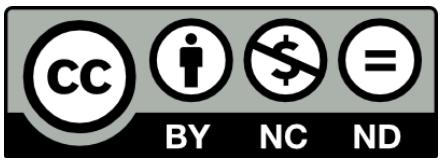
# Álgebra II


**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

# 1. $G-$conjuntos y $p$-grupos

**Definición 1.1.** Sea $G$ un grupo y $X$ un conjunto no vacío, una acción[1] de $G$ sobre $X$ es una aplicación:

$$\begin{array}{rccc} ac: & G\times X & \longrightarrow & X \\ & (g,x) & \longmapsto & ac(g,x) \end{array}$$

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 <u>acción trivial</u>:
$$\begin{array}{rccc} ac: & G\times X & \longrightarrow & X \\ & (g,x) & \longmapsto & x \end{array}$$

2. Si tenemos una acción $ac: G\times X\to X$ y $H<G$, podemos considerar la <u>acción por restricción</u> $ac: H\times X\to X$, 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 $X = \{1, \dots, n\}$ 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 1.1.** *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 $\phi$ está bien definida, es decir, que $\phi(g) \in \mathrm{Perm}(X)$ para cada $g \in G$. Para ello, veamos antes que $\phi$ 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 $\phi$ está bien definida.

  Además, por las dos propiedades anteriores, tenemos que $\phi$ 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 1.2** (Representación por permutaciones)**.** Sea $G$ un grupo y $X$ un conjunto no vacío, si tenemos una acción de $G$ sobre $X$, el homomorfismo $\phi$ dado por esta acción según la Proposición 1.1 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 $\phi$, 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 1.2** (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, $\phi: G \to \mathrm{Perm}(G)$ 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 $\phi$, obtenemos que:

$$G \cong G/\{1\} \cong Im(\phi)$$

Donde $Im(\phi) = \phi_*(G)$, que en la Proposición **??** vimos que es un subgrupo de $\mathrm{Perm}(G)$. □

**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 acción por conjugación se define como $ac: G \times G \to G$ dada por:
$$ac(g, h) = {}^gh = ghg^{-1}$$
Que es una acción, ya que:
$$\begin{aligned} {}^1h &= 1h1^{-1} = h \qquad \forall h \in G \\ {}^g({}^hl) &= g\,{}^hlg^{-1} = ghlh^{-1}g^{-1} = ghl(gh)^{-1} = {}^{gh}l \qquad \forall g, h, l \in G \end{aligned}$$
El homomorfismo asociado es:
$$\begin{array}{c} \phi: G \to \mathrm{Perm}(G) \\ \phi(g)(h) = ghg^{-1} \qquad \forall g, h \in G \end{array}$$
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 acción por conjugación en partes de $G$ 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 **??** vimos que $gHg^{-1}$ era un subgrupo de $G$, al que llamaremos subgrupo conjugado de $G$.

## 1.1. Órbitas de un elemento

**Definición 1.3** (Órbita)**.** Sea $G$ un grupo y $X$ un $G-$conjunto, definimos en $X$ una relación de equivalencia $\sim$ (se comprueba a continuación) dada por:

$$y \sim x \iff \exists g \in G \mid y = {}^gx$$

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 1.3.** *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 $z \sim x$. □

**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 $X$ desde los que podemos llegar a $x$ 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 1.4.** 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 1.5** (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 1.4.** *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:

  $$x = {}^1x = {}^{g^{-1}g}x = {}^{g^{-1}}({}^g x) = {}^{g^{-1}}x = y$$

  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:

  $${}^{gh}x = {}^g({}^h x) = {}^g x = x$$

  Por lo que $gh \in Stab_G(x)$.

□

**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 1.5.** *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:
$$\phi(gStab_G(x)) = {}^g x \qquad \forall gStab_G(x) \in G/_{Stab_G(x)}\sim$$

- 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:
$$\phi(gStab_G(x)) = {}^g x = {}^{g'h} x = {}^{g'}({}^h x) = {}^{g'} x = \phi(g'Stab_G(x))$$

- Veamos que es sobreyectiva: sea $y \in Orb(x)$, entonces $\exists g \in G$ de forma que:
$$y = {}^g x$$
Por lo que $y = \phi(gStab_G(x))$.

- Para la inyectividad, sean $g, g' \in G$ de forma que:
$${}^g x = \phi(gStab_G(x)) = \phi(g'Stab_G(x)) = {}^{g'} x$$
Entonces, podemos escribir:
$$x = {}^{g^{-1}}({}^g x) = {}^{g^{-1}}({}^{g'} x) = {}^{g^{-1}g'} x$$
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 1.6.** *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 1.6.** 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 1.7.** *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. En el caso de que $X$ sea un conjunto finito y tenga $n$ elementos:

$$X = \{x_1, \ldots, x_n\}$$

Por ser $\sim$ una relación de equivalencia, tenemos una partición de $X$, lo que nos da la igualdad:

$$|X| = \sum_{k=1}^{n} |Orb(x_k)|$$

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 $\Gamma$ contiene un único representante de cada una de las órbitas de elementos que no son puntos fijos ($\Gamma \subseteq X \setminus Fix(X)$):

$$|X| = \sum_{k=1}^{n} |Orb(x_k)| = |Fix(X)| + \sum_{y \in \Gamma} |Orb(y)|$$

Y aplicando finalmente la Proposición 1.5, llegamos a que:

$$|X| = \sum_{k=1}^{n} |Orb(x_k)| = |Fix(X)| + \sum_{y \in \Gamma} |Orb(y)| = |Fix(X)| + \sum_{y \in \Gamma} [G : Stab_G(y)]$$

A continuación, lo que haremos será estudiar los conjuntos $Orb(\cdot)$, $Stab_G(\cdot)$ y $Fix(X)$ para ciertos ejemplos comunes de acciones.

### 1.1.1. 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, $Fix(G) = \emptyset$.

### 1.1.2. 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 1.7** (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 1.8** (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 1.8.** *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 1.9.** *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:

$$Orb(h) = \{k \in G \mid \exists g \in G \text{ con } k = {}^g h = ghg^{-1}\} = \{ghg^{-1} \mid g \in G\} = Cl_G(h) \qquad \forall h \in G$$

De esta forma, llamaremos a la órbita de $h$ por la acción por conjugación la clase de conjugación de $h$ en $G$.

$$Stab_G(h) = \{g \in G \mid {}^g h = ghg^{-1} = h\} = \{g \in G \mid gh = hg\} = C_G(h)$$

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 1.5, 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:

$$Fix(X) = \{h \in G \mid ghg^{-1} = {}^g h = h \quad \forall g \in G\} = \{h \in G \mid gh = hg \quad \forall g \in G\} = Z(G)$$

**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**:

$$|G| = |Z(G)| + \sum_{y \in \Gamma} [G : C_G(y)]$$

Donde podemos pensar en $\Gamma$ en el conjunto formado por los representantes de las órbitas con más de un elemento.

Esta última podemos generalizarla para cualquier subgrupo $H \lhd G$, obteniendo la **fórmula de clases general**:

$$|H| = |H \cap Z(G)| + \sum_{y \in \Gamma} [G : C_G(y)]$$

### 1.1.3. 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.

[5]está bien definida gracias a la Proposición **??**

*Observación.* Sea $G$ un grupo, $H \in Subg(G)$, si consideramos la acción por conjugación sobre subgrupos, tenemos que:

$$Orb(H) = \{H\} \iff H \lhd G$$

Esto se debe a que:

$$Orb(H) = \{H\} \iff \{gHg^{-1} \mid g \in G\} = \{H\} \iff H \lhd G$$

Donde la última equivalencia se tiene gracias a la Proposición **??**, donde vimos una caracterización de los subgrupos normales.

