplus C_2 \oplus C_2$$
$$C_8 \oplus C_3 \oplus C_3 \oplus C_5 \oplus C_8 \cong C_{120} \oplus C_3$$
$$C_2 \oplus C_4 \oplus C_3 \oplus C_3 \oplus C_5 \cong C_{60} \oplus C_6$$
$$C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5 \cong C_{30} \oplus C_6 \oplus C_2$$

Corolario 6.2.1. *Si A es un grupo abeliano finito con $|A| = p_1 p_2 \dots p_k = n$, entonces salvo isomorfismo, el único grupo abeliano de orden n es el cíclico C_n.*

Demostración. Utilizando el Teorema 6.2, podemos escribir:

$$A \cong C_{p_1} \oplus C_{p_2} \oplus \dots \oplus C_{p_k}$$

Y como $\text{mcd}(p_i, p_j) = 1$ para cada $i, j \in \{1, \dots, k\}$ con $i \neq j$, tenemos que:

$$C_{p_1} \oplus C_{p_2} \oplus \dots \oplus C_{p_k} = C_{p_1 p_2 \dots p_k} = C_n$$

□

6.1.2. Descomposición cíclica

Teorema 6.3 (Descomposición cíclica de un grupo abeliano finito)**.**
Si A es un grupo abeliano finito, entonces existen unos únicos $d_1, d_2, \dots, d_t \in \mathbb{N}$ de forma que:

$$d_1 d_2 \dots d_t = |A| \qquad y \qquad d_i \mid d_j, \quad \forall j \leqslant i$$

Para los que se tiene que:

$$A \cong C_{d_1} \oplus C_{d_2} \oplus \dots \oplus C_{d_t}$$

Demostración. Supuesto que $|A| = p_1^{r_1} \dots p_k^{r_k}$ es la descomposición de $|A|$ en primos, si usamos la descomposición que nos da el Teorema 6.2, existen $t_1, t_2, \dots, t_k \in \mathbb{N}$ y

$$\begin{aligned} m_{i1} \geqslant m_{i2} \geqslant \dots \geqslant m_{it_i} \geqslant 1 \\ m_{i1} + m_{i2} + \dots + m_{it_i} = r_i \\ \forall i \in \{1, \dots, k\} \end{aligned}$$

De forma que:

$$A \cong \bigoplus_{i=1}^{k} \left(\bigoplus_{j=1}^{t_i} C_{p_i^{m_{ij}}} \right)$$

Sea $t = \text{máx}\{t_1, t_2, \dots, t_k\}$, definimos:

$$n_{ij} = \left\{ \begin{array}{ll} m_{ij} & \text{si } j \leqslant t_i \\ 0 & \text{si } j > t_i \end{array} \right. \qquad \forall j \in \{1, \dots, t\}, \in i\{1, \dots, k\}$$

Observemos que no hemos hecho mas que extender la anterior tabla dentada $(m_{ij})_{\substack{j \in \{1,\dots,t_i\} \\ i \in \{1,\dots,k\}}}$ a la tabla $k \times t$ $(n_{ij})_{\substack{j \in \{1,\dots,t\} \\ i \in \{1,\dots,k\}}}$, rellenando con ceros los huecos que no teníamos. De esta forma, si consideramos la matriz que en la entrada (i, j) tiene $p_i^{n_{ij}}$:

$$\begin{pmatrix} p_1^{n_{11}} & p_1^{n_{12}} & \dots & p_1^{n_{1t}} \\ p_2^{n_{21}} & p_2^{n_{22}} & \dots & p_2^{n_{2t}} \\ \vdots & \vdots & \ddots & \vdots \\ p_k^{n_{k1}} & p_k^{n_{k2}} & \dots & p_k^{n_{kt}} \end{pmatrix}$$

Tenemos que A es el producto directo de los grupos cíclicos de órdenes las entradas de la tabla anterior (ya que $A \cong A \oplus C_1 = A \oplus \{1\}$). Si tomamos el producto de los elementos de cada columna:

$$\begin{aligned}
d_1 &= p_1^{n_{11}} p_2^{n_{21}} \dots p_k^{n_{k1}} \\
d_2 &= p_1^{n_{12}} p_2^{n_{22}} \dots p_k^{n_{k2}} \\
&\vdots \\
d_t &= p_1^{n_{1t}} p_2^{n_{2t}} \dots p_k^{n_{kt}}
\end{aligned}$$

Efectivamente, tendremos que:

$$d_1 d_2 \dots d_t = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k} = |A|$$

Fijado $i \in \{1, \dots, k\}$, como $n_{ij} \geqslant n_{i(j+1)}$ (por la construcción realizada) para todo $j \in \{1, \dots, t-1\}$, tendremos entonces que si $u, v \in \{1, \dots, t\}$ con $u \leqslant v$, los exponentes de los primos en d_u serán mayores que los exponentes de los primos en d_v, por lo que $d_v \mid d_u$, lo que se verifica para todo $u \leqslant v$. Además, tendremos que:

$$\begin{aligned}
C_{d_1} &\cong C_{p_1^{n_{11}}} \oplus C_{p_2^{n_{21}}} \oplus \dots \oplus C_{p_k^{n_{k1}}} \\
&\vdots \\
C_{d_t} &\cong C_{p_1^{n_{1t}}} \oplus C_{p_2^{n_{2t}}} \oplus \dots \oplus C_{p_k^{n_{kt}}}
\end{aligned}$$

De donde $A \cong C_{d_1} \oplus C_{d_2} \oplus \dots \oplus C_{d_t}$. La unicidad de la descomposición viene de la unicidad de la descomposición del Teorema 6.2 más la construcción de los d_j realizada. □

Definición 6.2. Sea A un grupo abeliano finito, el Teorema 6.3 motiva las siguientes definiciones:

- La única descomposición obtenida para A en dicho teorema recibirá el nombre de descomposición cíclica de A.
- Los enteros d_j obtenidos recibirán el nombre de factores invariantes.

Ejemplo. Recuperando el ejemplo anterior, si tenemos A, un grupo abeliano finito con $|A| = 360 = 2^3 \cdot 3^2 \cdot 5$, buscaremos escribir para cada conjunto de divisores elementales las respectivas descomposiciones cíclicas:

- Para la partición $\{2^3, 3^2, 5\}$, teníamos la descomposición cíclica primaria:

  $$A \cong C_8 \oplus C_9 \oplus C_5$$

  Que siguiendo con la construcción realizada en la demostración anterior, nos da la tabla:

  $$\begin{pmatrix} 2^3 \\ 3^2 \\ 5 \end{pmatrix}$$

  Por tanto, obtenemos el factor invariante:

  $$d_1 = 2^3 \cdot 3^2 \cdot 5$$

  Por lo que la descomposición cíclica de A será $A \cong C_{360}$.

- Para la partición $\{2^2, 2, 3^2, 5\}$, la descomposición cíclica primaria fue:

$$A \cong C_4 \oplus C_2 \oplus C_9 \oplus C_5$$

En este caso, tendremos $t = \text{máx}\{2, 1, 1\} = 2$, por lo que tendremos dos factores invariantes, que podemos calcular de forma fácil a partir de la tabla:

$$\begin{pmatrix} 2^2 & 2 \\ 3^2 & 1 \\ 5 & 1 \end{pmatrix}$$

Por lo que tendremos (los productos de las columnas):

$$d_1 = 2^2 \cdot 3^2 \cdot 5 = 180$$
$$d_2 = 2 \cdot 1 \cdot 1 = 2$$

Y la descomposición cíclica es:

$$A \cong C_{180} \oplus C_2$$

- Para la descomposición $\{2, 2, 2, 3^2, 5\}$, teníamos:

$$A \cong C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5$$

Y tendremos $t = 3$, con:

$$\begin{pmatrix} 2 & 2 & 2 \\ 3^2 & 1 & 1 \\ 5 & 1 & 1 \end{pmatrix}$$

Por lo que:

$$A \cong C_{90} \oplus C_2 \oplus C_2$$

- Para $\{2^3, 3, 3, 5\}$, teníamos:

$$A \cong C_8 \oplus C_3 \oplus C_3 \oplus C_5$$

Y tenemos:

$$\begin{pmatrix} 2^3 & 1 \\ 3 & 3 \\ 5 & 1 \end{pmatrix}$$

La descomposición cíclica será:

$$A \cong C_{120} \oplus C_3$$

- Para $\{2^2, 2, 3, 3, 5\}$, teníamos:

$$A \cong C_4 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$$

Y tenemos:

$$\begin{pmatrix} 2^2 & 2 \\ 3 & 3 \\ 5 & 1 \end{pmatrix}$$

Por lo que tenemos la descomposición cíclica:

$$A \cong C_{60} \oplus C_6$$

- Para $\{2, 2, 2, 3, 3, 5\}$ teníamos:

$$A \cong C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$$

Y tenemos:

$$\begin{pmatrix} 2 & 2 & 2 \\ 3 & 3 & 1 \\ 5 & 1 & 1 \end{pmatrix}$$

Por lo que la descomposición cíclica será:

$$A \cong C_{30} \oplus C_6 \oplus C_2$$

Ejemplo. Sea A un grupo abeliano finito con $|A| = 180 = 2^2 \cdot 3^2 \cdot 5$, buscamos hayar sus posibles descomposiciones cíclicas y descomposiciones cíclicas primarias:

Divisores elementales	desc. cíclica primaria	factores invariantes	desc. cíclica
$\{2^2, 3^2, 5\}$	$C_4 \oplus C_9 \oplus C_5$	$d_1 = 2^2 \cdot 3^2 \cdot 5 = 180$	C_{180}
$\{2, 2, 3^2, 5\}$	$C_2 \oplus C_2 \oplus C_9 \oplus C_5$	$d_1 = 2 \cdot 3^2 \cdot 5 = 90$ $d_2 = 2$	$C_{90} \oplus C_2$
$\{2^2, 3, 3, 5\}$	$C_4 \oplus C_3 \oplus C_3 \oplus C_5$	$d_1 = 2^2 \cdot 3 \cdot 5 = 60$ $d_2 = 3$	$C_{60} \oplus C_3$
$\{2, 2, 3, 3, 5\}$	$C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$	$d_1 = 2 \cdot 3 \cdot 5 = 30$ $d_2 = 2 \cdot 3 = 6$	$C_{30} \oplus C_6$

Ejemplo. Listar los órdenes de todos los elementos de un grupo abeliano de orden 8.

