Álgebra II

Foto: José Juan Castro

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra II

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán
Arturo Olivares Martos

Granada, 2025

Índice general

1. Grupos cocientes y Teoremas de isomorfía

Este tema se centrará en las relaciones de equivalencia ${}_H\sim$ y $\sim_H$ definidas en el capítulo anterior, donde ya vimos propiedades de estas relaciones (recordamos la Proposición **??**), como que $G/{}_H\sim$ y $G/\sim_H$ eran biyectivos o el Teorema de Lagrange. Estaremos especialmente interesados en el caso en el que los conjuntos cocientes de estas dos relaciones de equivalencia coincidan, propiedad que nos dará los Teoremas de Isomorfía, que son el principal objeto de estudio de este tema.

1.1. Subgrupos normales

Definición 1.1 (Subgrupos normales)**.** Sea G un grupo y $H < G$, diremos que H es un subgrupo normal de G, denotado por $H \lhd G$, si las clases laterales de cada elemento coinciden, es decir, si:

$$xH = Hx \qquad \forall x \in G$$

En cuyo caso, tendremos que $G/{}_H\sim \ = G/\sim_H$, y notaremos a este conjunto como G/H, al que llamaremos conjunto de las clases laterales de H en G.

Definición 1.2 (Conjugado)**.** Sea G un grupo, $H \subseteq G$ y $x \in G$, definimos el conjugado de H por x como el conjunto:

$$xHx^{-1} = \{xhx^{-1} \mid h \in H\}$$

Proposición 1.1. *Sea G un grupo, $H < G$ y $x \in G$, entonces $xHx^{-1} < G$.*

Demostración. Para ello, sean $xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1}$, entonces:

$$xh_1x^{-1}(xh_2x^{-1})^{-1} = xh_1x^{-1}xh_2^{-1}x^{-1} = xh_1h_2^{-1}x^{-1} \in xHx^{-1}$$

Ya que como H es un subgrupo de G, entonces $h_1h_2^{-1} \in H$. □

Buscamos ahora formas cómodas de detectar cuándo un subgrupo de un grupo es normal o no, ya que es tedioso comprobar la igualdad $xH = Hx$ para todo elemento x del grupo que estemos considerando en cada caso.

Proposición 1.2 (Caracterización de subgrupos normales)**.**
Sea G un grupo y $H < G$, son equivalentes:

i) $H \lhd G$.

ii) $xhx^{-1} \in H \ \forall x \in G, \forall h \in H$.

iii) $xHx^{-1} \subseteq H \ \forall x \in G$.

iv) $xHx^{-1} = H \ \forall x \in G$.

Demostración. Veamos todas las implicaciones:

$i) \Longrightarrow ii)$ Sean $x \in G$ y $h \in H$, entonces $xh \in xH = Hx$ por ser $H \lhd G$, lo que nos dice que $\exists h' \in H$ de forma que $xh = h'x$ y multiplicando por x^{-1} a la derecha, llegamos a que:

$$xhx^{-1} = h' \in H$$

$ii) \Longleftrightarrow iii)$ Es claro.

$iii) \Longrightarrow iv)$ Sea $h \in H$ y dado $x \in G$, en particular tendremos que $x^{-1} \in G$, por lo que usando la hipótesis, tenemos que $x^{-1}hx \in x^{-1}Hx \subseteq H$, por lo que $x^{-1}hx \in H$ y tendremos que:

$$xx^{-1}hxx^{-1} = h \in xHx^{-1}$$

$iv) \Longrightarrow i)$ Fijado $x \in G$, veamos que $xH = Hx$:

$\subseteq)$ Si $xh \in xH$, entonces tendremos que:

$$xhx^{-1} \in xHx^{-1} = H$$

Con lo que existirá $h' \in H$ de forma que $xhx^{-1} = h'$. Si multilicamos por x a la derecha, obtenemos que:

$$xh = h'x \in Hx$$

$\supseteq)$ Para la otra inclusión, si $hx \in Hx$, tendremos que:

$$x^{-1}hx \in x^{-1}Hx = H$$

Por lo que existirá $h' \in H$ de forma que $x^{-1}hx = h'$. Si multiplicamos por x a la izquierda:

$$hx = xh' \in xH$$

□

Comprobar que $xhx^{-1} \in H$ para todo $x \in G$ y para todo $h \in H$ puede ser una labor tediosa, por lo que presentamos la siguiente Proposición, que puede resultar de utilidad a la hora de comprobar si un subgrupo H de un grupo G es normal o no.