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:

$$|Orb(H)| = [G : N_G(H)]$$

## 1.2. $p-$grupos

**Definición 1.9** ($p-$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 **??**):

$$O(x) = \frac{n}{\text{mcd}(x, n)} \qquad \forall x \in \mathbb{Z}_n$$

Por lo que:

$$O(1) = 8 = 2^3 \qquad O(2) = 4 = 2^2 \qquad O(3) = 8 = 2^3 \qquad O(4) = 2$$
$$O(5) = 8 = 2^3 \qquad O(6) = 4 = 2^2 \qquad O(7) = 8 = 2^3$$

**Teorema 1.10** (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 $\sigma = (1\ 2\ \ldots\ p) \in S_p$, consideramos $H = \langle\sigma\rangle = \{1, \sigma, \ldots, \sigma^{p-1}\} \subseteq S_p$. Consideramos también la acción $ac : H \times X \to X$ dada por (compruébese que es una acción):

$$ac(\sigma^k, (a_1, a_2, \ldots, a_p)) = \left(a_{\sigma^k(1)}, a_{\sigma^k(2)}, \ldots, a_{\sigma^k(p)}\right) \qquad \forall (a_1, \ldots, a_p) \in X, \forall \sigma^k \in H$$

Por la Proposición 1.5, tenemos que:

$$|Orb(z)| = [H : Stab_H(z)] = \frac{|H|}{|Stab_H(z)|} \qquad \forall z \in X$$

De donde tenemos que $|Orb(a_1, \ldots, a_p)|$ es un divisor de $|H|$, $\forall (a_1, \ldots, a_p) \in X$. En dicho caso, $|Orb(a_1, \ldots, a_p)| \in \{1, p\}$, 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 $Orb(a_1, \ldots, a_p)$:

$$\begin{aligned} Orb(a_1, \ldots, a_p) &= \left\{ \sigma^k (a_1, \ldots, a_p) \mid k \in \{0, \ldots, p-1\} \right\} \\ &= \{(a_1, \ldots, a_p), (a_2, \ldots, a_p, a_1), \ldots, (a_p, a_1, \ldots, a_{p-1})\} \end{aligned}$$

Por tanto, la órbita será unitaria si y solo si $a_1 = a_2 = \ldots = a_p$. Además, sabemos de la existencia de órbitas con un elemento ($r \geqslant 1$), como $Orb(1, 1, \ldots, 1)$. 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 $Orb(a, a, \ldots a)$ 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 1.10.1.** *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 1.11** (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 1.12.** *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 1.12.1.** *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 1.13.** *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:

    $$|Z(G)| = |G| - \sum_{h \in \Gamma} [G : C_G(h)]$$

    Y como $p$ 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.

### 1.2.1. $p-$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 1.10** ($p-$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 1.13.1** (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 1.13 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 $[H : P]$.

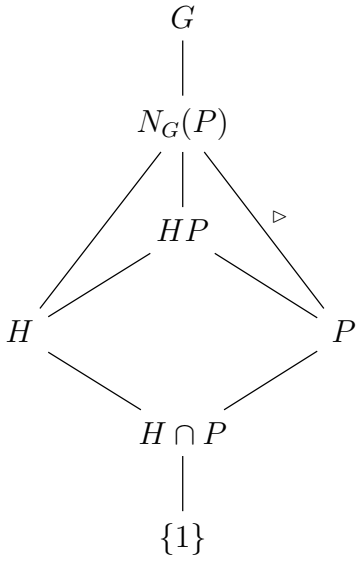
El siguiente Lema también recibe el nombre de Segundo Teorema de Sylow, aunque nos reservamos este nombre para el resultado que se demuestra a partir del Lema.

**Lema 1.14.** *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 1.8) 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:

  $$H < HP < N_G(P) \qquad [N_G(P) : P] = [N_G(P) : HP][HP : P]$$

  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 1.10.1), 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 $r = 1$. □

**Teorema 1.15** (Segundo Teorema de Sylow)**.** *Sea $G$ un grupo finito, $p$ un número primo, supongamos que $|G| = p^k m$ con $\text{mcd}(p, m) = 1$ 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 **??** que $gPg^{-1} < G$, para todo $g \in G$.
- Si $gxg^{-1} \in gPg^{-1}$, entonces:

  $$O(gxg^{-1}) = O(x) = p^k$$

  Para cierto $k \in \mathbb{N}$, por ser $P$ un $p-$grupo, por lo que $ac(g, P) = gPg^{-1}$ seguirá siendo un $p-$grupo.
- Además, 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 $\phi_g$ es sobreyectiva.
  - Si $gxg^{-1} = gyg^{-1}$, entonces $x = y$, por lo que $\phi_g$ 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:

$$\begin{aligned} Orb(P_1) &= \{gP_1g^{-1} \mid g \in G\} \\ Stab_G(P_1) &= \{g \in G \mid gP_1g^{-1} = P_1\} = N_G(P_1) \end{aligned}$$

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:

$$n_p = 1 + pn$$

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.

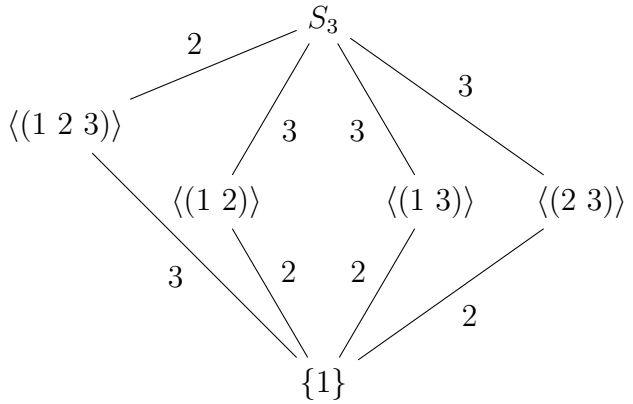



Figura 1.1: Diagrama de Hasse para los subgrupos de $S_3$.

  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:

$$\left.\begin{array}{rr} & n_3 \mid 2 \\ n_3 \equiv 1 & \mod 3 \end{array}\right\} \Longrightarrow n_3 = 1$$

- 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:
    $$\left.\begin{array}{rr} & n_2 \mid 3 \\ n_2 \equiv 1 & \text{mód } 2 \end{array}\right\} \Longrightarrow n_2 \in \{1, 3\}$$
    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:
    $$\left.\begin{array}{rr} & n_3 \mid 4 \\ n_3 \equiv 1 & \text{mód } 3 \end{array}\right\} \Longrightarrow n_3 \in \{1, 4\}$$
    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:
    $$\left.\begin{array}{rr} & n_2 \mid 3 \\ n_2 \equiv 1 & \text{mód } 2 \end{array}\right\} \Longrightarrow n_2 \in \{1, 3\}$$
    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 $Q = S_4$, <u>contradicción</u>.
    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:

$$\left.\begin{array}{rr} & n_3 \mid 8 \\ n_3 \equiv 1 & \text{mód } 3 \end{array}\right\} \Longrightarrow n_3 \in \{1, 4\}$$

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 1.15.1.** *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:

$$\left.\begin{array}{rr} & n_7 \mid 5 \\ n_7 \equiv 1 & \text{mód } 5 \end{array}\right\} \Longrightarrow n_7 = 1$$

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 1.16.** *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:*

$$G = \prod_{H \in Syl(G)} H$$

*Demostración.* En la caracterización de producto directo interno para una cantidad finita de subgrupos (Teorema **??**), vimos que $G$ era producto directo interno de todos ellos (los llamaremos $H_i$ con $i \in \{1, \dots, n\}$) si y solo si:

- $H_i \lhd G$ para todo $i \in \{1, \dots, n\}$.
- $H_1 H_2 \dots H_n = G$.
- $(H_1 \dots H_{i-1}) \cap H_i = \{1\}$, para todo $i \in \{2, \dots, k\}$

Basta pues, demostrar estos 3 puntos. Supuesto que $|G| = p_1^{n_1} \dots p_k^{n_k}$, llamamos $P_i$ al único $p_i-$subgrupo de Sylow, para todo $i \in \{1, \dots, k\}$.