Sea A un grupo abeliano finito de orden $8 = 2^3$, entonces lo podemos clasificar en:

- C_8, donde usaremos la Proposición 2.18 y el Corolario 2.18.2:
  - $O(0) = 1$.
  - Los elementos $1, 3, 5$ y 7 tienen orden 8.
  - $O(2) = {}^8/_{\text{mcd}(2,8)} = 4$.
  - $O(4) = {}^8/_{\text{mcd}(4,8)} = 2$.
  - $O(6) = {}^8/_{\text{mcd}(6,8)} = 4$.
- $C_4 \oplus C_2$, aplicamos que $O(a, b) = \text{mcm}(O(a), O(b))$: Como los órdenes de los elementos en C_4 son $\{1, 2, 4\}$ y en C_2 son $\{1, 2\}$, las posibilidades que tenemos son: $\{1, 2, 4\}$. Si primero listamos los órdenes de los elementos en C_4:
  - $O(0) = 1$.
  - $O(1) = 4$.
  - $O(3) = 4$.
  - $O(2) = 2$.

  Podemos ver de forma fácil que:
  - $O(0, 0) = 1$.

- $O(0,1) = 2$.
- $O(1,b) = 4 = O(3,b)$, $\forall b \in C_2$
- $O(2,b) = 2$, $\forall b \in C_2$.

- $C_2 \oplus C_2 \oplus C_2$, los órdenes son $\{1,2\}$ y todos tienen orden 2 salvo el elemento $(0,0,0)$, que tiene orden 1.

Ejemplo. Listar los órdenes de todos los elementos de un grupo abeliano de orden 12.

Sea A con $|A| = 12 = 2^2 \cdot 3$, tenemos entonces que $A \cong \mathbb{Z}_{12}$ o $A \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2$.

- En $\mathbb{Z}_{12}$:
  - $O(0) = 1$.
  - $1, 5, 7$ y 11 tienen orden 12.
  - $O(2) = {}^{12}/_{\text{mcd}(2,12)} = 6$.
  - $O(3) = {}^{12}/_{\text{mcd}(3,12)} = 4$.
  - $O(4) = {}^{12}/_{\text{mcd}(4,12)} = 3$.
  - $O(6) = {}^{12}/_{\text{mcd}(6,12)} = 2$.
  - $O(8) = {}^{12}/_{\text{mcd}(8,12)} = 3$.
  - $O(9) = {}^{12}/_{\text{mcd}(9,12)} = 4$.
  - $O(10) = {}^{12}/_{\text{mcd}(12,10)} = 6$.

- En $\mathbb{Z}_6 \oplus \mathbb{Z}_2$:

  $$O(a,b) \in \text{mcm}(Div(6), Div(2)) = \text{mcm}(\{1,2,3,6\},\{1,2\}) = \{1,2,3,6\} \qquad \forall (a,b) \in \mathbb{Z}_6 \oplus \mathbb{Z}_2$$

  El orden de los elementos de $\mathbb{Z}_6$ son:

  - $O(0) = 1$.
  - 1 y 5 tienen orden 6.
  - $O(2) = {}^{6}/_{\text{mcd}(2,6)} = 3$.
  - $O(3) = {}^{6}/_{\text{mcd}(3,6)} = 2$.
  - $O(4) = {}^{6}/_{\text{mcd}(4,6)} = 3$.

  Ahora:

  - $O(0,0) = 1$.
  - $O(0,1) = 2$, ya que $(0,1)^2 = (0,0)$.
  - $O(1,b) = O(5,b) = 6 \ \forall b \in \mathbb{Z}_2$.
  - $O(3,b) = 2 \ \forall b \in \mathbb{Z}_2$.
  - $O(2,0) = O(4,0) = 3$.
  - $O(2,1) = O(4,1) = 6$.

6.2. Clasificación de grupos abelianos no finitos

Buscamos ahora tratar de clasificar los grupos abelianos no finitos. Para ello, recordaremos lo que es un grupo finitamente generado, e introduciremos nuevos conceptos.

Definición 6.3. Un grupo abeliano A se dice que es finitamente generado si existe un conjunto:

$$X = \{x_1, \dots, x_r\} \subseteq A$$

De forma que para todo $a \in A$, existen $\lambda_1, \dots, \lambda_r \in \mathbb{Z}$ de forma que:

$$a = \sum_{k=1}^{r} \lambda_k x_k$$

En dicho caso, diremos que X es un sistema de generadores de A, y notaremos:

$$A = \langle x_1, \dots, x_r \rangle$$

Definición 6.4 (Base)**.** Sea A un grupo abeliano, un conjunto de generadores $X = \{x_1, \dots, x_r\}$ de A es una base si los elementos de X son $\mathbb{Z}-$linealmente independientes. Es decir, que si $\lambda_1, \dots, \lambda_r \in \mathbb{Z}$ con:

$$\sum_{k=1}^{r} \lambda_k x_k = 0$$

Entonces, ha de ser $\lambda_k = 0$ para todo $k \in \{1, \dots, r\}$. En dicho caso, diremos que A es un grupo abeliano libre de rango r.

Proposición 6.4. *Si A es un grupo abeliano libre de rango r, entonces:*

$$A \cong \mathbb{Z}^r$$

Demostración. Como A es un grupo abeliano libre de rango r, para dar un homomorfismo de A en cualquier otro grupo basta dar las imágenes de los elementos de la base de A.

De esta forma, si $X = \{x_1, \dots, x_r\}$ es una base de A, definimos el homomorfismo $\phi : A \to \mathbb{Z}^r$ de la forma más canónica posible sobre los elementos de la base de A:

$$\begin{gathered}
\phi(x_1) = (1, 0, \dots, 0) \\
\phi(x_2) = (0, 1, \dots, 0) \\
\vdots \\
\phi(x_r) = (0, 0, \dots, 1)
\end{gathered}$$

Dado $a \in A$, como X es una base de A, existirán $\lambda_1, \dots, \lambda_r \in \mathbb{Z}$ de forma que:

$$a = \sum_{k=1}^{r} \lambda_k x_k$$

Por lo que:

$$\phi(a) = \phi\left(\sum_{k=1}^{r} \lambda_k x_k\right) = \sum_{k=1}^{r} \phi(\lambda_k x_k) = \sum_{k=1}^{r} \lambda_k \phi(x_k)$$

Es fácil ver que ϕ es biyectiva, por lo que ϕ nos da un isomorfismo entre A y $\mathbb{Z}^r$. □

6.2.1. Proceso de clasificación

Una vez entendidas las definiciones básicas necesarias para comenzar el estudio de los grupos abelianos no finitos procederemos ahora a explicar el procedimiento por el cual somos capaces de clasificar cualquier grupo abeliano no finito. Esto es, dar un isomorfismo estándar para cualquier grupo abeliano no finito dado.

Este procedimiento requiere de una gran cantidad de resultados que tienen que ver con cómo son los subrupos y los cocientes de grupos como $\mathbb{Z}^r$ para $r \in \mathbb{N}$, que ya hemos visto que es el único grupo libre de rango r, salvo isomorfismo. Como esta intención escapa al interés de la asignatura y como seremos capaces de clasificar los grupos abelianos no finitos mediante un procedimiento algorítmico, mostraremos ahora los resultados que nos permiten realizarlo, la mayoría de ellos sin demostración.

Animamos al lector a profundizar más en estos teoremas de clasificación, que seguro se encuentran en algún libro de la bibliografía de la asignatura.

El primer problema con el que nos encontramos es con el de cómo conocer un grupo abeliano no finito, ya que al tener infinitos elementos no nos es posible listar todos sus elementos para conocerlo bien. Como puede adivinarse, lo que haremos será trabajar con grupos abeliano finitamente generados, y las relaciones entre los elementos del grupo las deduciremos a partir de las relaciones entre los generadores del grupo. Esto nos conlleva a pensar que la forma en la que describiremos un grupo abeliano no finito será mediante su **presentación**.

Como a lo largo de este capítulo siempre conoceremos un grupo por su presentación, impondremos ahora varias reglas para tratar de estandarizar la forma en la que nos den las presentaciones, con el fin también de hacer los razonamientos abstractos y genéricos con una notación más fácil y cómoda. Estas reglas las crearemos a partir de la clasificación de un ejemplo de grupo abeliano no finito.

Ejemplo. Se pide clasificar el grupo:

$$G = \langle x, y, z \mid x^3 = y^4, x^2 z = z^{-1} y, xy = yx, xz = zx, yz = zy \rangle$$

Este grupo nos viene dado con la notación multiplicativa, algo habitual en grupos y que venimos haciendo durante toda la asignatura, pero podemos tratar de escribir el grupo con notación aditiva, algo que nos será más cómodo en estos casos:

$$G = \langle x, y, z \mid 3x = 4y, 2x + z = -z + y, x + y = y + x, x + z = z + x, y + z = z + y \rangle$$

Además, como nuestro objetivo es trabajar con grupos abelianos esta notación estará más que justificada, aprovechando la intuición de que es mucho más natural que una suma sea abeliana antes que un producto lo sea (podemos pensar en las matrices, por ejemplo). De esta forma, convenimos en eliminar de la presentación del grupo todas las relaciones que nos indiquen la conmutatividad entre los generadores del grupo, por simplicidad:

$$G = \langle x, y, z \mid 3x = 4y, 2x + z = -z + y \rangle$$

Finalmente, convenimos estandarizar la forma en la que damos las ecuaciones, tratando de expresar estas siempre como una combinación lineal de los generadores igualadas a ceros:

$$G = \langle x, y, z \mid 3x - 4y = 0, 2x + 2z - y = 0 \rangle$$

Con las tres reglas de notación introducidas en el ejemplo superior, cualquier grupo abeliano finitamente generado vendrá dado a nosotros como una presentación del estilo:

$$G = \left\langle x_1, x_2, \dots, x_n \mid \begin{array}{c} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0 \end{array} \right\rangle$$

Notemos que, de esta forma, dar un grupo es equivalente a dar una matriz. Es decir, dada una matriz $m \times n$, podemos pensar que hay un grupo asociado a dicha matriz que tendrá n elementos que generen el grupo y que dichos elementos cumplan m relaciones entre sí. Así, la presentación superior nos da la matriz:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Esta matriz recibirá el nombre de <u>matriz de relaciones</u> del grupo.