Proposición 1.3. *Sea G un grupo, $H < G$ y $S \subseteq G$ de forma que $G = \langle S \rangle$, entonces:*

$$xhx^{-1} \in H \quad \forall x \in G, \forall h \in H \Longleftrightarrow shs^{-1} \in H \quad \forall s \in S \cup S^{-1}, \forall h \in H$$

Donde $S^{-1} = \{x \in G \mid x^{-1} \in S\}$. Es decir, basta comprobar la condición con los generadores de G y con los inversos de los generadores de G.

Demostración. Veamos las dos implicaciones:

$\Longrightarrow$) En particular, tenemos que $x \in S \cup S^{-1} \subseteq G$.

$\Longleftarrow$) Sea $x \in G = \langle S \rangle$, entonces existirán $s_1, \ldots, s_n \in S$ y $\gamma_1, \ldots, \gamma_n \in \{\pm 1\}$ de forma que:

$$x = s_1^{\gamma_1} \ldots s_n^{\gamma_n}$$

Por inducción sobre n:

- Si $n = 1$: Entonces $x = s^\gamma$ con $s \in S$ y $\gamma \in \{\pm 1\}$. Distinguimos casos:
  - Si $\gamma = 1$, entonces:
  $$xhx^{-1} = shs^{-1} \in H \qquad \forall h \in H$$
  - Si $\gamma = -1$, entonces:
  $$xhx^{-1} = s^{-1}hs \in H \qquad \forall h \in H$$
- Supuesto para $m < n$, veámoslo para n:
  $$xhx^{-1} = s_1^{\gamma_1} s_2^{\gamma_2} \ldots s_n^{\gamma_n} h s_n^{-\gamma_n} \ldots s_2^{-\gamma_2} s_1^{-\gamma_1}$$
  Si cogemos $y = s_2^{\gamma_2} \ldots s_n^{\gamma_n}$, por hipótesis de inducción tendremos que:
  $$yhy^{-1} = s_2^{\gamma_2} \ldots s_n^{\gamma_n} h s_n^{-\gamma_n} \ldots s_2^{-\gamma_2} \in H$$
  Por lo que:
  $$xhx^{-1} = s_1^{\gamma_1} yhy^{-1} s_1^{-\gamma_1} \in H$$

□

Ejemplo. Hemos caracterizado ya a los grupos normales, pero veamos ejemplos de ellos:

1. Dado un grupo G, los dos subgrupos impropios de G siempre son subgrupos normales del mismo:
   - Para el caso $H = \{e\}$:
   $$xex^{-1} = xx^{-1} = e \in \{e\} \qquad \forall x \in G$$
   Y por la Proposición anterior, tenemos que $\{e\} \lhd G$.
   - Para el caso $H = G$:
   $$xhx^{-1} \in G \qquad \forall x \in G, \forall h \in G$$
   Y por la misma razón, también tenemos que $G \lhd G$.
2. En un grupo abeliano G, todos sus subgrupos son normales (sea $H < G$):
$$xH = \{xh \mid h \in H\} = \{hx \mid h \in H\} = Hx \qquad \forall x \in G$$

3. Todo subgrupo de índice 2 es normal, es decir, si $H < G$ con $[G : H] = 2$, entonces $H \lhd G$.

   Para verlo, si tomamos $x \in G \setminus H$, como $[G : H] = 2$, tenemos que:

   $$H \cup xH = G = H \cup Hx$$

   En ambos casos, como son particiones disjuntas, tenemos que $xH = Hx$ para todo $x \in G \setminus H$ (y si $x \in H$, entonces $xH = H = Hx$), con lo que $H \lhd G$.

4. En S_3, si consideramos $H = \langle (1\ 2) \rangle$, H no es un subgrupo normal de S_3, como se vio en el correspondiente ejemplo del tema anterior, y podemos volverlo a comprobar con la caracterización, ya que $(2\ 3) \in S_3$ y:

   $$(2\ 3)(1\ 2)(2\ 3)^{-1} = (1\ 3) \notin H$$

   Igual les pasa a los subgrupos $\langle (2\ 3) \rangle$ y $\langle (1\ 3) \rangle$. Sea ahora $A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$, como $[S_3 : A_3] = 2$, tenemos que $A_3 \lhd S_3$:

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

5. La relación de "ser un subgrupo normal de" no es transitiva, es decir, si G es un grupo con $K < H < G$, $K \lhd H$ y $H \lhd G$, entonces no necesariamente se tiene que $K \lhd G$. La situación es la descrita en la Figura 1.1

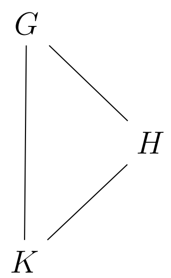
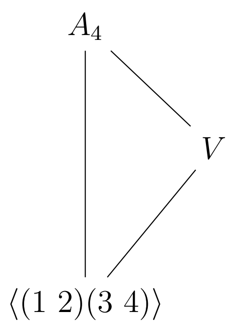
   

   Figura 1.1: Situación descrita.