- Por hipótesis, tendremos que $P_i \lhd G$ para todo $i \in \{1, \dots, k\}$.
- También:
$$|P_1 P_2 \dots P_K| = |P_1||P_2| \dots |P_k| = |G|$$
Y como tenemos siempre que $P_1 P_2 \dots P_k < G$, deducimos que $P_1 P_2 \dots P_k = G$.
- Fijado $i \in \{2, \dots, k\}$, veamos que $(P_1 \dots P_{i-1}) \cap P_i = \{1\}$. Para ello, sea $x \in (P_1 \dots P_{i-1}) \cap P_i$, tenemos:
$$\left.\begin{array}{l} O(x) \mid |P_1 \dots P_{i-1}| = p_1^{n_1} \dots p_{i-1}^{n_{i-1}} \\ O(x) \mid |P_i| = p_i^{n_i} \end{array}\right\} \Longrightarrow O(x) = 1 \Longrightarrow x = 1$$

□

*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.

# 2. 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.

## 2.1. 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 **??** vimos que:

$$C_n \oplus C_m \cong C_{nm} \iff \text{mcd}(n, m) = 1$$

2. En el Teorema 1.16 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 2.1** (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 $\beta_i$, 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:

$$\begin{aligned} 4 &\longrightarrow A \cong C_{81} \\ 3,1 &\longrightarrow A \cong C_{27} \oplus C_3 \\ 2,2 &\longrightarrow A \cong C_9 \oplus C_9 \\ 2,1,1 &\longrightarrow A \cong C_9 \oplus C_3 \oplus C_3 \\ 1,1,1,1 &\longrightarrow A \cong C_3 \oplus C_3 \oplus C_3 \oplus C_3 \end{aligned}$$

### 2.1.1. Descomposición cíclica primaria

**Teorema 2.2** (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 2.1, 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 2.1.** Sea $A$ un grupo abeliano finito, el Teorema 2.2 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 |
|---:|---|
| $2^3\ 3^2\ 5$ | $C_8 \oplus C_9 \oplus C_5$ |
| $2^2\ 2\ 3^2\ 5$ | $C_4 \oplus C_2 \oplus C_9 \oplus C_5$ |
| $2\ 2\ 2\ 3^2\ 5$ | $C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5$ |
| $2^3\ 3\ 3\ 5$ | $C_8 \oplus C_3 \oplus C_3 \oplus C_5 \oplus C_8$ |
| $2\ 2^2\ 3\ 3\ 5$ | $C_2 \oplus C_4 \oplus C_3 \oplus C_3 \oplus C_5$ |
| $2\ 2\ 2\ 3\ 3\ 5$ | $C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$ |

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 **??**, podemos escribir (multiplicando aquellos cíclicos de mayor orden que sean primos relativos):

$$\begin{aligned}
C_8 \oplus C_9 \oplus C_5 &\cong C_{360} \\
C_4 \oplus C_2 \oplus C_9 \oplus C_5 &\cong C_{180} \oplus C_2 \\
C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5 &\cong C_{90} \oplus C_2 \oplus C_2 \\
C_8 \oplus C_3 \oplus C_3 \oplus C_5 \oplus C_8 &\cong C_{120} \oplus C_3 \\
C_2 \oplus C_4 \oplus C_3 \oplus C_3 \oplus C_5 &\cong C_{60} \oplus C_6 \\
C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5 &\cong C_{30} \oplus C_6 \oplus C_2
\end{aligned}$$

**Corolario 2.2.1.** *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 2.2, podemos escribir:

$$A \cong C_{p_1} \oplus C_{p_2} \oplus \ldots \oplus C_{p_k}$$

Y como $\text{mcd}(p_i, p_j) = 1$ para cada $i, j \in \{1, \ldots, k\}$ con $i \neq j$, tenemos que:

$$C_{p_1} \oplus C_{p_2} \oplus \ldots \oplus C_{p_k} = C_{p_1 p_2 \ldots p_k} = C_n$$

□

## 2.1.2. Descomposición cíclica

**Teorema 2.3** (Descomposición cíclica de un grupo abeliano finito)**.**
*Si $A$ es un grupo abeliano finito, entonces existen unos únicos $d_1, d_2, \ldots, d_t \in \mathbb{N}$ de forma que:*

$$d_1 d_2 \ldots d_t = |A| \qquad y \qquad d_i \mid d_j, \quad \forall j \leqslant i$$

*Para los que se tiene que:*

$$A \cong C_{d_1} \oplus C_{d_2} \oplus \ldots \oplus C_{d_t}$$

*Demostración.* Supuesto que $|A| = p_1^{r_1} \ldots p_k^{r_k}$ es la descomposición de $|A|$ en primos, si usamos la descomposición que nos da el Teorema 2.2, existen $t_1, t_2, \ldots, t_k \in \mathbb{N}$ y

$$\begin{aligned} m_{i1} \geqslant m_{i2} \geqslant \ldots \geqslant m_{it_i} \geqslant 1 \\ m_{i1} + m_{i2} + \ldots + m_{it_i} = r_i \\ \forall i \in \{1, \ldots, k\} \end{aligned}$$

De forma que:

$$A \cong \bigoplus_{i=1}^{k} \left( \bigoplus_{j=1}^{t_i} C_{p_i^{m_{ij}}} \right)$$

Sea $t = \text{máx}\{t_1, t_2, \ldots, t_k\}$, definimos:

$$n_{ij} = \begin{cases} m_{ij} & \text{si } j \leqslant t_i \\ 0 & \text{si } j > t_i \end{cases} \qquad \forall j \in \{1, \ldots, t\}, \in i\{1, \ldots, k\}$$

Observemos que no hemos hecho mas que extender la anterior tabla dentada $(m_{ij})_{\substack{j \in \{1,\ldots,t_i\} \\ i \in \{1,\ldots,k\}}}$ a la tabla $k \times t$ $(n_{ij})_{\substack{j \in \{1,\ldots,t\} \\ i \in \{1,\ldots,k\}}}$, rellenando con ceros los huecos que no teníamos. De esta forma, si consideramos la matriz que en la entrada $(i, j)$ tiene $p_i^{n_{ij}}$:

$$\begin{pmatrix} p_1^{n_{11}} & p_1^{n_{12}} & \ldots & p_1^{n_{1t}} \\ p_2^{n_{21}} & p_2^{n_{22}} & \ldots & p_2^{n_{2t}} \\ \vdots & \vdots & \ddots & \vdots \\ p_k^{n_{k1}} & p_k^{n_{k2}} & \ldots & p_k^{n_{kt}} \end{pmatrix}$$

Tenemos que $A$ es la suma directa 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 $n_{ij} \geqslant n_{ij+1}$ (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 2.2 más la construcción de los $d_j$ realizada. □