Una vez introducida la matriz de relaciones de un grupo a partir de su presentación, si volvemos a la presentación del grupo, podemos observar que dar una presentación de un grupo G generado por los elementos $\{x_1, x_2, \dots, x_n\}$ es equivalente a dar un epimorfismo $\phi : \mathbb{Z}^n \to G$ de forma que la base canónica[1] de $\mathbb{Z}^n$ $\{e_1, e_2, \dots, e_n\}$ tenga como imágenes:

$$\phi(e_k) = x_k \qquad \forall k \in \{1, \dots, n\}$$

Y que además el conjunto:

$$\left\{ \begin{array}{c} a_{11}e_1 + a_{12}e_2 + \cdots + a_{1n}e_n, \\ a_{21}e_1 + a_{22}e_2 + \cdots + a_{2n}e_n, \\ \vdots \\ a_{m1}e_1 + a_{m2}e_2 + \cdots + a_{mn}e_n \end{array} \right\}$$

Sea un sistema de generadores de $\ker(\phi)$. Aplicando el Primer Teorema de Isomorfía sobre ϕ obtenemos que:

$$\mathbb{Z}^n / \ker(\phi) \cong G$$

Por lo que parece que vamos por buen camino si queremos clasificar todos los grupos no abelianos finitamente generados, nos falta estudiar cómo son los grupos cocientes de $\mathbb{Z}^n$. Como dijimos anteriormente, no vamos a hacerlo, por lo que mostraremos ahora una serie de resultados sin demostración que nos ayudarán a seguir en nuestra tarea.

Observemos ahora que podemos hacer los siguientes cambios en una base de un grupo libre y que tras ellos seguiremos teniendo una base del mismo:

[1]Podemos trasladar el concepto de "base canónica de $\mathbb{R}^n$" que teníamos en Álgebra Lineal a este ámbito de clasificación de grupos.

1. Sustituir un elemento de una base por su opuesto.
2. Reordenar los elementos de la base.
3. Sumarle a un elemento de la base otro elemento de la base distinto a él.

Estos cambios en la base de un grupo libre dan lugar a las siguientes transformaciones elementales sobre las columnas de una matriz e relaciones:

1. Cambiar una columna por su opuesta.
2. Reordenar las columnas de la matriz.
3. Sumar a todos los elementos de la columna $i-$ésima un múltiplo de los elementos de la columna $j-$ésima, con $j \neq i$.

Como las columnas de una matriz no tienen nada de especial, de forma análoga pueden justificarse estas operaciones sobre las filas de una matriz, sustituyendo la palabra "columna" por "fila". Estas transformaciones dan lugar al siguiente resultado:

Proposición 6.5. *Si M es la matriz de relaciones de una presentación de un grupo abeliano G, es decir:*

$$G = \langle x_1, \ldots, x_n \mid MX = 0 \rangle$$

Donde:

$$X = \left(\begin{array}{c} x_1 \\ \vdots \\ x_n \end{array} \right)$$

Y M' es una matriz obtenida mediante transformaciones elementales del tipo 1, 2 o 3 sobre filas o columnas de M, entonces M' también es una matriz de relaciones de una presentación de G.

Teorema 6.6. *Dada $M \in \mathcal{M}_{m,n}(\mathbb{Z})$, podemos realizar transformaciones elementales en M del tipo 1, 2 o 3 en las filas y/o columnas de M hasta llegar a una matriz diagonal de la forma[2]:*

$$M' = \left(\begin{array}{cccc} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_r \\ 0 & 0 & \cdots & 0 \end{array} \right)$$

Donde $d_i \mid d_{i+1}$ para $i \in \{1, \ldots, r-1\}$ y r es el rango de M. Además, si M' es la matriz de relaciones de un grupo G generado por n generadores, entonces:

$$G \cong \mathbb{Z}^{n-r} \oplus \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r}$$

[2]Puede que la matriz no tenga filas de ceros y que en su lugar tenga columnas de ceros, o que no tenga ni filas ni columnas de ceros, todo dependerá del orden y del rango de la matriz.

Definición 6.5. Si G es un grupo abeliano finitamente generado, este tendrá su matriz de relaciones $M \in \mathcal{M}_{m,n}(\mathbb{Z})$, sobre la que podemos aplicar las transformaciones pertinentes para conseguir la matriz M' del Teorema anterior, obteniendo que:

$$G \cong \mathbb{Z}^{n-r} \oplus \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r}$$

Para ciertos enteros $n, r, d_1, d_2, \ldots, d_r \in \mathbb{Z}$, con $d_i \mid d_{i+1}$ $\forall i \in \{1, \ldots, r-1\}$

- La matriz M' obtenida a partir de M recibirá el nombre de forma normal de Smith de M.
- A los elementos d_i obtenidos en M' los llamaremos factores invariantes de M.
- Diremos que G tiene rango $n - r$.
- Diremos que $\mathbb{Z}^{n-r}$ es la parte libre de G.
- Diremos que $\mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r}$ es la parte de torsión de G, o grupo de torsión de G, denotado por $T(G)$.

6.2.2. Ejemplos

Una vez explicado el procedimiento teórico, mostraremos varios ejemplos de cómo conseguir la forma normal de Smith de una matriz dada, así como ejemplos sobre cómo podemos clasificar los grupos abelianos no finitos finitamente generados.

Ejemplo. Se pide calcular la forma normal de Smith de:

$$\begin{pmatrix} 0 & 2 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 7 & 10 & 6 \end{pmatrix}$$

Aplicaremos a continuación un algoritmo similar al que usábamos en Geometría I para calcular la forma normal de Hermite de una matriz, por lo que los pasos mediante los que "intentamos tener un número en una cierta posición de una matriz" no los explicaremos, confiando en que el lector es suficientemente habilidoso como para conseguirlo por él mismo. Sin embargo, explicaremos algunos pasos clave en el algoritmo a aplicar que sí debemos tener en cuenta.

En primer lugar, calcularemos el máximo común divisor de los elementos que aparecen en las entradas de la matriz, en este caso, tenemos que es 1, por lo que buscamos escribir un 1 en la posición[3] $(1, 1)$ de la matriz. Como consejo, diremos que es recomendable no hacer ceros en los elementos hasta no tener algún 1 disponible. Una forma de conseguir un 1 en la posición $(1, 1)$ es (usaremos una notación informal para describir las operaciones, $F_4 - F_3$ debe entenderse como "a la fila 4 le restamos la 3"):

$$\begin{pmatrix} 0 & 2 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 7 & 10 & 6 \end{pmatrix} \xrightarrow{F_4 - F_3} \begin{pmatrix} 0 & 2 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 1 & 4 & 0 \end{pmatrix} \xrightarrow{F_1 \leftrightarrow F_4} \begin{pmatrix} 1 & 4 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix}$$

[3] La esquina superior izquierda.

Una vez tenemos el 1 en la posición deseada, tratamos de rellenar la primera fila y la primera columna entera con ceros (salvo el 1 que acabamos de colocar), algo que ya sabíamos hacer de otras asignaturas:

$$\begin{pmatrix} 1 & 4 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix} \xrightarrow[C_1-C_3]{F_1-2F_4} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & -6 \\ 0 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix}$$

Ahora el máximo común divisor de todos los elementos es 2, por lo que tratamos de poner un 2 en la siguiente posición de la diagonal de la matriz, tras el 1 de antes:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & -6 \\ 0 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix} \xrightarrow{F_2 \leftrightarrow F_4} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 6 & 6 \\ 0 & -4 & -6 \end{pmatrix}$$

Ahora, hacemos ceros debajo de este 2:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 6 & 6 \\ 0 & -4 & -6 \end{pmatrix} \xrightarrow[F_4+2F_2]{F_3-3F_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & -6 \end{pmatrix}$$

El máximo común divisor de los elementos que nos quedan es 6, que ya está en la posición deseada, por lo que solo nos queda hacer ceros en la última fila:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & -6 \end{pmatrix} \xrightarrow{F_4+F_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

Tenemos ya la forma normal de Smith de la matriz original.

Ejemplo. Calcular la forma normal de Smith de:

$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix}$$

Como no está en forma normal de Smith porque el primer elemento no se corresponde con el máximo común divisor de todos los demás (que es 2), veamos cómo podemos añadir este 2 a la posición $(1,1)$ de la matriz. Mostraremos solo las operaciones a realizar sobre M, entendiendo que el algoritmo que explicamos en el ejemplo anterior está ya claro

$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{F_2+F_1} \begin{pmatrix} 4 & 0 & 0 \\ 4 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{C_2-C_1} \begin{pmatrix} 4 & -4 & 0 \\ 4 & 2 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{-F_1}$$
$$\begin{pmatrix} -4 & 4 & 0 \\ 4 & 2 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{F_2\leftrightarrow F_1} \begin{pmatrix} 4 & 2 & 0 \\ -4 & 4 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{C_2\leftrightarrow C_1} \begin{pmatrix} 2 & 4 & 0 \\ 4 & -4 & 0 \\ 0 & 0 & 8 \end{pmatrix}$$
$$\xrightarrow{F_2-2F_1} \begin{pmatrix} 2 & 4 & 0 \\ 0 & -12 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{C_2-2C_1} \begin{pmatrix} 2 & 0 & 0 \\ 0 & -12 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{F_2+2F_3} \begin{pmatrix} 2 & 0 & 0 \\ 0 & -12 & 16 \\ 0 & 0 & 8 \end{pmatrix}$$
$$\xrightarrow{C_2+C_3} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 16 \\ 0 & 8 & 8 \end{pmatrix} \xrightarrow{F_3-2F_2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 16 \\ 0 & 0 & -24 \end{pmatrix} \xrightarrow[-C_3]{C_3-4C_2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 24 \end{pmatrix}$$

Ejemplo. Sea A el grupo:

$$A = \left\langle x,y,z,t \mid \begin{array}{r} 14x+4y+4z+14t=0 \\ -6x+4y+4z+10t=0 \\ -16x-4y-4z-20t=0 \end{array} \right\rangle$$

Se pide calcular el rango de A y todos los grupos abelianos del mismo orden que el grupo de torsión de A que no sean isomorfos al grupo de torsión de A.