   Por ejemplo, en A_4 consideramos el grupo de Klein V y $\langle (1\ 2)(3\ 4) \rangle$. Vamos a ver que $\langle (1\ 2)(3\ 4) \rangle \lhd V$ y que $V \lhd A_4$ pero no se cumple que $\langle (1\ 2)(3\ 4) \rangle \lhd A_4$:

   - En primer lugar, $\langle (1\ 2)(3\ 4) \rangle \lhd V$, por ser $[V : \langle (1\ 2)(3\ 4) \rangle] = 2$.

- Veamos ahora que $V \lhd A_4$. Para ello, consideramos:

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

Por la Proposición 1.3, basta comprobar la caracterización para todos los generadores de $A_4 = \langle (1\ 2\ 3), (1\ 2\ 4) \rangle$:

$$\begin{aligned}
&(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} \in V \\
&(1\ 2\ 3)(1\ 3)(2\ 4)(1\ 2\ 3)^{-1} \in V \\
&(1\ 2\ 3)(1\ 4)(2\ 3)(1\ 2\ 3)^{-1} \in V \\
&(1\ 2\ 3)1(1\ 2\ 3)^{-1} \in V \\
&(1\ 2\ 4)(1\ 2)(3\ 4)(1\ 2\ 4)^{-1} \in V \\
&(1\ 2\ 4)(1\ 3)(2\ 4)(1\ 2\ 4)^{-1} \in V \\
&(1\ 2\ 4)(1\ 4)(2\ 3)(1\ 2\ 4)^{-1} \in V \\
&(1\ 2\ 4)1(1\ 2\ 4)^{-1} \in V
\end{aligned}$$

- Veremos ahora que no se tiene que $\langle (1\ 2)(3\ 4) \rangle \lhd A_4$, ya que:

$$(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} = (1\ 4)(2\ 3) \notin A_4$$

Hemos visto ya que la relación $\lhd$ no es en general transitiva. Sin embargo, de ella podemos deducir ciertas relaciones, como se pone de manifiesto en este Corolario:

Corolario 1.3.1. *Como corolario de la Proposición 1.2, si G es un grupo de forma que $A \subseteq B \subseteq G$ con $A \lhd G$ y $B < G$, entonces $A \lhd B$.*

Demostración. Por la Proposición 1.2, tendremos que $xax^{-1} \in A$ para todo $x \in G$ y $a \in A$. Sea $b \in B$, como en particular $b \in G$, también se cumplirá:

$$bab^{-1} \in A \qquad \forall b \in B, a \in A$$

Concluimos que $A \lhd B$. □

Definición 1.3 (Centro)**.** Sea G un grupo, definimos el centro de G como el conjunto de los elementos de G que conmutan con todos los demás, es decir, el conjunto:

$$Z(G) = \{a \in G \mid ax = xa, \forall x \in G\}$$

Podemos entender $Z(G)$ como "la parte abeliana del grupo" G.

Proposición 1.4. *Sea G un grupo, se verifica:*

i) $Z(G) < G$.

ii) $Z(G) \lhd G$.

iii) *Si G es abeliano, entonces* $Z(G) = G$.

Demostración. Demostramos las propiedades:

i) Sean $a, b \in Z(G)$ y dado $x \in G$, entonces:

$$(ab^{-1})x = a(b^{-1}x) = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} = a(xb^{-1}) = (ax)b = (xa)b = x(ab^{-1})$$

Por lo que $ab^{-1} \in Z(G)$, lo que nos dice que $Z(G)$ es un subgrupo de G.

ii) Sea $x \in G$, entonces:

$$xZ(G) = \{xz \mid z \in Z(G)\} = \{zx \mid z \in Z(G)\} = Z(G)x$$

iii) Es evidente.