**Definición 2.2.** Sea $A$ un grupo abeliano finito, el Teorema 2.3 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 |
|---|---|---|---|
| $\{2^2, 3^2, 5\}$ | $C_4 \oplus C_9 \oplus C_5$ | $d_1 = 2^2 \cdot 3^2 \cdot 5 = 180$ | $C_{180}$ |
| $\{2, 2, 3^2, 5\}$ | $C_2 \oplus C_2 \oplus C_9 \oplus C_5$ | $d_1 = 2 \cdot 3^2 \cdot 5 = 90$<br>$d_2 = 2$ | $C_{90} \oplus C_2$ |
| $\{2^2, 3, 3, 5\}$ | $C_4 \oplus C_3 \oplus C_3 \oplus C_5$ | $d_1 = 2^2 \cdot 3 \cdot 5 = 60$<br>$d_2 = 3$ | $C_{60} \oplus C_3$ |
| $\{2, 2, 3, 3, 5\}$ | $C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$ | $d_1 = 2 \cdot 3 \cdot 5 = 30$<br>$d_2 = 2 \cdot 3 = 6$ | $C_{30} \oplus C_6$ |

**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 **??** y el Corolario **??**:
  - $O(0) = 1$.
  - 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 $\mathbb{Z}_6 \oplus \mathbb{Z}_2$:

$$O(a,b) \in \text{mcm}(Div(6), Div(2)) = \text{mcm}(\{1,2,3,6\},\{1,2\}) = \{1,2,3,6\} \quad \forall (a,b) \in \mathbb{Z}_6 \oplus \mathbb{Z}_2$$

  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:
  - $O(0,0) = 1$.
  - $O(1,b) = O(5,b) = 6$ $\forall b \in \mathbb{Z}_2$.
  - $O(3,b) = 2$ $\forall b \in \mathbb{Z}_2$.
  - $O(2,0) = O(4,0) = 3$.
  - $O(2,1) = O(4,1) = 6$.

## 2.2. 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 2.3.** 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 2.4** (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 2.4.** *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 $A$:

$$\begin{aligned} \phi(x_1) &= (1, 0, \dots, 0) \\ \phi(x_2) &= (0, 1, \dots, 0) \\ &\vdots \\ \phi(x_r) &= (0, 0, \dots, 1) \end{aligned}$$

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 $\phi$ es biyectiva, por lo que $\phi$ nos da un isomorfismo entre $A$ y $\mathbb{Z}^r$. □

*Observación.* Observemos que si $A$ es un grupo abeliano libre de rango $r$, entonces tendremos que:

$$A \cong \mathbb{Z}^r$$

Además, si $H < A$, tendremos entonces que $H \cong \mathbb{Z}^s$, para cierta $s \leqslant r$.

De esta forma, si $A$ es un grupo finitamente generado, podemos descomponerlo en:

$$A \cong F \oplus T(A)$$

Que será la descomposición estándar de $A$. $F$ será un grupo abeliano libre de rango finito y:

$$T(A) = \{a \in A \mid O(a) < +\infty\}$$

Que recibe el nombre de subgrupo de torsión de $A$.

**Proposición 2.5.** *El subgrupo de torsión de un grupo es un grupo abeliano finito.*

De esta forma, existirán $r \geqslant 0$ y $d_1, \ldots, d_s$ con $d_i \mid d_j$ con $j \leqslant i$ de forma que:

$$d_1 d_2 \ldots d_s = |T(A)|$$

Por lo que:

$$A \cong \mathbb{Z}^r \oplus \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \ldots \oplus \mathbb{Z}_{d_s}$$

- Llamaremos $r$ al rango de $A$.
- A los $d_i$ los llamaremos factores invariantes de $A$.

**Ejemplo.** Si tomamos:

$$A = \langle x, y, z \mid x^3 = y^4, x^2 z = z^{-1} y, xy = yx, xz = zx, yz = zy \rangle$$

Si lo escribimos en notación aditiva:

$$A = \langle x, y, z \mid 3x = 4y, 2x + z = y - z, x + y = y + x, x + z = z + x, y + z = z + y \rangle$$

Si nos olvidamos de las últimas y pensamos que el grupo es abeliano, así como despejando:

$$A = \langle x, y, z \mid 3x - 4y = 0, 2x - y + 2z = 0 \rangle$$

Y tenemos el sistema:

$$M = \begin{pmatrix} 3 & -4 & 0 \\ 2 & -1 & 2 \end{pmatrix}$$

Tenemos 3 incógnitas y $rg(M) = 2$, un Sistema Compatible Indeterminado, con un parámetro libre. Veremos que transformaremos $M$ en:

$$\begin{pmatrix} 3 & -4 & 0 \\ 2 & -1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

Que es la forma normal de Smith (parecido a Hermite pero en $\mathbb{Z}$). De esta forma, tendremos que:

$$A \cong \mathbb{Z} \oplus \{0\} \oplus \mathbb{Z}_2 \cong \mathbb{Z} \oplus \mathbb{Z}_2$$

Sea:

$$A = \left\langle x_1, x_2, \ldots, x_n \mid \begin{array}{c} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0 \end{array} \right\rangle$$

con $n$ generadores y $m \leqslant n$ relaciones siendo. Sea:

$$X = \{e_1, \ldots, e_n\}$$

Consideramos $F = \langle X \rangle$, que será $F \cong \mathbb{Z}^r$. La descomposición estándar de $A$ será:

$$A = F + T(A)$$

Si definimos:

$$\begin{array}{rccc} \varphi: & F & \longrightarrow & A \\ & e_i & \longmapsto & x_i \end{array}$$

Tenemos que $\varphi$ está bien definida, así como que es sobreyectiva. Tendremos:

$$\ker(\varphi) < F$$

Por lo que:

$$\ker(\varphi) \cong \mathbb{Z}^m$$

De esta forma, si $\{y_1, \ldots, y_m\}$ es una base de $\ker(\varphi)$, cumplirá que (basta aplicar $\varphi$):

$$\left\{ \begin{array}{rl} a_{11}e_1 + a_{12}e_2 + \ldots + a_{1n}e_n & = y_1 \\ & \vdots \\ a_{m1}e_1 + a_{m2}e_2 + \ldots + a_{mn}e_n & = y_m \end{array} \right.$$

De esta forma, tenemos:

$$\ker(\varphi) \xrightarrow{i} F \to A$$

De forma que la matriz:

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

A la que llamaremos matrices de relaciones del grupo, que nos lleva el vector $(y_1, \ldots, y_m)$ en $(x_1, \ldots, x_n)$, tras multiplicar por $(e_1, \ldots, e_n)$, y tendremos aplicando Teoremas de Isomorfía que:

$$A \cong F/\ker(\varphi)$$

Esta matriz la convertiremos en la forma normal de Smith.

Como los factores invariantes eran productos de primos, no nos podrá salir ningún 1, por lo que esos unos los eliminaremos, ya que como factores invariantes han de ser mayor que 1.

**Ejemplo.** En $A = \mathbb{Z} \oplus \mathbb{Z}_2$, una base para $\mathbb{Z}$ es:

$$X = \{1\}$$

Y un sistema de generadores para $\mathbb{Z} \oplus \mathbb{Z}_2$ es:

$$\{(1, 1)\}$$

### 2.2.1. Forma Normal de Smith de una matriz

**Ejemplo.** Una forma de Hermite por filas es:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Las operaciones elementamos sobre matrices eran:

- Intercambiar filas.
- Mutiplicar una fila por un número.
- Sumar un múltiplo de una fila a otra.