Sea:

$$M = \begin{pmatrix} 14 & 4 & 4 & 14 \\ -6 & 4 & 4 & 10 \\ -16 & -4 & -4 & -20 \end{pmatrix}$$

Vamos a calcular la forma normal de Smith de M, con el fin de clasificar A para conocer su rango y grupo de torsión ($-(F_1+F_3)$ significa que primero a la fila 1 le sumamos la 3 y que luego consideramos los opuestos de los elementos de la fila 1 como la nueva fila 1).

$$\begin{pmatrix} 14 & 4 & 4 & 14 \\ -6 & 4 & 4 & 10 \\ -16 & -4 & -4 & -20 \end{pmatrix} \xrightarrow{-(F_1+F_3)} \begin{pmatrix} 2 & 0 & 0 & 6 \\ -6 & 4 & 4 & 10 \\ -16 & -4 & -4 & -20 \end{pmatrix} \xrightarrow{C_4-3C_1}$$
$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ -6 & 4 & 4 & 28 \\ -16 & -4 & -4 & 28 \end{pmatrix} \xrightarrow{\substack{F_2+3F_1 \\ F_3+8F_1}} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 4 & 28 \\ 0 & -4 & -4 & 28 \end{pmatrix} \xrightarrow{F_2+F_3}$$
$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 56 \\ 0 & -4 & -4 & 28 \end{pmatrix} \xrightarrow{F_2\leftrightarrow F_3} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -4 & -4 & 28 \\ 0 & 0 & 0 & 56 \end{pmatrix} \xrightarrow{F_2'=-F_2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 4 & -28 \\ 0 & 0 & 0 & 56 \end{pmatrix} \xrightarrow{C_3+7C_2}$$
$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 4 & 0 \\ 0 & 0 & 0 & 56 \end{pmatrix} \xrightarrow{C_3-C_2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 56 \end{pmatrix} \xrightarrow{C_3\leftrightarrow C_4} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 56 & 0 \end{pmatrix}$$

De esta forma, tendremos que:

$$A \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{56}$$

Por lo que el rango de A es 1 y su grupo de torsión es:

$$T(A) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{56}$$

Un grupo de orden $2 \cdot 4 \cdot 56 = 448 = 2^6 \cdot 7$. Esta de arriba es su descomposición cíclica, de la que podemos sacar fácilmente su descomposición cíclica primaria:

$$T(A) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_7$$

Que como vemos, corresponde a la partición $\{2, 2^2, 2^3, 7\}$. Para calcular todos los grupos abelianos de orden 448 no isomorfos a $T(A)$, calculamos las distintas particiones de 6 (el exponente del 2):

$$\begin{gathered} 6 \\ 5,1 \\ 4,1,1 \\ 4,2 \\ 3,1,1,1 \\ 3,2,1 \\ 3,3 \\ 2,1,1,1,1 \\ 2,2,1,1 \\ 2,2,2 \\ 1,1,1,1,1,1 \end{gathered}$$

Calculamos para cada una de ellas el grupo correspondiente en descomposición cíclica primaria (no nos especifican una o la otra, luego elegimos la que queramos):

Divisores elementales	Descomposición cíclica primaria
$2^6, 7$	$C_{64} \oplus C_7$
$2^5, 2, 7$	$C_{32} \oplus C_2 \oplus C_7$
$2^4, 2, 2, 7$	$C_{16} \oplus C_2 \oplus C_2 \oplus C_7$
$2^4, 2^2, 7$	$C_{16} \oplus C_4 \oplus C_7$
$2^3, 2, 2, 2, 7$	$C_8 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_7$
$2^3, 2^2, 2, 7$	$C_8 \oplus C_4 \oplus C_2 \oplus C_7$
$2^3, 2^3, 7$	$C_8 \oplus C_8 \oplus C_7$
$2^2, 2, 2, 2, 2, 7$	$C_4 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_7$
$2^2, 2^2, 2, 2, 7$	$C_4 \oplus C_4 \oplus C_2 \oplus C_2 \oplus C_7$
$2^2, 2^2, 2^2, 7$	$C_4 \oplus C_4 \oplus C_4 \oplus C_7$
$2, 2, 2, 2, 2, 2, 7$	$C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_7$

Si quitamos el grupo correspondiente a $\{2^3, 2^2, 2, 7\}$, tenemos todos los grupos no isomorfos a $T(A)$ de orden $|T(A)|$.

Podemos hacernos más preguntas que sabemos responder sobre A, como:

- ¿Hay algún elemento de orden infinito en A?

  Sí, $(1, 0, 0, 0)$.

- ¿Hay algún elemento de orden 56?
  Sí, $(0, 0, 0, 1)$.
- ¿Hay algún elemento de orden 8?
  Sí, $(0, 0, 0, 7)$, o también $(0, 1, 1, 7)$.

7. Clasificación de grupos de orden bajo

Clasificar grupos es una tarea dura y difícil, por lo que nos centraremos en aprender a clasificar grupos de orden bajo. En concreto, nuestro objetivo será saber clasificar todos los grupos de orden menor o igual que 15.

Grupos abelianos

En el Capítulo anterior aprendimos ya a clasificar todos los grupos abelianos finitos. En particular, sabemos ya clasificar todos los grupos abelianos finitos de orden menor o igual que 15:

Orden	Grupos		
1	$\{1\}$		
2	C_2		
3	C_3		
4	C_4,	$C_2 \oplus C_2$	
5	C_5		
6	C_6		
7	C_7		
8	C_8,	$C_2 \oplus C_4$,	$C_2 \oplus C_2 \oplus C_2$
9	C_9,	$C_3 \oplus C_3$	
10	C_{10}		
11	C_{11}		
12	C_{12},	$C_2 \oplus C_6$	
13	C_{13}		
14	C_{14}		
15	C_{15}		
$\vdots$	$\vdots$		

Por tanto, nos centraremos ahora en tratar de describir todos los grupos finitos no abelianos de orden menor o igual que 15.

7.1. Producto semidirecto

Con el fin de conseguir nuestro objetivo, definiremos el producto semidirecto, herramienta que nos permitirá escribir muchos grupos no abelianos (aunque no todos).

Ejemplo. En el Capítulo 1 vimos que $Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$ es isomorfo a:

$$Q_2^{\text{abs}} = \langle x, y \mid x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle$$

Es decir, teníamos una aplicación (gracias a Teorema de Dyck) $f : Q_2 \to Q_2^{\text{abs}}$ dada por:

$$f(x) = i \qquad f(y) = j$$

Que además era un epimorfismo, porque $Q_2^{\text{abs}} = \langle i, j\rangle$. Veamos que $|Q_2^{\text{abs}}| = 8$, de una forma distinta que contar elementos:

Demostración. Como $x^4 = 1$, si consideramos $H = \langle x\rangle$, tendremos que $|H| \leqslant 4$. Ahora, como:

$$yxy^{-1} = x^{-1} \in H$$

Tenemos que $H \lhd Q_2^{\text{abs}}$. Si escribimos Q_2^{abs} en su partición de clases (como $Q_2^{\text{abs}} = \langle x, y\rangle$, si un elemento no está en H es porque es producto de y por algo más):

$$Q_2^{\text{abs}} \cong H \cup yH$$

Ya que $y \notin H$, de donde al tomar cocientes:

$$Q_2^{\text{abs}}/H = \langle yH\rangle$$

Ahora, como:

$$(yH)^2 = y^2H = x^2H = H$$

Entonces $O(yH) = 2$, por lo que:

$$|Q_2^{\text{abs}}/H| = 2$$

Si aplicamos el Primer Teorema de Isomorfía sobre f:

$$Q_2^{\text{abs}}/\ker(f) \cong Im(f) = Q_2$$

De donde $|Q_2^{\text{abs}}| = |Q_2||\ker(f)| \geqslant 8$. Concluimos que $|Q_2^{\text{abs}}| = 8$. □

El hecho de introducir Q_2^{abs} en el Capítulo 1 fue para ahora generalizar lo que hacíamos con Q_2 a todo grupo, con el producto semidirecto.

Definición 7.1 (Grupos dicíclicos)**.** Para cada $k \in \mathbb{N} \setminus \{0\}$, definimos el $k-$ésimo grupo dicíclico como el grupo:

$$Q_k = \left\langle x, y \mid x^{2k} = 1, y^2 = x^k, yxy^{-1} = x^{-1}\right\rangle$$

Ejemplo. Estudiemos los grupos dicíclicos:

- Para $k = 1$:

  $$Q_1 = \langle x, y \mid x^2 = 1, y^2 = x, yxy^{-1} = x\rangle$$

  Nos preguntamos qué grupo es. Si tratamos de describir los elementos, obtenemos:

  $$\{1, x, y, xy\} = \{1, y, y^2, y^3\}$$

  Es decir, $Q_1 \cong C_4$.

- Observemos que si[1] $k = 2$, obtenemos Q_2^{abs}:

$$Q_2 = \langle x, y \mid x^4 = 1, y^2 = x^2, yx = x^{-1}y\rangle = Q_2^{\text{abs}}$$

- Para $k \geqslant 3$, veamos que:

$$2k \leqslant |Q_k| \leqslant 4k \qquad \forall k \geqslant 3$$

Y si k es impar, entonces $|Q_k| = 4k$.

Demostración. Si recordamos al grupo diédrico de orden k:

$$D_k = \langle r, s \mid r^k = s^2 = 1, sr = r^{-1}s\rangle$$

Recordamos que:

$$Q_k = \langle x, y \mid x^{2k} = 1, y^2 = x^k, yx = x^{-1}y\rangle$$

Y observamos que:

- $r^{2k} = (r^k)^2 = 1$.
- $s^2 = 1 = r^k$.
- $sr = r^{-1}s$.

El Teorema de Dyck nos da un homomorfismo $f : Q_k \to D_k$ de forma que:

$$f(x) = r \qquad f(y) = s$$

Como además $D_k = \langle r, s\rangle$, tenemos que f es un epimorfismo. Si aplicamos el Primer Teorema de Isomorfía sobre f, obtenemos que:

$$Q_k/\ker(f) \cong D_k$$

En primer lugar, observamos que Q_k no es abeliano, ya que D_k no lo es y cualquier cociente de un grupo abeliano es abeliano. Veamos que:

$$2k \leqslant |Q_k| \leqslant 4k$$

- Para la desigualdad de la izquierda, sabemos que $|D_k| = 2k$, y por ser $[Q_k : \ker(f)] = |D_k|$, sabemos que $2k$ divide a $|Q_k|$, de donde $|Q_k| \geqslant 2k$.
- Para la otra, si tomamos $H = \langle x\rangle$, como $x^{2k} = 1$, tendremos que $|H| \leqslant 2k$. Como además también tenemos que:

$$\begin{aligned} yxy^{-1} &= x^{-1} \in H \\ y^{-1}xy &= x^{-1} \in H \end{aligned}$$

Tendremos que $H \lhd Q_k$, de donde al considerar el cociente, tendremos que:

$$Q_k/H = \langle yH\rangle$$

[1]Aquí cometemos un pequeño abuso de notación, ya que Q_2 no es el grupo de los cuaternios, sino el segundo grupo dicíclico.