□

Ejemplo. Ejemplos interesantes:

- Veamos que $Z(S_n) = 1$ cuando $n \geqslant 3$. Para ello, supongamos que $n \geqslant 3$ y consideremos $1 \neq \sigma \in S_n$, con lo que existirán $i, j \in \{1, \ldots, n\}$ con $i \neq j$ de forma que $\sigma(i) = j$.

  En dicho caso, $\exists k \in \{1, \ldots, n\} \setminus \{i, j\}$ ($n \geqslant 3$). Si consideramos $\tau = (j\ k)$:

  $$\left.\begin{array}{r} \sigma\tau(i) = \sigma(i) = j \\ \tau\sigma(i) = \tau(j) = k \end{array}\right\} \Longrightarrow \sigma\tau \neq \tau\sigma$$

  Por tanto, $\sigma \notin Z(S_n)$, para todo $\sigma \in S_n \setminus \{1\}$.

- Veamos que que $Z(A_n) = 1$ cuando $n \geqslant 4$. Para $n \geqslant 4$, $\exists i, j \in \{1, \ldots, n\}$ con $i \neq j$ de forma que $\sigma(i) = j$, con lo que podemos encontrar $k, l \in \{1, \ldots, n\}$, distintos entre sí y distintos de i y j. Consideramos:

  $$\tau = (j\ k\ l) \in A_4$$

  Y tenemos de la misma forma que:

  $$\left.\begin{array}{r} \sigma\tau(i) = k \\ \tau\sigma(i) = j \end{array}\right\} \Longrightarrow Z(A_n) = \{1\}$$

Proposición 1.5. *Sea G un grupo, $H < G$, entonces, equivalen:*

i) $H \lhd G$.

ii) $\forall x, y \in G$ *con* $xy \in H$, *entonces* $yx \in H$

Demostración. Veamos las dos implicaciones:

i) $\Longrightarrow$ *ii)* Sean $x, y \in G$ con $xy \in H$, entonces $\exists h \in H$ de forma que $xy = h$, de donde $y = x^{-1}h \in x^{-1}H = Hx^{-1}$, por lo que $\exists h' \in H$ con $y = h'x^{-1}$ y multiplicando a la derecha por x, llegamos a que $yx = h' \in H$.

ii) $\Longrightarrow$ *i)* Sean $x \in G$ y $h \in H$, tenemos que:

$$h = x^{-1}(xh) \in H$$

De donde deducimos por hipótesis que $(xh)x^{-1} \in H$, lo que nos dice que $H \lhd G$. □

1.2. Grupo cociente

Mostraremos ahora la propiedad que más nos interesa de los grupos normales: dotan al conjunto cociente de estructura de grupo.

Teorema 1.6. *Sea G un grupo y $H \lhd G$, entonces en el conjunto G/H podemos definir una operación binaria $G/H \times G/H \longrightarrow G/H$ que dota a G/H de estructura de grupo, de modo que la proyección canónica $p : G \to G/H$ sea un homomorfismo de grupos. De esta forma, llamaremos a G/H grupo cociente.*

Demostración. Definimos la operación binaria $\cdot : G/H \times G/H \longrightarrow G/H$ dada por:

$$xH \cdot yH = xyH \qquad \forall xH, yH \in G/H$$

A esta operación la denotaremos a partir de ahora por yuxtaposición.

- En primer lugar, comprobemos que está bien definida, es decir, si $xH = x'H$ y $yH = y'H$, entonces $xyH = x'y'H$. Para ello:

$$\left.\begin{array}{l} xH = x'H \\ yH = y'H \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} \exists h_1, h_2 \in H \\ x' = xh_1 \\ y' = yh_2 \end{array}\right.$$

  Vemos ahora que dado $h \in H$:

  $\supseteq$)

  $$x'y'h = xh_1yh_2h \overset{(*)}{=} xyh_1'h_2h \in xyH$$

  Donde en $(*)$ hemos usado que $H \lhd G$, por lo que $Hy = yH$ y podemos encontrar un h_1' de forma que $h_1y = yh_1'$. Tenemos $x'y'H \subseteq xyH$.

  $\subseteq$)

  $$xyh = x'h_1^{-1}y'h_2^{-1}h \overset{(*)}{=} x'y'h_1''h_2^{-1}h \in x'y'H$$

  Donde en $(*)$ hemos usado una idea similar a la anterior, lo que nos da la otra inclusión.

- Que la operación es asociativa es claro, ya que la operación de G era asociativa.

- El elemento neutro de la operación es $1H = H$.

- Fijado un elemento $xH \in G/H$, tendremos que $(xH)^{-1} = x^{-1}H$.