Al hacer la forma normal de Smith podemos encontrar dos matrices $P$ y $Q$ regulares de forma que:

$$PAQ = \begin{pmatrix} d_1 & & & & \\ & d_2 & & & \\ & & \ddots & & \\ & & & d_s & \\ & & & & 0 \end{pmatrix}$$

De forma que $d_i \mid d_{i+1}$. $P$ contenía las transformaciones elementales por filas y $Q$ por columnas.

**Ejemplo.** Si consideramos:

$$\begin{pmatrix} 0 & 2 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 7 & 10 & 6 \end{pmatrix}$$

Como mcd de todos los elementos es 1, tenemos que poner un 1 arriba (consejo: no hacer ceros hasta poner un 1). Para ello, hacemos la cuarta fila más la segunda:

$$\begin{pmatrix} 0 & 2 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 1 & 6 & 0 \end{pmatrix}$$

Si nos la llevamos a la primera posición:

$$\begin{pmatrix} 1 & 6 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix}$$

Ahora, hacemos ceros en la primera fila, salvo el 1. Restamos a la primera la cuarta multiplicada por 3:

$$\begin{pmatrix} 1 & 0 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & -6 \\ 0 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix}$$

Como el mcd es 2, hay que sacar un 2 en la posición $2,2$. Para ello, intercambiamos las filas segunda y cuarta:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 6 & 6 \\ 0 & -4 & -6 \end{pmatrix}$$

Hacemos ceros:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

Como el mcd es 6 y tenemos un 6, hemos terminado. Hemos conseguido la forma normal de Smith.

**Ejemplo.** Calcular el rango de $A$ y todos los grupos abelianos no isomorfos de orden igual que la torsión.

$$A = \left\langle x, y, z, t \mid \begin{array}{c} 14x + 4y + 4z + 14t = 0 \\ -6x + 4y + 4z + 10t = 0 \\ -16x - 4y - 4z - 20t = 0 \end{array} \right\rangle$$

Calculamos la forma normal de Smith de la matriz:

$$\begin{pmatrix} 14 & 4 & 4 & 14 \\ -6 & 4 & 4 & 10 \\ -16 & -4 & -4 & -20 \end{pmatrix} \overset{F_1' = -(F_1 + F_3)}{\longrightarrow} \begin{pmatrix} 2 & 0 & 0 & 6 \\ -6 & 4 & 4 & 10 \\ -16 & -4 & -4 & -20 \end{pmatrix} \overset{C_4 - 3C_1}{\longrightarrow}$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ -6 & 4 & 4 & 28 \\ -16 & -4 & -4 & 28 \end{pmatrix} \overset{\substack{F_2 + 3F_1 \\ F_3 + 8F_1}}{\longrightarrow} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 4 & 28 \\ 0 & -4 & -4 & 28 \end{pmatrix} \overset{F_2 + F_3}{\longrightarrow}$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 56 \\ 0 & -4 & -4 & 28 \end{pmatrix} \overset{F_2 \leftrightarrow F_3}{\longrightarrow} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -4 & -4 & 28 \\ 0 & 0 & 0 & 56 \end{pmatrix} \overset{F_2' = -F_2}{\longrightarrow} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 4 & -28 \\ 0 & 0 & 0 & 56 \end{pmatrix} \overset{C_3 + 7C_2}{\longrightarrow}$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 4 & 0 \\ 0 & 0 & 0 & 56 \end{pmatrix} \overset{C_3 - C_2}{\longrightarrow} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 56 \end{pmatrix} \overset{C_3 \leftrightarrow C_4}{\longrightarrow} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 56 & 0 \end{pmatrix}$$

Por tanto, el rango de $A$ es (el número de incógnitas menos el rango de la matriz) 3. Ahora, la descomposición cíclica sería:

$$T(A) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{56}$$

Y la descomposición cíclica primaria:

$$T(A) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_7$$

Y tendremos:

$$A \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{56} \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_7$$

Para ello, buscamos los grupos $G$ con orden $2 \cdot 4 \cdot 8 \cdot 7 = 448 = 2^6 \cdot 7$ y descartamos el isomorfo a $T(A)$:

| Divisores elementales | Factores invariantes |
|---|---|
| $2^6, 7$ | $448$ |
| $2, 2^5, 7$ | $2, 224$ |
| $2, 2, 2^4, 7$ | $2, 2, 112$ |
| $2, 2, 2, 2, 2^3, 7$ | $2, 2, 2, 56$ |
| $2, 2, 2, 2, 2, 2^2, 7$ | $2, 2, 2, 2, 28$ |
| $2, 2, 2, 2, 2, 2, 2, 7$ | $2, 2, 2, 2, 2, 14$ |
| $2, 2^2, 2^3, 7$ | $2, 4, 56$ |
| $2^2, 2^2, 2^2, 7$ | $4, 4, 28$ |
| $2^3, 2^3, 7$ | $8, 56$ |
| $2^2, 2^4, 7$ | $4, 112$ |
| $2, 2, 2^2, 2^2$ | $2, 2, 4, 28$ |

¿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:

$$(0, 1, 1, 7)$$

**Ejemplo.** Forma normal de Smith de:

$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix}$$

Como no está en forma normal, hemos de añadir elementos para poder hayar el 2:

$$2 = \text{mcd}(4, 6, 8)$$

$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix} \overset{F_2+F_1}{\longrightarrow} \begin{pmatrix} 4 & 0 & 0 \\ 4 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix} \overset{C_2-C_1}{\longrightarrow} \begin{pmatrix} 4 & -4 & 0 \\ 4 & 2 & 0 \\ 0 & 0 & 8 \end{pmatrix} \longrightarrow$$
$$\begin{pmatrix} -4 & 4 & 0 \\ 4 & 2 & 0 \\ 0 & 0 & 8 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 4 & 0 \\ -4 & 4 & 0 \\ 0 & 0 & 8 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 4 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 8 \end{pmatrix} \longrightarrow$$
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 8 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 8 \\ 0 & 0 & 8 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 8 \\ 0 & -8 & 8 \end{pmatrix} \longrightarrow$$
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 8 \\ 0 & 0 & 24 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 24 \end{pmatrix}$$

**Ejemplo.** Sea $G$ un grupo abeliano de orden $n$ y $l(G)$ su longitud (la longitud de su serie de composición). Si la descomposición en factores primos de $n$ es:

$$n = p_1^{r_1} \dots p_r^{e_r}$$

Entonces:

$$l(G) = e_1 + \dots e_r$$

Y los factores de composición son:

$$fact(G) = (C_{p_1}, \overset{e_1}{\dots}, C_{p_1}, C_{p_2} \overset{e_2}{\dots}, C_{p_2}, \dots, C_{p_r} \overset{e_r}{\dots}, C_{p_r})$$

Como:

$$G \cong (C_{p_1^{\alpha_{11}}} \oplus \dots \oplus C_{p_1^{\alpha_{1n_1}}}) \oplus \dots \oplus (C_{p_r^{\alpha_{r1}}} \oplus \dots \oplus C_{p_r^{\alpha_{rn_1}}})$$

Para:

$$\begin{array}{cc} \alpha_{11} \geqslant \dots \geqslant \alpha_{1n_1} \geqslant 1 & \alpha_{11} + \dots + \alpha_{1n_1} = e_1 \\ \vdots & \vdots \\ \alpha_{r1} \geqslant \dots \geqslant \alpha_{rn_1} \geqslant 1 & \alpha_{r1} + \dots + \alpha_{rn_1} = e_r \end{array}$$

Como $G$ es abeliano, los factores de composición son cíclicos.