De esta forma, como:

$$(yH)^2 = y^2H = x^kH = H$$

Deducimos que $O(yH) \leqslant 2$, por lo que:

$$|Q_k/H| \leqslant 2$$

De donde tenemos que:

$$|Q_k| = |Q_k/H||H| \leqslant 2k + 2k = 4k$$

Si suponemos ahora que $k = 2t+1$ para cierto $t \in \mathbb{N}$, si consideramos el cíclico de orden 4:

$$C_4 = \langle a \mid a^4 = 1\rangle$$

Como:

- $(a^2)^{2k} = (a^4)^k = 1$.
- $a^2 = a^{4t+2} = a^{2k} = (a^2)^k$.
- $aa^2 = a^3 = a^2a = (a^2)^{-1}a$.

Podemos aplicar el Teorema de Dyck, obteniendo un homomorfismo $f : Q_k \to C_4$ de forma que:

$$f(x) = a^2 \qquad f(y) = a$$

Que de hecho es un epimorfismo, ya que $C_4 = \langle a\rangle$. Al igual que antes, tendremos que:

$$Q_k/\ker(f) \cong C_4$$

De donde 4 divide a $|Q_k|$. Como también teníamos antes que $2k$ dividía a $|Q_k|$, tenemos que $\operatorname{mcm}(2k, 4)$ divide a $|Q_k|$ y como k era impar, tenemos que:

$$\operatorname{mcm}(2k, 4) = 4k$$

De donde $4k$ divide a $|Q_k|$, por lo que $4k \leqslant |Q_k|$, y la otra desigualdad que teníamos ya probada nos da la igualdad. $\square$

Ejemplo. Grupos no abelianos de orden 12 conocíamos:

- A_4.
- D_6.

Y ahora conocemos Q_3. Próximamente veremos que estos grupos son los únicos grupos que existen de orden 12, salvo isomorfismo.

Antes de proceder con la definición del producto semidirecto, daremos una útil Proposición que nos será de ayuda a la hora de construir productos semidirectos:

Proposición 7.1. *Sea $n \in \mathbb{N}$, entonces:*

$$Aut(C_n) \cong U(\mathbb{Z}_n)$$

En particular, $Aut(C_n)$ es un grupo abeliano de orden[2] *$\varphi(n)$, donde φ es la función de Euler:*

$$\varphi(n) = |\{m \in \mathbb{N} \mid 1 \leqslant m \leqslant n \land \text{mcd}(n, m) = 1\}| \qquad \forall n \in \mathbb{N}$$

Demostración. Se hizo en el Ejercicio 2.3.17 de la relación de ejercicios. □

Observación. Si p es un número primo, entones:

$$Aut(C_p) \cong C_{p-1}$$

Ya que $Aut(C_p) \cong U(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$.

Definición 7.2 (Producto semidirecto)**.** Sean K, H dos grupos y dado un homomorfismo $\theta : H \to Aut(K)$, sobre el producto cartesiano de K por H podemos definir la operación:

$$(k_1, h_1)(k_2, h_2) = (k_1\theta(h_1)(k_2), h_1h_2) \qquad \forall (k_1, h_1), (k_2, h_2) \in K \times H$$

Se verifia que $K \times H$ con esta operación tiene estructura de grupo (como ponemos de manifiesto en la siguiente Proposición), al que llamaremos **producto semidirecto de K por H relativo a θ**, y que denotaremos por:

$$K \rtimes_\theta H$$

Observemos que, en particular, θ es un homomorfismo de H sobre Perm(K), por lo que θ nos define una acción:

$$\theta(h)(k) = {}^hk \qquad \forall h \in H, k \in K$$

Por lo que será habitual escribir:

$$(k_1, h_1)(k_2, h_2) = (k_1\, {}^{h_1}k_2, h_1h_2)$$

Y no se nos debe olvidar que $\theta(h) \in Aut(K)$ para todo $h \in H$, ya que esta propeidad es importante a la hora de ver que $K \rtimes_\theta H$ es un grupo.

Proposición 7.2. *Se verifica que $K \times H$ con la operación definida en la definición anterior es un grupo.*

Demostración. Veamos que efectivamente cumple con todas las condiciones de ser un grupo:

- Para la propiedad asociativa, si $a, b, c \in K$ y $x, y, z \in H$:

$$\begin{aligned}((a, x)(b, y))(c, z) &= (a\,{}^xb, xy)(c, z) = (a\,{}^xb\,{}^{xy}c, xyz)\\ (a, x)((b, y)(c, z)) &= (a, x)(b\,{}^yc, yz) = (a\,{}^x(b\,{}^yc), xyz) = (a\,{}^xb\,{}^{xy}c, xyz)\end{aligned}$$

[2]En Álgebra I se demostró que $|U(\mathbb{Z}_n)| = \varphi(n)$.

- El elemento $(1,1)$ es el neutro:

$$(k,h)(1,1) = (k\,{}^h1, h) = (k,h)$$
$$(1,1)(k,h) = (1\,{}^1k, h) = (k,h)$$
$$\forall (k,h) \in K \times H$$

- Para el inverso, dado $(k,h) \in K \times H$, el inverso será:

$$(k,h)^{-1} = \left({}^{h^{-1}}k^{-1}, h^{-1}\right)$$

Ya que:

$$(k,h)\left({}^{h^{-1}}k^{-1}, h^{-1}\right) = \left(k\,{}^{h}\left({}^{h^{-1}}k^{-1}\right), hh^{-1}\right) = \left(k\,{}^{hh^{-1}}k^{-1}, 1\right) = (kk^{-1}, 1) = (1,1)$$

$\square$

Ejemplo. Veamos:

- Si $\theta(k) = id_H$ para todo $k \in K$, entonces $K \rtimes_\theta H = K \times H$, ya que:

$$(k_1,h_1)(k_2,h_2) = (k_1\,{}^{h_1}k_2, h_1h_2) = (k_1k_2, h_1h_1) \qquad \forall (k_1,h_1),(k_2,h_2) \in K \times H$$

- Como ejemplo útil del producto semidirecto, veamos si somos capaces de escribir S_3 como producto semidirecto de C_3 por C_2 relativo a algún homomorfismo θ:

$$S_3 \cong C_3 \rtimes_\theta C_2$$

- Veamos cómo escribir S_3 como producto semidirecto:

$$S_3 \cong C_3 \rtimes_\theta C_2$$

Tenemos los elementos:

$$C_3 \times C_2 = \{(x,y) \mid x \in C_3, y \in C_2\}$$

Buscamos qué homomorfismo $\theta : C_2 \to Aut(C_3)$ hemos de coger. Como θ ha de ser un homomorfismo, sabemos que $\theta(0) = id_{C_3}$, por lo que solo hemos de determinar la imagen de $1 \in C_2$. Además, como $Aut(C_3) \cong C_2$, solo hay dos isomorfismos de C_3 en C_3:

$$\begin{array}{cc} id_{C_3} & x^{-1} \\ 0 \longmapsto 0 & 0 \longmapsto 0 \\ 1 \longmapsto 1 & 1 \longmapsto 2 \\ 2 \longmapsto 2 & 2 \longmapsto 1 \end{array}$$

Si cogemos $\theta(1) = id_{C_3}$, en el ejemplo superior vimos que entonces tendremos que $C_3 \rtimes_\theta C_2 = C_3 \times C_2$, y sabemos que $C_3 \times C_2 \cong C_6$. Sin embargo, S_3 no es cíclico, luego no vamos a tener que $S_3 \cong C_3 \rtimes_\theta C_2$. Nos decantamos por tanto a coger $\theta(1)(x) = x^{-1}\ \forall x \in C_3$.

De esta forma, tendremos que $|C_3 \rtimes_\theta C_2| = 6$ y como podemos clasificar todos los grupos de orden 6 en S_3 (no abeliano) y en C_6 (abeliano), si vemos que $C_3 \rtimes_\theta C_2$ no es abeliano, tendremos que $C_3 \rtimes_\theta C_2 \cong S_3$, que es lo que queríamos probar. Para ello (usamos notación aditiva por representar C_3 y C_2 con notación aditiva):

$$\begin{aligned}(1,0)+(0,1) &= (1+\theta(0)(0), 0+1) = (1,1)\\ (0,1)+(1,0) &= (0+\theta(1)(1), 1+0) = (2,1)\end{aligned}$$

Como $(1,1) \neq (2,1)$, tenemos que $C_3 \rtimes_\theta C_2$ no es abeliano, por lo que ha de ser $C_3 \rtimes_\theta C_2 \cong S_3$.

- Veamos que $Q_3 = C_3 \rtimes_\theta C_4$. De nuevo, el homomorfismo a considerar será:

  $$\begin{array}{rccc}\theta: & C_4 & \longrightarrow & Aut(C_3)\\ & y & \longmapsto & \theta(y)(x) = x^{-1}\end{array}$$

  Tendremos:

  $$C_3 \rtimes_\theta C_4 = \langle x, y \mid x^3 = 1, y^4 = 1, {}^y x = x^{-1}\rangle$$

  Y queremos ver el isomorfismo con:

  $$Q_3 = \langle c, d \mid c^6 = 1, d^2 = c^3, dc = c^{-1}d\rangle$$

  Si cogemos:

  $$c = (x^2, y) \qquad d = (1, y)$$

  Vemos que:

  - $c^6 = 1$.
  - $d^2 = c^3$.
  - $dc = c^{-1}d$, que equivale a ver que $cdc = d$. Para ello:

  $$(x^2,y)(1,y)(x^2,y) = (x^2,y)\left(1\,{}^y x^2, y^2\right) = (x^2,y)(x,y^2) = (x^2\,{}^y x, y^3) = (x,y^3)$$

  $$(x^2,1)(1,y)(x^2,1) = (x^2,y)(x^2,1) = (x^2\,{}^y x^2, y) = (x^3,y) = (1,y)$$

- Si $n \geqslant 3$, si consideramos $\theta : C_2 \to Aut(C_n)$ dado por:

  $$\theta(y)(x) = x^{-1} \qquad \forall x \in C_2, y \in C_n$$

  Tendremos que $C_n \rtimes_\theta C_2 \cong D_n$.