Concluimos que G/H es un grupo.

Ahora, consideramos la proyección canónica $p : G \to G/H$, que viene definida por $p(x) = xH$ para todo $x \in G$. Gracias a la definición de la operación de G/H, tenemos que:

$$p(xy) = xyH = xHyH = p(x)p(y) \qquad \forall x, y \in G$$

Lo que demuestra que p es un homomorfismo de grupos. □

Notemos la importancia de considerar en el teorema anterior H como subgrupo normal de G, ya que es lo que nos ha permitido comprobar que la operación de G/H estaba bien definida. Como propiedades a destacar del grupo cociente G/H:

- Sabemos por el capítulo anterior que el orden del grupo G/H es (si G es finito):

$$|G/H| = [G : H] = \frac{|G|}{|H|}$$

- Además, si $p : G \to G/H$ es la proyección al cociente, tenemos que:

$$\ker(p) = \{x \in G \mid p(x) = H\} = \{x \in G \mid xH = H\} = \{x \in H\} = H$$

Ejemplo. Algunas consecuencias de que G/H sea un grupo:

1. En S_3, si consideramos $A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\} \lhd S_3$, tenemos que:

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

   Que por ser un grupo de orden 2, ya sabemos por el capítulo anterior que ha de ser $S_3/A_3 \cong \mathbb{Z}_2$.

2. Si consideramos $H < \mathbb{Z}$, entonces $H \lhd \mathbb{Z}$, ya que $\mathbb{Z}$ es abeliano. Además, sabemos que $\exists n \in \mathbb{Z}$ de forma que $H = n\mathbb{Z}$. De esta forma, tendremos que:

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$

   Por lo que el grupo cociente de $\mathbb{Z}$ bajo cualquier subgrupo normal suyo ya era conocido para nosotros, puesto que todos ellos son de la forma $\mathbb{Z}_n$, para cierto $n \in \mathbb{N}$.

3. Veamos otra vez que A_4 no tiene subgrupos de orden 6. Si $H < A_4$ con $|H| = 6$, entonces:

$$[A_4 : H] = \frac{A_4}{H} = 2$$

   Por tanto, $H \lhd A_4$. De esta forma, $A_4/H \cong \mathbb{Z}_2$, por ser el único grupo de orden 2. Si el cociente es isomorfo con $\mathbb{Z}_2$ y consideramos $xH \in A_4/H$, entonces:

$$(xH)^2 = x^2H = H \qquad \forall x \in A_4$$

   Por tanto, los cuadrados de los 8 $3-$ciclos de A_4 pertenecerían a H, de donde $|H| \geqslant 8$, <u>contradicción</u>.

Proposición 1.7. *Sea G un grupo y $H < G$, entonces: $H \lhd G$ si y solo si existe un homomorfismo de grupos $f : G \to G'$ de forma que* $\ker(f) = H$.

Demostración. Veamos las dos implicaciones:

$\Longrightarrow$) Si $H \lhd G$, entonces la proyección canónica $p : G \to G/H$ es un homomorfismo de grupos de forma que $\ker(p) = H$, gracias al Teorema 1.6.

$\Longleftarrow$) Supongamos ahora que existe un homomorfismo $f : G \to G'$ de grupos de forma que $\ker(f) = H$, sabemos ya que $H < G$ por ser $H = f^*(\{1\})$. Sean $x \in G$ y $h \in H$, tenemos que:

$$f(xhx^{-1}) = f(x)f(h)(f(x))^{-1} = f(x)(f(x))^{-1} = 1$$

De donde deducimos que $xhx^{-1} \in \ker(f) = H$, lo que nos dice que $H \lhd G$. □

Observación. De esta forma, dado un homomorfismo de grupos $f : G \to G'$, tendremos siempre que $\ker(f) \lhd G$, ya que por ser $\{1\} < G'$ un subgrupo, tendremos que $\ker(f) = f^*(\{1\}) < G$ y por la Proposición 1.7, automáticamente tenemos que $\ker(f) \lhd G$.

Teorema 1.8 (Propiedad universal del grupo cociente)**.** *Sea G un grupo, $H \lhd G$, $p : G \to G/H$ la proyección canónica al cociente, entonces para cualquier homomorfismo $f : G \to G'$ tal que $H \subseteq \ker(f)$, existe un único homomorfismo de grupos $\varphi : G/H \to G'$ de forma que $\varphi \circ p = f$.*

Más aún, tendremos que:

$$\begin{aligned} f \textit{ sobreyectiva} &\Longleftrightarrow \varphi \textit{ sobreyectiva} \\ H = \ker(f) &\Longleftrightarrow \varphi \textit{ inyectiva} \end{aligned}$$

La situación descrita podemos observarla en la Figura 1.2. Este resultado nos dice que el diagrama conmuta.