Para conseguir la serie de composición, lo que haremos será considerar la descomposición de $G$ en suma de grupos cíclicos y en cada paso, iremos quitando un grupo cíclico:

$$\begin{aligned} G_1 &= (C_{p_1^{\alpha_{12}}} \oplus \dots \oplus C_{p_1^{\alpha_{1n_1}}}) \oplus \dots \oplus (C_{p_r^{\alpha_{r1}}} \oplus \dots \oplus C_{p_r^{\alpha_{rn_1}}}) \\ G_2 &= (C_{p_1^{\alpha_{13}}} \oplus \dots \oplus C_{p_1^{\alpha_{1n_1}}}) \oplus \dots \oplus (C_{p_r^{\alpha_{r1}}} \oplus \dots \oplus C_{p_r^{\alpha_{rn_1}}}) \\ &\vdots \\ G_{n_1} &= (C_{p_2^{\alpha_{21}}} \oplus \dots \oplus C_{p_2^{\alpha_{2n_2}}}) \oplus \dots \oplus (C_{p_r^{\alpha_{r1}}} \oplus \dots \oplus C_{p_r^{\alpha_{rn_1}}}) \\ &\vdots \end{aligned}$$

**Ejemplo.** Sea $A$ un grupo con $|A| = 40 = 2^3 \cdot 5$:

| Descomposición | Descomp. cíclica primaria | Factores invariantes | Descomp. cíclica |
|---|---|---|---|
| $2^3, 5$ | $C_8 \oplus C_5$ | $40$ | $C_{40}$ |
| $2, 2^2, 5$ | $C_2 \oplus C_4 \oplus C_5$ | $2, 20$ | $C_2 \oplus C_{20}$ |
| $2, 2, 2, 5$ | $C_2 \oplus C_2 \oplus C_2 \oplus C_5$ | $2, 2, 10$ | $C_2 \oplus C_2 \oplus C_{10}$ |

Como $l(A) = 4$ por el ejercicio anterior, series de composición serán:

$$C_{40} \rhd C_{20} \rhd C_{10} \rhd C_5 \rhd \{1\}$$
$$C_{40} \rhd C_8 \rhd C_4 \rhd C_2 \rhd \{1\}$$

Los factores de composición de la primera son:

$$C_{40}/C_{20} \cong C_2 \qquad C_{20}/C_{10} \cong C_2 \qquad C_{10}/C_5 \cong C_2 \qquad C_5/\{1\} \cong C_5$$

**Ejemplo.** Sea:

$$G = \langle a, b, c \mid \begin{matrix} 2a - 6b + 18c = 0 \\ 6a + 6c = 0 \end{matrix} \rangle$$

Y sea:

$$H = \mathbb{Z}^3/\langle (1, -9, 3), (1, -7, 1), (1, -1, 1) \rangle$$

Tenemos la matriz:

$$\begin{pmatrix} 2 & -6 & 18 \\ 6 & 0 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & -6 & 18 \\ 0 & 18 & -48 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 18 & 48 \end{pmatrix} \longrightarrow$$
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 18 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix} \longrightarrow$$

Por lo que $G$ tiene rango 1 y sus descommposiciones cíclica y cíclica primaria son:

$$G \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

Con $H$ tenemos lo mismo:

$$\begin{pmatrix} 1 & 1 & 1 \\ -9 & -7 & -1 \\ 3 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ -9 & 2 & 8 \\ 3 & -2 & -2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 8 \\ 0 & -2 & -2 \end{pmatrix} \longrightarrow$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 8 \\ 0 & 0 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

Por lo que:

$$H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$$

y $H$ no tiene parte libre. Tendremos:

$$l(H) = 3$$

Los factores de composición serán $\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3$.

$$G \ncong H$$
$$T(G) \cong T(H) = H$$

¿Cuáles son los elementos de orden 6 de $H$? Tiene al menos:

$$O(a,1) = O(a,5) = 6 \qquad \forall a \in \mathbb{Z}_2$$

También tendremos:

$$O(1,2) = \text{mcm}(O(1), O(2)) = \text{mcm}(2,3) = 6$$

¿$G$ tiene elementos de orden 6? Sí, los mismos pero con un 0 en primera coordenada.

# 3. 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 oden 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.

## 3.1. 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 **??** 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 epimorfimo, 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 $Q_2^{\text{abs}}$ en su partición de clases:

$$Q_2^{\text{abs}} \cong H \cup yH$$

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 $Q_2^{\text{abs}}$ en el Capítulo **??** fue para ahora generalizar lo que hacíamos con $Q_2$ a todo grupo, con el producto semidirecto.

**Definición 3.1** (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 $k = 2$, obtenemos $Q_2^{\text{abs}}$:

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

- Para $k \geqslant 3$, tendremos que tiene un cociente isomorfo a $D_k$, por lo que no será abeliano. Sin embargo, podemos acotar el orden de $Q_k$:

$$2k \leqslant |Q_k| \leqslant 4k \qquad \forall k \geqslant 3$$

Y si $k$ es impar, tendremos que $|Q_k| = 4k$.

*Demostración.* Si recordamos al grupo diédrico de orden $k$:

$$D_k = \langle r, s \mid r^k = s^2 = 1, sr = r^{-1}s \rangle$$

Tenemos que $r^{2k} = (r^k)^2 = 1$ y tenemos la primera relación. Para la segunda, tenemos que $s^2 = 1 = r^k$. Finalmente, $sr = r^{-1}s$ nos da la tercera (compruébese). Podemos aplicar el Teorema de Dyck, que nos da un homomorfismo $f : Q_k \to D_k$ de forma que:

$$f(x) = r \qquad f(y) = s$$

Además, sabemos que $f$ es un epimorfimo, ya que $D_k = \langle r, s \rangle$. Por el Primer Teorema de Isomorfía aplicado a $f$, podemos asegurar que:

$$Q_k / \ker(f) \cong D_k$$

Por tanto, el dicíclico de orden $k$ no será abeliano.

$\geqslant$) Sabemos que $|D_k| = 2k$, y por el epimorfismo anterior, sabemos que $2k$ divide a $|Q_k|$, de donde $2k \leqslant Q_k$.

$\leqslant$) Usando que $x^{2k} = 1$, si tomamos $H = \langle x \rangle$, tenemos que:

$$|H| = |\langle x \rangle| \leqslant 2k$$

Como también tenemos que:

$$yxy^{-1} = x^{-1} \in H$$

Tendremos que $H \lhd Q_k$, de donde al considerar el cociente, tendremos al igual que antes que:

$$Q_k / H \cong \langle yH \rangle$$

De esta forma:

$$(yH)^2 = y^2 H = x^k H = H$$

Por lo que $y^2 \notin yH$ y:

$$|Q_k / H| \leqslant 2$$

De donde deduimos que:

$$|Q_k| = |Q_k / H||H| \leqslant 4k$$

Suponiendo ahora que $k = 2t + 1$ para cierto $t \in \mathbb{N}$, consideramos el cíclico de orden 4:

$$C_4 = \langle a \mid a^4 = 1 \rangle$$

1. Tenemos que:
$$(a^2)^{2k} = (a^4)^k = 1$$
2. Además:
$$(a^2)^k = a^{2k} = a^{4t+2} = a^2$$
3. Finalmente:
$$aa^2 = a^3 = a^2a = (a^2)^{-1}a$$

Por el Teorema de Dyck, podemos construir el homomorfismo $f : Q_k \to C_4$ dado por:
$$f(x) = a^2 \qquad f(y) = a$$
Que de hecho es un epimorfismo, ya que $C_4 = \langle a \rangle$. Al igual que antes:
$$Q_k/\ker(f) \cong C_4$$
De donde llegamos a que 4 divide a $|Q_k|$. Como además $2k$ divide a $|Q_k|$, tenemos que $\text{mcm}(2k, 4)$ divide a $|Q_k|$ y, como $k$ era impar, tendremos que:
$$\text{mcm}(2k, 4) = 4$$
De donde $4k \leqslant |Q_k|$, que con la desigualdad anterior nos da la igualdad. □