7.1.1. Propiedades

Definición 7.3. Dado un homomorfismo $\theta : H \to Aut(K)$ que nos da un producto semidirecto $K \rtimes_\theta H$, sobre este producto definimos:

- La inyección en primera coordenada, $\lambda_1 : K \to K \rtimes_\theta H$ dada por:

$$\lambda_1(k) = (k, 1) \qquad \forall k \in K$$

- La inyección en segunda coordenada, $\lambda_2 : H \to K \rtimes_\theta H$ dada por:

$$\lambda_2(h) = (1, h) \qquad \forall h \in H$$

- La proyección $\pi : K \rtimes_\theta H \to H$ dada por:

$$\pi(k, h) = h \qquad \forall (k, h) \in K \rtimes_\theta H$$

$$\begin{tikzcd}
K \arrow[r, "\lambda_1"] & K \rtimes_\theta H \arrow[d, "\pi"] & H \arrow[l, "\lambda_2"'] \\
& H &
\end{tikzcd}$$

Proposición 7.3. *Si $K \rtimes_\theta H$ es un producto semidirecto, se verifica que:*

1. *$\lambda_1, \lambda_2, \pi$ son homomorfismos de grupos.*
2. *$\pi\lambda_1$ es trivial.*
3. *$\pi\lambda_2 = id_H$.*
4. *$(k, h) = (k, 1)(1, h)\ \forall (k, h) \in K \rtimes_\theta H$.*

Demostración. Veamos cada propiedad:

1. Vemos que:

$$\lambda_1(k_1)\lambda_1(k_2) = (k_1, 1)(k_2, 1) = (k_1\,{}^{1}k_2, 1) = (k_1k_2, 1) = \lambda_1(k_1k_2) \qquad \forall k_1, k_2 \in K$$
$$\lambda_2(h_1)\lambda_2(h_2) = (1, h_1)(1, h_2) = (1\,{}^{1}1, h_1h_2) = (1, h_1h_2) = \lambda_2(h_1h_2) \qquad \forall h_1, h_2 \in H$$

   Y para la proyección:

$$\pi(k_1, h_1)\pi(k_2, h_2) = h_1h_2 = \pi(k_1\,{}^{h_1}k_2, h_1h_2) = \pi((k_1, h_1)(k_2, h_2))$$
$$\forall (k_1, h_1), (k_2, h_2) \in K \rtimes_\theta H$$

2. $(\pi\lambda_1)(k) = \pi(k, 1) = 1\ \forall k \in K$.
3. $(\pi\lambda_2)(h) = \pi(k, h) = h\ \forall h \in H$.
4. $(k, 1)(1, h) = (k\,{}^{1}1, h) = (k, h)\ \forall (k, h) \in K \rtimes_\theta H$.

□

De forma análoga a la propiedad universal del producto directo, podemos tener la propiedad universal para el producto semidirecto.

Teorema 7.4 (Propiedad Universal del Producto Semidirecto)**.** *Sean K, H dos grupos y $\theta : H \to Aut(K)$ un homomorfismo, consideramos $G = K \rtimes_\theta H$. Sea T un grupo, para cada par de homomorfismos $f : K \to T$ y $g : H \to T$ que verifiquen:*

$$f(\theta(h)(k)) = g(h)f(k)(g(h))^{-1} \qquad \forall k \in K, \forall h \in H$$

Entonces, existe un único homomorfismo $\varphi : G \to T$ de forma que:

$$\varphi(k, 1) = f(k) \qquad \varphi(1, h) = g(h) \qquad \forall k \in K, \forall h \in H$$

Y por tanto, $\varphi(k, h) = f(k)g(h)$ $\forall (k, h) \in G$.

$$\begin{tikzcd}
K \arrow[dr, "f"'] & K \rtimes_\theta H \arrow[d, dashed, "\varphi"] & H \arrow[dl, "g"] \\
& T &
\end{tikzcd}$$

Demostración. Definiendo $\varphi : G \to T$ por:

$$\varphi(k, h) = f(k)g(h) \qquad \forall (k, h) \in G$$

Veamos que φ es un homomorfismo:

$$\begin{aligned}
\varphi((k_1, h_1)(k_2, h_2)) &= \varphi(k_1\theta(h_1)(k_2), h_1h_2) = f(k_1\theta(h_1)(k_2))g(h_1h_2) \\
&= f(k_1)f(\theta(h_1)(k_2))g(h_1)g(h_2) = f(k_1)g(h_1)f(k_2)g(h_1)^{-1}g(h_1)g(h_2) \\
&= f(k_1)g(h_1)f(k_2)g(h_2) = \varphi(k_1, h_1)\varphi(k_2, h_2) \\
&\forall (k_1, h_1), (k_2, h_2) \in K \rtimes_\theta H
\end{aligned}$$

En particular, tendremos que:

$$\begin{aligned}
\varphi(k, 1) &= f(k)g(1) = f(k) \qquad \forall k \in K \\
\varphi(1, h) &= f(1)g(h) = g(h) \qquad \forall h \in H
\end{aligned}$$

Ahora, si $\phi : G \to T$ es otro homomorfismo que verifica que:

$$\phi(k, 1) = f(k) \qquad \phi(1, h) = g(h) \qquad \forall k \in K, \forall h \in H$$

Entonces:

$$\phi(k, h) = \phi(k, 1)\phi(1, h) = f(k)g(h) = \varphi(k, h) \qquad \forall (k, h) \in K \rtimes_\theta H$$

Por lo que $\phi = \varphi$. □

La siguiente Proposición nos será de utilidad para clasificar grupos haciéndolos isomorfos a un producto semidirecto, a partir del orden.

Teorema 7.5. *Sea G un grupo y $K, H < G$ con $K \lhd G$ que verifican:*

- $KH = G$.
- $K \cap H = \{1\}$.

Sea $\theta : H \to Aut(K)$ *un homomorfismo que nos da la acción por conjugación*[3] $ac : H \times K \to K$*:*

$$\theta(h)(k) = hkh^{-1} \qquad \forall (k,h) \in K \rtimes_\theta H$$

Entonces, $K \rtimes_\theta H \cong G$.

Demostración. Definiremos la aplicación $f : K \rtimes_\theta H \to G$ dada por:

$$f(k,h) = kh \qquad \forall k \in K, \forall h \in H$$

Veamos que es un isomorfismo:

- f es sobreyectiva, ya que $G = KH$, de donde cualquier elemento $g \in G$ se escribe como $g = kh$, para cierto $(k,h) \in K \rtimes_\theta H$.
- Para la inyectividad, si $f(k_1,h_1) = f(k_2,h_2)$, entonces $k_1h_1 = k_2h_2$, de donde $k_2^{-1}k_1 = h_2h_1^{-1}$:
  - $k_2^{-1}k_1 \in K$.
  - $h_2h_1^{-1} \in H$.

  Y como $H \cap K = \{1\}$, concluimos que $k_1 = k_2$ y $h_1 = h_2$, de donde f es inyectiva.
- Para ver que f es un homomorfismo, si $(k_1,h_1),(k_2,h_2) \in K \rtimes_\theta H$:

$$\begin{aligned} f((k_1,h_1)(k_2,h_2)) &= f(k_1\,{}^{h_1}k_2, h_1h_2) = f(k_1h_1k_2h_1^{-1}, h_1h_2) \\ &= k_1h_1k_2h_1^{-1}h_1h_2 = k_1h_1k_2h_2 = f(k_1,h_1)f(k_2,h_2) \end{aligned}$$

□

Definición 7.4.

- Si G verifica las condiciones del Teorema anterior, decimos que G es <u>producto semidirecto interno</u> de K y H.
- Si $K < G$, un subgrupo $H < G$ se llama <u>complemento para K en G</u> si $G = KH$ con $K \cap H = \{1\}$.

De esta forma, tendremos que G será un producto semidirecto interno de dos subgrupos propios suyos si y solo si algún subgrupo propio normal tiene un complemento.

Ejemplo. Mostraremos ahora que dado un grupo G, no siempre será posible encontrar dos subgrupos propios suyos de forma que G sea producto semidirecto interno de ellos. Como vismo en la definición superior, este motivo puede ser por dos razones:

[3] La condición $K \lhd G$ nos dice que θ está bien definida

- Que G no tenga subgrupos normales propios, como puede ser cualquier grupo simple.
- Que G tenga subgrupos normales propios, pero que no seamos capaces de encontrar ningún complemento para algún subgrupo.

  Por ejemplo, si recordamos el Diagrama de Hasse de Q_2:

$$\begin{tikzcd}
 & Q_2 \arrow[dl, dash, "2"'] \arrow[d, dash, "2"'] \arrow[dr, dash, "2"] & \\
\langle i \rangle \arrow[dr, dash, "2"'] & \langle j \rangle \arrow[d, dash, "2"'] & \langle k \rangle \arrow[dl, dash, "2"] \\
 & \langle -1 \rangle \arrow[d, dash, "2"'] & \\
 & \{1\} &
\end{tikzcd}$$

Figura 7.1: Diagrama de Hasse para los subgrupos del grupo de los cuaternios.

  Vemos que todos los subgrupo de Q_2 son normales, pero sin embargo:

$$\langle i \rangle \cap \langle j \rangle \cap \langle k \rangle \cap \langle -1 \rangle = \{1, -1\}$$

  Por lo que dado un subgrupo normal propio de Q_2 no vamos a poder encontrar un complemento para él en Q_2.

Ejemplo. Como ejemplos de aplicaciones inmediantas del último Teorema, tenemos (no especificaremos bajo qué homomorfismo se realiza el producto semidirecto, entendiendo que es la acción por conjugación):

- Sea $G = S_n$, $K = A_n \lhd S_n$ y $H = \langle (1\ 2) \rangle \cong \mathbb{Z}_2$, entonces:

$$A_n H = S_n \qquad A_n \cap H = \{1\}$$

  Por lo que estamos en las condinciones de aplicar el Teorema, con lo que:

$$S_n \cong A_n \rtimes \mathbb{Z}_2$$

- En $G = S_4$, si tomamos $K = V \lhd S_4$, $H = S_3 = Stab_{S_4}(V)$, tenemos que:

$$VH = S_4 \qquad V \cap H = \{1\}$$

  Por lo que:

$$S_4 \cong V \rtimes S_3$$

- Sea $G = A_4$, $K = V \lhd A_4$, $H = \langle (1\ 2\ 3) \rangle$, tenemos que:

$$A_4 \cong V \rtimes H$$

Definición 7.5. Sea G un grupo, si tomamos $\theta : AutG) \to AutG)$ dado por:

$$\theta(\phi)(x) = \phi(x) \qquad \forall \phi \in AutG), \forall x \in G$$

Definimos el grupo holomorfo de G por:

$$Hol(G) = G \rtimes_\theta AutG)$$

7.2. Grupos de orden pq

En esta sección aprenderemos a clasificar los grupos no abelianos de orden pq con $p < q$ primos. recordemos que por ahora, los únicos grupos que sabemos clasificar son los grupos de orden primo (todos ellos son cíclicos), los de orden 4 (C_4 si es cíclico y v si no) y los de orden 6 (C_6 si es abeliano y s_3 si no).