Demostración. Definimos $\varphi : G/H \to G'$ de la forma más natural posible:

$$\varphi(xH) = f(x) \qquad \forall xH \in G/H$$

- En primer lugar, veamos que está bien definida. Para ello, sean $x, y \in G$ de forma que $xH = yH$, entonces $y^{-1}x \in H \subseteq \ker(f)$, de donde:

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

- Veamos ahora que φ es un homomorfismo:

$$\varphi(xHyH) = \varphi(xyH) = f(xy) = f(x)f(y) = \varphi(xH)\varphi(xy) \qquad \forall x, y \in G$$

- Veamos que $\varphi \circ p = f$:

$$(\varphi \circ p)(x) = \varphi(p(x)) = \varphi(xH) = f(x) \qquad \forall x \in G$$

- Para la unicidad, supongamos que existe otra función $\psi : G/H \to G'$ de forma que $\psi \circ p = f$. En cuyo caso:

$$\psi(xH) = \psi(p(x)) = (\psi \circ p)(x) = f(x) = \varphi(xH) \qquad \forall xH \in G/H$$

  Por lo que $\psi = \varphi$.

Veamos la relación entre la sobreyectividad de f y φ:

$$f \text{ sobreyectiva} \Longleftrightarrow \varphi \text{ sobreyectiva}$$

$\Longleftarrow$) Como $f = \varphi \circ p$ y la composición de aplicaciones sobreyectivas es sobreyectiva, concluimos que f será sobreyectiva.

$\Longrightarrow$) Supongamos que f es sobreyectiva y sea $y \in G'$, por lo que $\exists x \in G$ de forma que $f(x) = y$, pero:

$$y = f(x) = \varphi(p(x)) = \varphi(xH)$$

Concluimos que φ es sobreyectiva.

Veamos ahora la relación de inyectividad:

$$H = \ker(f) \Longleftrightarrow \varphi \text{ inyectiva}$$

$\Longrightarrow$) Si $H = \ker(f)$ y $\varphi(xH) = 1$, entonces:

$$1 = \varphi(xH) = f(x) \Longrightarrow x \in \ker(f) = H$$

Con lo que $xH = H$, lo que nos dice que φ es inyectiva[1] ($\ker(\varphi) = \{H\}$).

$\Longleftarrow$) Vamos a ver que $\ker(f) \subseteq H$, ya que conocemos $H \subseteq \ker(f)$ por hipótesis. Para ello, sea $x \in \ker(f)$, entonces:

$$1 = f(x) = \varphi(p(x)) = \varphi(xH) \Longrightarrow xH \in \ker(\varphi)$$

Pero como φ es inyectiva, tenemos que $\ker(\varphi) = \{H\}$, con lo que $xH = H$, de donde $x \in H$.

□

La idea que subyace y que debemos entender de la propiedad universal del grupo cociente es la siguiente: G/H es la mejor forma de "colapsar H al elemento neutro sin perder las propiedades de grupo". Como ya vimos en el Teorema 1.6, en el que definimos al grupo cociente y donde vimos que la proyección canónica era un homomorfismo, resulta que en el grupo cociente, H es el elemento neutro de la operación, por lo que hemos conseguido colapsar H al elemento neutro.

Ahora, la propiedad universal del grupo cociente nos dice que si tenemos cualquier homomorfismo de grupos que "mata a H" (es decir, lo envía al núcleo del homomorfismo), entonces necesariamente ese homomorfismo ha de pasar por G/H, es decir, que existirá un único homomorfismo $\varphi : G/H \to G'$ que haga que el diagrama siguiente conmute. Cualquier homomorfismo que "mate a H" podremos factorizarlo pasando por el grupo cociente, luego este grupo ha de ser el que mejor colapsa a H.

$$\begin{tikzcd} G \arrow[r, "p"] \arrow[dr, "f"'] & G/H \arrow[d, dotted, "\varphi"] \\ & G' \end{tikzcd}$$

Figura 1.2: Situación del Teorema 1.8.

[1] Ya que H es el elemento neutro en G/H.