**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, salvo isomorfismo.

**Definición 3.2** (Producto semidirecto)**.** Dados dos grupos, $K$, $H$ y una acción $\theta : H \to Aut(K)$, consideramos el conjunto producto cartesiano:
$$G = K \times H = \{(k, h) \mid k \in K, h \in H\}$$
Sobre el que definimos la siguiente operación:
$$(k_1, h_1)(k_2, h_2) = ({k_1}^{h_1}k_2, h_1h_2)$$
Se verifica que $K \times H$ con esta operación tiene estructura de grupo, al que llamaremos **producto semidirecto de $K$ por $H$ relativo a $\theta$**, que denotaremos por:
$$K \rtimes_\theta H$$

**Teorema 3.1.** *Se verifica que $K \times H$ con esta operación tiene estructura de grupo*

*Demostración.* Veamos:

- El elemento $(1,1)$ es el neutro:

$$(k,h)(1,1) = (k\,{}^{h}1, h) = (k,h)$$
$$(1,1)(k,h) = (1,\,{}^{1}k, h) = (k,h)$$
$$\forall (k,h) \in K \times H$$

- Para el inverso, dado $(k,h) \in K \times H$, el inverso será:

$$(k,h)^{-1} = ({}^{h^{-1}}k^{-1}, h^{-1})$$

$$(k,h)\left({}^{h^{-1}}k^{-1}, h^{-1}\right) = \left(k\,{}^{h}\left({}^{h^{-1}}k^{-1}\right), hh^{-1}\right) = \left(k\,{}^{hh^{-1}}k^{-1}, 1\right) = (kk^{-1}, 1) = (1,1)$$

□

**Ejemplo.** Veamos:

- Si $\theta = 1$, tenemos que el producto semidirecto coincide con el producto directo:

$$\theta(1)(h) = {}^{1}h = h \qquad \forall h \in H$$

De donde:

$$(k_1,h_1)(k_2,h_2) = (k_1\,{}^{h_1}k_2, h_1h_2) = (k_1k_2, h_1h_2) \qquad \forall (k_1,h_1),(k_2,h_2) \in K \times H$$

- 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. Será:

$$\theta(y)(x) = x^{-1} \qquad \forall y \in C_2, \forall x \in C_3$$

Ya que $Aut(C_3) \cong C_2 = \{1, x\}$. Los elementos serán:

$$C_3 \rtimes_\theta C_2 = \langle x, y \mid x^3 = 1, y^2 = 1, algo \rangle$$

Con $|C_3 \rtimes_\theta C_2| = 6$. Los grupos que conocemos de orden 6 son $S_3$ y $C_6$, que podemos distinguir en función de si el grupo es abeliano o no. Veamos que no lo es:

$$(x,y^2)(1,y) = (x^2\,{}^{y}1, y^2) = (x^2, 1)$$
$$(1,y)(x^2,y) = (1\,{}^{y}x^2, y^2) = (x,1)$$

Como $x \neq x^2$, no es conmutativo, por lo que $C_3 \rtimes_\theta C_2 \cong D_3$. Por tanto, completamos la presentación pensando en la de $D_3$:

$$C_3 \rtimes_\theta C_2 = \langle x, y \mid x^3 = 1, y^2 = 1, xy = yx^{-1} \rangle$$

En definitiva, el único producto semidirecto de dos grupos de orden 6 es $S_3$.

- 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 $n \geqslant 3$, 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 $C_n \rtimes_\theta C_2 \cong D_n$.

**Definición 3.3.** En el producto semidirecto, definimos:

$$\begin{array}{ccccc} K & \xrightarrow{\lambda_1} & K \rtimes H & \xleftarrow{\lambda_2} & H \\ & & \downarrow \pi & & \\ & & H & & \end{array}$$

Por:

$$\begin{aligned} \lambda_1(k) &= (k, 1) \\ \lambda_2(h) &= (1, h) \\ \pi(k, h) &= h \end{aligned}$$

**Proposición 3.2.** *Se verifica que:*

1. $\lambda_1, \lambda_2, \pi$ *son homomorfismos de grupos.*
2. $\pi\lambda_1$ *es trivial.*
3. $\pi\lambda_2 = id_H$.

De forma análoga a la propiedad universal del producto directo, podemos tener la propiedad universal para el producto semidirecto.
La siguiente Proposición nos será de utilidad para clasificar grupos haciéndolos isomorfoso a un producto semidirecto, a partir del orden.

**Teorema 3.3.** *Sea $G$ un grupo y $K, H < G$ con $K \lhd G$, $KH = G$ y $K \cap H = \{1\}$, sea $\theta : H \to Aut(K)$ un homomorfismo que nos da la acción $ac : H \times K \to K$ por conjugación*[1]*:*

$$\theta(h)(k) = hkh^{-1} \qquad \forall h \in H, \forall k \in K$$

*Entonces, $K \rtimes_\theta H \cong G$.*

[1]La condición $K \lhd G$ nos dice que $\theta$ está bien definida

*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 ciertos $k \in K$, $h \in H$.
- 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 3.4.** Si $G$ verifica las condiciones de la Proposición anterior, decimos que $G$ es producto semidirecto interno de $K$ y $H$.

**Definición 3.5** (Complemento de un subgrupo)**.** Si $K < G$, un subgrupo $H < G$ se llama complemento para $K$ en $G$ si $G = KH$ con $K \cap H = \{1\}$.

*Observación.* Con esta última definición, tendremos que $G$ será un producto semidirecto interno de dos subgrupos propios si y solo si algún subgrupo normal propio tiene un complemento.

**Ejemplo.** Esto último no siempre será posible. Por ejemplo, si $G$ es simple, no tendrá subgrupos normales propios, por lo que no será producto semidirecto interno de dos subgrupos.

Si $G$ es un grupo que sí tiene subgrupos normales propios, tampoco somos capaces siempre de poner como un producto semidirecto. Por ejemplo, $Q_2$ no es un producto semidirecto interno de subgrupos propios. Si recordamos su diagrama de Hasse:

$$\begin{aligned} \langle i \rangle \cap \langle j \rangle &= \{1, -1\} \\ \langle i \rangle \cap \langle k \rangle &= \{1, -1\} \\ \langle j \rangle \cap \langle k \rangle &= \{1, -1\} \end{aligned}$$

Dado un subgrupo normal, no seremos capaces de complementarlo con otro.

**Ejemplo.** Para cualquier grupo $K$, si tomamos $H = Aut(K)$ y $\theta = 1_{Aut(K)}$, si tomamos:

$$K \rtimes_\theta Aut(K) = Hol(K)$$

Al que llamaremos grupo holomorfo de $K$.