En tal caso, el primer teorema de Sylow nos da la existencia de:

- P, un $p-$subgrupo de Sylow de orden p.
- Q, un $q-$subgrupo de Sylow de orden q.

Estudiemos cuántos $p-$subgrupos de Sylow y $q-$subgrupos de Sylow tendrá nuestro grupo G, de orden $|G| = pq$. Para ello, el Segundo Teorema de Sylow nos dice que:

$$\left.\begin{array}{r} n_q \mid p \\ n_q \equiv 1 \mod q \end{array}\right\} \Longrightarrow n_q \in \{1, p\}$$

Pero como $p < q$, no puede ser $n_q = p$, ya que entonces $p \equiv 0 \mod q$. De esta forma, sabemos que q es el único $q-$subgrupo de g, por lo que $q \lhd g$. En esta situación, tenemos que:

- $Q \cap P = \{1\}$, ya que si tomo $x \in Q \cap P$, tendremos que existen $k, l \in \mathbb{N}$ de forma que $p^k = O(x) = q^l$, luego ha de ser $k = 0 = l$ y $O(x) = 1$, luego $x = 1$.
- $QP = G$, ya que si aplicamos el segundo teorema de isomorfía: Tenemos que $QP/Q \cong P/P \cap Q$, de donde:

  $$|QP||P \cap Q| = |QP| = |Q||P| = QP = |G|$$

  Y como $QP < G$, tenemos que $PQ = G$.

Por tanto, si G es un grupo de orden pq con $p < q$, Q su único $q-$subgrupo de Sylow y P un $p-$subgrupo de Sylow, vamos a poder escribir siempre:

$$G \cong Q \rtimes P$$

Como $|Q| = q$, tenemos que $Q \cong C_q$. de la misma forma, como $|P| = p$, tenemos que $P \cong C_p$. Ahora, veamos qué opciones tenemos para n_p. Sabemos que:

$$\left.\begin{array}{r} n_p \mid q \\ n_p \equiv 1 \mod p \end{array}\right\} \Longrightarrow n_p \in \{1, q\}$$

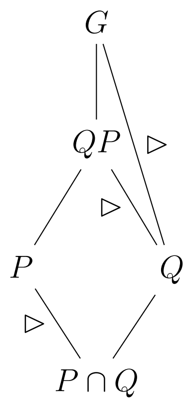


Figura 7.2: situación del teorema 3.10.

- Si $n_q = 1 = n_p$, entonces: tendremos que $P, Q \lhd G$, por lo que:

$$G \cong Q \rtimes P \cong Q \times P \cong C_q \times C_p \cong C_{pq}$$

- Si $n_q = 1$ y $n_p = q$, entonces:

$$q \equiv 1 \mod p \quad \Longrightarrow \quad q - 1 \equiv 0 \mod p$$

  de donde $p \mid q - 1$. Vamos a tratar estudiar cuántos grupos de la forma $G \cong C_q \rtimes_\theta C_p$ tenemos, cada uno de ellos dado por un homomorfismo $\theta : C_p \to Aut(C_q)$ distinto.

  Por la Proposición 7.1, tenemos que $Aut(C_q) \cong C_{q-1}$, por lo que es un grupo cíclico de orden $q - 1$. Sabemos por tanto que existe un único subgrupo cíclico $\langle \alpha \rangle < Aut(C_q)$ de orden p.

  De esta forma, cualquier homomorfismo $\theta : C_p \to Aut(C_q)$ debe aplicar y (el generador de C_p) en una potencia de α (ya que necesitamos que $(\theta(y))^p = 1$). Por tanto, existen p homomorfismos de esta forma, $\theta_k : C_p \to Aut(C_q)$ dado por:

$$\theta_k(y) = \alpha^k \qquad \forall k \in \{0, \ldots, p-1\}$$

  Notemos que θ_0 es el homomorfismo trivial, por lo que estamos en el caso anterior, $C_q \rtimes_{\theta_0} C_p \cong C_q \times C_p$. para los $p - 1$ homomorfismos restantes, los grupos $C_q \rtimes_{\theta_k} C_p$ son todos isomorfos entre sí, ya que para cada k, existe un generador $y_k \in C_p$ de forma que $\theta_k(y_k) = \alpha$, por lo que todos son el mismo, salvo la elección del generador de C_p. de esta forma, salvo isomorfismo, los $p - 1$ grupos se reducen en uno, que es:

$$G \cong C_q \rtimes_\theta C_p = \langle x, y \mid x^q = 1, y^p = 1, yxy^{-1} = \alpha(x) \rangle$$

  con $\alpha \in Aut(C_q)$ con orden p.

Ejemplo. Un caso particular del razonamiento descrito arriba es cuando $p = 2$ y $q > 2$, en cuyo caso tenemos que $2 \mid q - 1$ (ya que q va a ser impar, por ser primo mayor que 2):

$$C_q \rtimes C_2 = \langle x, y \mid x^q = 1, y^2 = 1, yxy^{-1} = \alpha(x) \rangle$$

Para cierto $\alpha \in Aut(C_q)$ con $o(\alpha) = 2$. sin embargo, automorfismos de C_q en C_q de orden 2 solo hay uno:

$$x \longmapsto x^{-1}$$

Por lo que tendremos:

$$C_q \rtimes C_2 = \langle x, y \mid x^q = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle = D_q$$

Por lo que si tenemos un grupo G de orden $|G| = 2q$ con $q \neq 2$ primo, entonces G será abeliano o será isomorfo a D_q.

Una vez estudiados los grupos de orden pq, p, q primos con $p < q$, observemos que ahora sabemos clasificar:

- Los grupos de orden[4] $6 = 2 \cdot 3$, que serán isomorfos a C_6 o a d_3.
- Los grupos de orden $10 = 2 \cdot 5$, que serán isomorfos a C_{10} o a D_5.
- Los grupos de orden $14 = 2 \cdot 7$, que serán isomorfos a C_{14} o a D_7.
- Los grupos de orden $15 = 3 \cdot 5$, que serán isomorfos a C_{15} y veamos que no hay otra posibilidad, ya que (sabemos ya que $n_5 = 1$):

$$\left.\begin{array}{r} n_3 \mid 5 \\ n_3 \equiv 1 \mod 3 \end{array}\right\} \longrightarrow n_3 = 1$$

  Por lo que solo tenemos dicha opción.

Si enumeramos todos los números del 1 al 15, tan solo nos quedan grupos de 2 órdenes que no sabemos clasificar, los grupos de orden 12 y los de orden 8.

7.3. Grupos de orden 12

Sea G un grupo de orden $|G| = 12 = 2^2 \cdot 3$:

Si G es abeliano, sabemos por el capítulo anterior que será isomorfo a:

$$C_2 \times C_2 \times C_3 \cong C_2 \times C_6 \qquad C_4 \times C_3 \cong C_{12}$$

Supuesto que G no es abeliano:

$$\left.\begin{array}{r} n_2 \mid 3 \\ n_2 \equiv 1 \mod 2 \end{array}\right\} \Longrightarrow n_2 \in \{1, 3\}$$

$$\left.\begin{array}{r} n_3 \mid 4 \\ n_3 \equiv 1 \mod 4 \end{array}\right\} \Longrightarrow n_3 \in \{1, 4\}$$

[4] ya lo sabíamos hacer de antes, pero ahora por otros motivos

- Supongamos que $n_2 = 3$ y $n_3 = 4$, entonces tendremos:

$$P_1, P_2, P_3, P_4 \in Syl_3(G) \qquad |P_i| = 3$$
$$Q_1, Q_2, Q_3 \in Syl_2(G) \qquad |Q_i| = 4$$

Por lo que deberíamos tener 8 elementos distintos de orden 3 (2 por cada $3-$subgrupo), el elemento neutro del grupo y nos queda espacio para 3 elementos más, que serán los elementos que necesitemos para los $2-$subgrupos. Por tanto, todos los $2-$subgrupos deberían contener a estos 3 elementos más el 1 y deberían ser distintos todos ellos, algo que es imposible.

Por tanto, tenemos que bien $n_3 = 1$ o bien $n_2 = 1$. En cualquier caso, tendremos la existencia de un $p-$subgrupo de Sylow ($p \in \{2, 3\}$) normal en G, así como que su intersección será trivial, y aplicando el segundo teorema de isomorfía tendremos que $HK = G$ (si K y H son los subgrupos de Sylow de G), por lo que en cualquier caso tendremos que $G \cong K \rtimes_\theta H$.

- Si $n_2 = 1 = n_3$, entonces tenemos dos subgrupos normales, con lo que:

$$G \cong C_2 \times C_6 \quad \text{o} \quad G \cong C_{12}$$

El primer caso si el $4-$subgrupo de Sylow es isomorfo a $C_2 \times C_2$ y el segundo si es isomorfo a C_4, por lo que volvemos al caso abeliano.