1.3. Teoremas de isomorfía

Teorema 1.9 (Primer Teorema de Isomorfía para grupos)**.** *Sea $f : G \to G'$ un homomorfismo de grupos, entonces existe un isomorfismo de grupos de forma que*

$$G/\ker(f) \cong Imf$$

Y vendrá definido por $x\ker(f) \longmapsto f(x)$.

Demostración. En primer lugar, por un resultado de la Proposición 1.7, tenemos que $\ker(f) \lhd G$. De esta forma, podemos considerar la proyección canónica al cociente $p : G \to G/\ker(f)$. Consideramos ahora la restriccion del codominio de f a su imagen, lo que nos da un epimorfismo. Por la propiedad universal del grupo cociente, tenemos que existe un único homomorfismo $\varphi : G/\ker(f) \to Im(f)$ que hace conmutar el siguiente diagrama:

$$\begin{tikzcd} G \arrow[r, "p"] \arrow[dr, "f"'] & G/\ker(f) \arrow[d, dotted, "\varphi"] \\ & Im(f) \end{tikzcd}$$

Finalmente, aplicando el Teorema 1.8:

- φ es sobreyectiva debido a que la restricción de f en codominio a su imagen es sobreyectiva.
- φ es inyectiva ya que el grupo normal que consideramos para hacer el cociente es $\ker(f)$. □

Ejemplo. Como consecuencia del primer teorema de isomorfía: consideramos $\mathbb{K}$, un cuerpo finito con $|\mathbb{K}| = q$ elementos. La aplicación $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$ es un homomorfismo de grupos y tenemos que:

$$\ker(\det) = \mathrm{SL}_n(\mathbb{K})$$

Con lo que $\mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K}) \cong Im(\det) = \mathbb{K}^*$. Usémoslo para calcular $|\mathrm{SL}_n(\mathbb{K})|$, ya que la isomorfía recién encontrada nos dice que:

$$|\mathbb{K}^*| = |\mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K})| = \frac{|\mathrm{GL}_n(\mathbb{K})|}{|\mathrm{SL}_n(\mathbb{K})|} \Longrightarrow |\mathrm{SL}_n(\mathbb{K})| = \frac{|\mathrm{GL}_n(\mathbb{K})|}{|\mathbb{K}^*|} = \frac{|\mathrm{GL}_n(\mathbb{K})|}{q-1}$$

Teorema 1.10 (Segundo Teorema de Isomorfía para grupos)**.** *Sea G un grupo, $H, K < G$ de forma que $K \lhd G$, entonces:*

$$H \cap K \lhd H$$

Y existe un isomorfismo de grupos de forma que

$$H/H \cap K \cong HK/K$$

La situación descrita podemos observarla en la Figura 1.3.

Demostración. En primer lugar, justifiquemos de forma breve que el grupo de la derecha del isomorfismo tiene todo el sentido, es decir, que HK es efectivamente un grupo (no lo sabemos a priori) y que $K \lhd HK$. Para ello:

- Para ver que HK es un grupo (un subgrupo de G), como vimos en la Proposición **??**, hemos de ver que $HK = KH$. Para ello, como $K \lhd G$, tenemos que:
$$xK = Kx \qquad \forall x \in G$$
En particular, para $x \in H$, por lo que $HK = KH$.

- Como tenemos que $K < HK < G$ con $K \lhd G$, tendremos que $K \lhd HK$.

Consideramos ahora el homomorfismo resultante de componer la inclusión de H en G con la proyección al cociente G/K:

$$\begin{aligned} H &\xrightarrow{i} G \xrightarrow{p} G/K \\ x &\longmapsto x \longmapsto xK \end{aligned}$$

Si calculamos ahora la imagen y el núcleo de este homomorfismo:

$$\begin{aligned} Im(p \circ i) &= \{(p \circ i)(h) \mid h \in H\} = \{p(h) \mid h \in H\} = \{hK \mid h \in H\} \overset{(*)}{=} HK/K \\ \ker(p \circ i) &= \{h \in H \mid hK = (p \circ i)(h) = K\} = \{h \in H \mid h \in K\} = H \cap K \end{aligned}$$

Como $H \cap K = \ker(p \circ i)$, tenemos por la Proposición 1.7 que $H \cap K \lhd H$. Si aplicamos el Primer Teorema de Isomorfía al homomorfismo $p \circ i$, llegamos a que:

$$\frac{H}{H \cap K} = \frac{H}{\ker(p \circ i)} \cong Im(p \circ i) = HK/K$$

La igualdad $(*)$ anterior puede parecer rara, pero es muy natural, veamos que:

$$\{hK \mid h \in H\} = HK/K$$

$\subseteq$) Dado $h \in H$, en particular tendremos que $h = h \cdot 1 \in HK$, con lo que $hK \in HK/K$.