Por ejemplo:

$$Hol(\mathbb{Z}_2 \times \mathbb{Z}_2) = S_4$$

**Ejemplo.** Como ejemplos de aplicaciones inmediantas del último Teorema, tenemos:

- 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:

  $$A_4 \cong V \rtimes H$$

### 3.1.1. Grupos de orden $pq$

Veamos ahora cómo son los grupos $G$ con $|G| = pq$ con $p < q$ y $p, q$ primos. En dicho caso, tendremos:

- $P \in Syl_p(G)$
- $Q \in Syl_q(G)$

$$\left.\begin{array}{rr} n_q \mid p \\ n_q \equiv 1 \mod p \end{array}\right\} \Longrightarrow n_q \in \{1, p\}$$

Pero como $p < q$, no puede ser $n_q = p$, ya que entonces $p \equiv 1 \mod q$. De esta forma, sabemos que $Q$ es el único $q-$subgrupo de $G$, por lo que $Q \lhd G$. De esta forma, tenemos que:

$$Q \cap P = \{1\} \qquad QP = G$$

Por tanto, 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 $P \cong C_p$. En definitiva, tenemos que $n_q = 1$. Ahora:

$$\left.\begin{array}{rr} n_p \mid q \\ n_p \equiv 1 \mod p \end{array}\right\} \Longrightarrow n_p \in \{1, q\}$$

- Si $n_q = 1 = n_p$, entonces tendremos que $P, Q \lhd G$, por lo que:

$$G \cong Q \rtimes P \cong Q \times P \cong C_q \times C_p \cong C$$

- Si $n_q = 1$ y $n_p = q$, entonces $p \mid q-1$. Si buscamos una accion:

$$C_p \to Aut(C_q) \cong U(C_q) \cong C_{q-1}$$

Como $p \mid q-1$, sabemos que existe un único subgrupo cíclico $\langle \alpha \rangle \subseteq Aut(C_q)$ de orden $p$.

Una acción $\theta : C_p \to Aut(C_q)$ vendrá dado por:

$$\theta(y) = \alpha^j$$

Podemos definir $\theta_i$ que a cada $y_i \longmapsto \alpha^i$, para $i \in \{0, \dots, p-1\}$. Para $i = 0$:

$$\theta_0(y_0) = 1$$

Luego tenemos $G \cong C_{pq}$. Para el resto de los casos, como son todas isomorfas, tomamos $\theta(y_i) = \alpha$.

En conclusión:

$$G \cong C_q \rtimes C_p \cong \langle x, y \mid x^q = 1, y^p = 1, yxy^{-1} = \alpha(x) \rangle$$

Con lo que así se describen todos los grupos $G$ no abelianos de orden $pq$.

**Ejemplo.** En el caso $p = 2$, para $C_{2q}$:

$$C_q \rtimes C_2 = \langle x, y \mid x^q = 1, y^2 = 1, yxy^{-1} = \alpha(x) \rangle$$

Pero:

$$\alpha \in Aut(C_q) \qquad O(\alpha) = 2$$

Y morfismos de $C_q$ en $C_q$ de orden 2 solo hay uno:

$$x \longmapsto x^{-1}$$

Por tanto:

$$C_q \rtimes C_2 = \langle x, y \mid x^q = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle = D_q$$

Por lo que grupos $G$ con $|G| = 2q$ tenemos que $G$ es abeliano o que es $D_q$.

Repasando lo que sabemos clasificar:

$$\begin{aligned} |G| = 6 &\longmapsto C_6, & D_3 \cong S_3 \\ |G| = 10 &\longmapsto C_{10}, & D_5 \\ |G| = 14 &\longmapsto C_{14}, & D_7 \\ |G| = 15 &\longmapsto C_{15}, ? \end{aligned}$$

Vamos a ver el caso que $|G| = 15$, con lo que tenemos haciendo cuentas que $n_3 = 1 = n_5$, por lo que concluimos que grupos de orden 15 solo tenemos $C_{15}$. Este razonamiento puede seguirser para $|G| = n$ para $n \geqslant 15$, si el lector desea hacerlo.

### 3.1.2. Grupos de orden 12

Sea $G$ un grupo de orden $|G| = 12 = 2^2 \cdot 3$.

Sabemos que grupos abelianos de orden 12 tenemos:

$$C_2 \times C_2 \times C_3 \cong C_2 \times C_6 \qquad C_4 \times C_3 \cong C_{12}$$

Supuesto que $G$ no es abeliano:

$$\left.\begin{array}{rr} & n_2 \mid 3 \\ n_2 \equiv 1 & \text{mód } 2 \end{array}\right\} \Longrightarrow n_2 \in \{1, 3\}$$
$$\left.\begin{array}{rr} & n_3 \mid 4 \\ n_3 \equiv 1 & \text{mód } 4 \end{array}\right\} \Longrightarrow n_3 \in \{1, 4\}$$

- Supongamos que $n_4 = 3$ 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 sacamos 8 elementos distintos de orden 3 y 9 elementos de orden 2 o 4, con lo que este caso es imposible.

- Si $n_2 = 1$ o $n_3 = 1$, tendremos en cualquier caso de la existencia de un $p-$subgrupo de Sylow ($p \in \{2, 3\}$) $K \lhd G$. Si consideramos su complemento, $H < G$, tendremos que:

  $$G \cong K \rtimes_\theta H$$

  Si suponemos que $K \in Syl_3(G)$ y $H \in Syl_2(G)$ (en otro caso es análogo), tendremos entonces que $K \cong C_3$ y $|H| = 4$, por lo que $H \cong C_4$ o $H \cong C_2 \times C_2$

- 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 $H = C_2 \times C_2$ y el segundo si $H = C_4$, por lo que volvemos al caso abeliano.

- Si $n_3 = 1$ y $n_2 = 3$, tenemos entonces que:

  $$G \cong K \rtimes H \cong \left\{ \begin{array}{l} C_3 \rtimes C_4 \\ C_3 \rtimes C_2 \times C_2 \end{array} \right.$$

  Y vendrá por una acción:

  $$\theta : C_4 \to Aut(C_3)$$
  $$\theta : C_2 \times C_2 \to Aut(C_3)$$

  Alguno de ellos. sin embargo, como $Aut(C_3) \cong C_2 = \{1, x^{-1}\}$

- En $C_3 \rtimes C_4$ para la acción ${}^x y = x^{-1}$, tenemos que:

  $$C_3 \rtimes C_4 = \langle x, y \mid x^3 = 1, y^4 = 1, yxy^{-1} = x^{-1} \rangle$$

- En $C_3 \rtimes (C_2 \times C_2)$, los automorfismos de la forma:

$$C_2 \times C_2 \to Aut(C_3)$$

Solo tenemos uno no trivial, que es ($y, x$ son los generadores):

$$\begin{aligned} &\theta : C_2 \times C_2 \to Aut(C_3) \\ &y \longmapsto \alpha \\ &x \longmapsto 1 \end{aligned}$$

Tendremos que:

$C_3 \rtimes_\theta (C_2 \times C_2) = \langle x, y, z \mid x^3 = 1, y^2 = z^2 = 1, yxy^{-1} = x^{-1}, zxz^{-1} = x, yzy^{-1} = zy \rangle$

Que es isomorfo a $D_6 \cong D_3 \times C_2$, tomando $r = xy$ y $s = yz$

- 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:

$$\begin{aligned} &\phi : G \to Perm(Syl_3(G)) \cong S_4 \\ &G/\ker(\phi) \cong G \cong Im(\phi) \subseteq S_4 \end{aligned}$$

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.

$$\begin{aligned} &\theta_1 : x \longmapsto \alpha \\ &\alpha \begin{cases} y \longmapsto z \\ z \longmapsto yz \end{cases} \end{aligned}$$

$$\begin{aligned} &\theta_2 : x \longmapsto \alpha^2 \\ &\alpha^2 \begin{cases} y \longmapsto yz \\ z \longmapsto y \end{cases} \end{aligned}$$

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.

### 3.1.3. 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. Los grupos abelianos son:

$$C_2 \times C_2 \times C_2 \qquad C_2 \times C_4 \qquad C_8$$

**No abelianos**

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, 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 podemos emplear también este mismo tipo de razonamiento.