- Si $n_3 = 1$ y $n_2 = 3$, tenemos entonces dos casos a considerar:

$$G \cong K \rtimes H \cong \left\{ \begin{array}{l} C_3 \rtimes C_4 \\ C_3 \rtimes (C_2 \times C_2) \end{array} \right.$$

Ambos casos vendrán dados por un homomorfismo de codominio $Aut(C_3)$, donde el único automorfismo no trivial es el dado por:

$$x \overset{\alpha}{\longmapsto} x^{-1}$$

  - Para el caso $C_3 \rtimes C_4$, el único homomorfismo no trivial $\theta : C_4 \to Aut(C_3)$ que podemos considerar es el que lleva el generador de C_4 en α, es decir, si $C_4 = \langle y \rangle$, entonces consideramos:

$$\theta(y) = \alpha$$

y la imagen del homomorfismo quedará totalmente determinada de esta forma. En este caso, tenemos:

$$C_3 \rtimes C_4 = \langle x, y \mid x^3 = 1, y^4 = 1, yxy^{-1} = x^{-1} \rangle = Q_3$$

  - En el caso $C_3 \rtimes (C_2 \times C_2)$, tenemos tres homomorfismos no triviales a considerar (el trivial es el que manda ambos generadores a 1), suponiendo que $C_2 \times C_2 = \langle y, z \rangle$, entonces tendremos:

$$\theta_1(y) = 1 \qquad \theta_1(z) = \alpha$$
$$\theta_2(y) = \alpha \qquad \theta_2(z) = 1$$
$$\theta_3(y) = \alpha \qquad \theta_3(z) = \alpha$$

Observemos que en el último caso tendremos:

$$\theta_3(yz) = \theta_3(y)\theta_3(z) = \alpha^2 = 1$$

Y que $C_2 \times C_2 = \langle y, yz \rangle$. De esta forma, cada homomorfismo nos dará un grupo (la última relación viene porque y conmuta con z):

$$\langle x, y, z \mid x^3 = y^2 = z^2 = 1, yxy^{-1} = x, zxz^{-1} = x^{-1}, yzy^{-1} = z \rangle$$
$$\langle x, y, z \mid x^3 = y^2 = z^2 = 1, yxy^{-1} = x^{-1}, zxz^{-1} = x, yzy^{-1} = z \rangle$$
$$\langle x, y, yz \mid x^3 = y^2 = (yz)^2 = 1, yxy^{-1} = x^{-1}, ((yz)x(yz))^{-1} = x, yzy^{-1} = z \rangle$$

Sin embargo, todos ellos serán isomorfos entre sí (es fácil buscar un homomorfismo aplicando el Teorema de Dyck), por lo que nos quedamos con uno de ellos (con θ_2):

$$C_3 \rtimes_\theta (C_2 \times C_2) = \langle x, y, z \mid x^3 = y^2 = z^2 = 1, yxy^{-1} = x^{-1}, zxz^{-1} = x, yzy^{-1} = z \rangle$$

Si tomamos $r = xy$ y $s = yz$, obtenemos que es isomorfo a $D_6 \cong D_3 \times C_2$.

- En el caso $n_3 = 4$ y $n_2 = 1$, hay un ejercicio en la relación de $p-$grupos que decía que si un grupo de orden 12 tiene más de $3-$subgrupos de Sylow, entonces $G \cong a_4$. Para ello:

$$\phi : G \to Perm(Syl_3(G)) \cong S_4$$
$$G/\ker(\phi) \cong G \cong Im(\phi) \subseteq S_4$$

Por lo que $G < S_4$ con $|G| = 12$, luego ha de ser $G \cong A_4$. tendremos ahora:

$$G \cong H \rtimes K \cong \begin{cases} C_4 \rtimes C_3 \\ (C_2 \times C_2) \rtimes C_3 \end{cases}$$

  - Si $C_4 \rtimes C_3$, tendremos que la única acción no trivial es

$$\begin{array}{rccc} \theta : & C_3 & \longrightarrow & Aut(C_4) \cong C_2 \\ & y & \longmapsto & y^{-1} \end{array}$$

  con orden 2. Sin embargo, como su orden ha de dividir a $|C_3| = 3$, el morfismo no divide a 3, luego no hay nada no trivial ahí: todos los automorfismos son triviales. En dicho caso, tenemos:

$$C_4 \rtimes C_3 = C_4 \times C_3 = C_{12}$$

  - En el caso $(C_2 \times C_2) \rtimes C_3$, buscamos una acción $C_3 \to Aut(C_2 \times C_2) \cong s_3$, por lo que tendremos dos automorfismos no triviales de $C_2 \times C_2$ de orden 3.

$$\theta_1 : x \longmapsto \alpha$$
$$\alpha \begin{cases} y \longmapsto z \\ z \longmapsto yz \end{cases}$$

$$\theta_2 : x \longmapsto \alpha^2$$
$$\alpha^2 \left\{ \begin{array}{l} y \longmapsto yz \\ z \longmapsto y \end{array} \right.$$

Que podemos pensarlo con:

$$(1,0),(0,1) \longmapsto (0,1),(1,1)$$

Por lo que:

$$\begin{aligned} &(C_2 \times C_2) \rtimes_{\theta_1} C_3 \\ &= \langle x, y, z \mid x^3 = 1, y^2 = z^2 = 1, xyx^{-1} = z, xzx^{-1} = zy, yz = zy \rangle \cong A_4 \end{aligned}$$

este último isomorfismo no sale fácil. ver que un grupo es A_4 suele verse siempre viendo que tiene más de un $3-$subgrupo de Sylow.

Como resumen, salvo isomorfismos hay 5 grupos de orden 12:

- Dos abelianos, C_{12} y $C_2 \times C_6$.
- Tres no abelianos, D_6, Q_3 y A_4.

7.4. Grupos de orden 8

Sea G un grupo de orden 8, no vamos a tener $p-$subgrupos de Sylow, porque el único es el total, luego no nos aporta información sobre la estructura de G. Recordamos que los grpuos abelianos de orden 8 son:

$$C_2 \times C_2 \times C_2 \qquad C_2 \times C_4 \qquad C_8$$

Si G es un grupo no abeliano de orden 8, entonces no existen elementos en G de orden 8, ya que entonces G sería cíclico, luego abeliano. Por tanto, los elementos de G tendrán orden 2 o 4. Tampoco pueden ser todos de orden 2, puesto que G también sería abeliano:

$$(xy)(xy) = 1 \longrightarrow xy = yx \qquad \forall x, y \in G$$

Por lo que $\exists a \in G$ de forma que $O(a) = 4$. consideramos:

$$H = \langle a \rangle = \{1, a, a^2, a^3\}$$

Tenemos que $[G : H] = 2$, por lo que $H \lhd G$. dado $b \in G \setminus H$, tendremos dos clases en el cociente:

$$G = H \cup Hb$$

De esta forma, podemos describir G como:

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

si consideramos b^2, veamos en qué clase está. supuesto que $b^2 \in Hb$, entonces:

- Puede ser que $b^2 = b \Longrightarrow b = 1$.

- Puede ser $b^2 = ab \Longrightarrow b = a$.
- Puede ser $b^2 = a^2b \Longrightarrow b = a^2$.
- Puede ser $b^2 = a^3b \Longrightarrow b = a^3$.

Todas imposibles, por lo que $b^2 \in H = \{1, a, a^2, a^3\}$, de donde:

- Si $b^2 = a$, entonces $O(b^2) = O(a) \longrightarrow O(b) = 8$, imposible.
- Si $b^2 = a^3$, entonces $O(b^2) = O(a^3) = O(a)$, imposible.
- Si $b^2 = 1$, veamos que $ba = a^3b$. como $h \lhd g$, tenemos que $bab^{-1} \in h$, pero como $O(b) = 2$, tenemos que $bab \in h$ y:

  $$O(bab) = O(a) = 4$$

  de donde $bab \in \{a, a^3\}$. si $bab = a$, entonces G es abeliano, imposible, por lo que:

  $$bab = a^3$$

  por lo que en este caso tenemos:

  $$G = \langle a, b \mid a^4 = b^2 = 1, ba = a^3b\rangle = D_4$$

- Si $b^2 = a^2$, vamos a probar la misma igualdad: $ba = a^3b$. para ello, como $H \lhd G$, tenemos que $bab^{-1} \in h$, pero como:

  $$O(bab^{-1}) = O(a) = 4$$

  Por lo que $bab^{-1} \in \{a, a^3\}$. Si $bab^{-1} = a$, entonces es abeliano, por lo que también tenemos $bab = a^3$. En este caso:

  $$G = \langle a, b \mid a^4 = 1, a^2 = b^2, ba = a^3b\rangle = Q_2$$

de esta forma, los únicos grupos no abelianos de orden 8 son:

$$D_4 \qquad Q_2$$

Para grupos de orden 12 podríamos haber emplear también este mismo tipo de razonamiento.

7.5. Clasificación de grupos de orden menor o igual que 15

Sabemos ya los únicos grupos de orden menor o igual a 15 que hay salvo isomorfismos, los cuales vamos a listar a continuación en una tabla resumen:

- De orden 1: $\{1\}$.
- De orden 2: C_2.

- De orden 3: C_3.
- De orden 4: $C_4, C_2 \oplus C_2$.
- De orden 5: C_5.
- De orden 6: C_6, D_3.
- De orden 7: C_7.
- De orden 8: $C_8, C_4 \oplus C_2, C_2 \oplus C_2 \oplus C_2, D_4, Q_2$.
- De orden 9: $C_9, C_3 \oplus C_3$.
- De orden 10: C_{10}, D_5.
- De orden 11: C_{11}.
- De orden 12: $C_{12}, C_6 \oplus C_2, D_6, Q_3, A_4$.
- De orden 13: C_{13}.
- De orden 14: C_{14}, D_7.
- De orden 15: C_{15}.

Ya que:

- De orden 1 solo está el grupo trivial, como vimos en los primeros capítulos.
- Como 2 es primo, solo está el grupo cíclico.
- Como 3 es primo, solo está el grupo cíclico.
- Como 4 es un primo al cuadrado, por un corolario del Teorema de Burnside sabemos que tiene que ser abeliano, luego no hay más.
- Como 5 es primo, solo está el grupo cíclico.
- $6 = 2 \cdot 3$, de la forma pq con $p = 2$, luego solo está el cíclico y D_3.
- Como 7 es primo, solo está el grupo cíclico.
- Para 8 hemos realizado un análisis especial, obteniendo que hay 5 grupos, 3 abelianos y 2 no abelianos.
- Como 9 es un primo al cuadrado, sabemos que tiene que ser un grupo abeliano.
- $10 = 2 \cdot 5$, de la forma pq con $p = 2$, luego solo está el cíclico y D_5.
- Como 11 es primo, solo está el grupo cíclico.
- Para 12 hemos realizado un análisis especial, obteniendo que hay 5 grupos de orden 12, 2 abelianos y 3 no abelianos.
- Como 13 es primo, solo está el grupo cíclico.

- $14 = 2 \cdot 7$, de la forma pq con $p = 2$, luego solo está el cíclico y D_7.
- $15 = 3 \cdot 5$, de la forma pq y anteriormente discutimos este caso.

Si ha llegado hasta aquí y desea saber cómo se clasifican los grupos de orden pq, 12 y 8, le recomendamos que consulte `https://github.com/Joshoccas/3-DGIIM/tree/main/SegundoCuatrimestre/`.