$\supseteq$) Sea $hkK \in HK/K$ para ciertos $h \in H$, $k \in K$, por la definición del producto en el grupo cociente tenemos:

$$hkK = (hK)(kK) = (hK)K = hK \in \{hK \mid h \in H\}$$

□

El Segundo Teorema de Isomorfía para grupos puede recordarse fácilmente observando la siguiente figura, donde pensamos en que $HK/K \cong H/H \cap K$ bajo las hipótesis del Teorema, que podemos recordar observando las diagonales del paralelogramo:

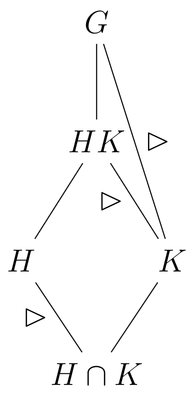


Figura 1.3: Situación del Teorema 1.10.

Ejemplo. Sea $H < S_n$ un subgrupo conteniendo una permutación impar, entonces $[H : H \cap A_n] = 2$. Es decir, H tiene el mismo número de permutaciones pares que de impares.

Para verlo, sabemos que $[S_n : A_n] = 2$, luego $A_n \lhd S_n$ y además, como H tiene una permutación impar, tenemos que $H \not\subseteq A_n$, por lo que tenemos:

$$HA_n = S_n$$

Que se puede deducir observando el retículo de subgrupos de S_n. Por el Segundo Teorema de Isomorfía, tenemos que:

$$H/H \cap A_n \cong S_n/A_n \cong \mathbb{Z}_2$$

Teorema 1.11 (Tercer Teorema de Isomorfía para grupos, o del doble cociente)**.** *Sea G un grupo, $N \lhd G$, entonces existe una biyección entre los subgrupos de G que contienen a N y los subgrupos de G/N, dada por $H \longmapsto H/N$.*

Además, $H \lhd G \Longleftrightarrow H/N \lhd G/N$. En este caso:

$$\frac{G/N}{H/N} \cong G/H$$

Demostración. Si consideramos la proyección al cociente $p : G \to G/N$ dada por $p(x) = xN$ para todo $x \in G$, consideramos las aplicaciones imagen directa e imagen inversa por p, dadas por:

$$\begin{gathered} p_* : \mathcal{P}(G) \to \mathcal{P}(G/N) \\ p^* : \mathcal{P}(G/N) \to \mathcal{P}(G) \\ p_*(H) = \{p(h) \mid h \in H\} \subseteq G/N \\ p^*(J) = \{x \in G \mid p(x) \in J\} \subseteq G \end{gathered}$$

Que podemos restringirlas en dominio y codominio a los conjuntos:

$$\begin{aligned} \mathcal{A} &= \{H < G \mid N \subseteq H\} \\ \mathcal{B} &= \{J < G/N\} \end{aligned}$$

Obteniendo aplicaciones (que nombramos igual ya que nos olvidamos de las otras):

$$p_* : \mathcal{A} \to \mathcal{B}$$
$$p^* : \mathcal{B} \to \mathcal{A}$$

Veamos que estas aplicaciones están bien definidas (es decir, que podemos poner $\mathcal{B}$ como codominio de p_* y $\mathcal{A}$ como codominio de p^*):

- Para p_*, hemos de observar primero que si cogemos $H \in \mathcal{A}$, entonces tendremos por el Corolario 1.3.1 que $N \lhd H$. En segundo lugar, ya vimos en la Proposición **??** que si $H < G$ entonces $p_*(H) < G/N$, por lo que la aplicación p_* está bien definida. Vemos lo que pasa cuando la aplicamos a un elemento de $\mathcal{A}$:
$$p_*(H) = \{p(h) \mid h \in H\} = \{hN \mid h \in H\} = H/N < G/N$$

- Para p^*, vimos también en la Proposición **??** que si $J < G/N$ (es decir, $J \in \mathcal{B}$), entonces $p^*(J) < G$. Veamos que $N \subseteq p^*(J)$. Para ello, vemos que:
$$p(n) = nN = N \in J \qquad \forall n \in N$$
Donde $N \in J$ por ser N el elemento neutro para el grupo G/N y ser $J < G/N$. En conclusión, $n \in p^*(J)$ $\forall n \in N$, y concluimos que p^* está bien definida.

Veamos ahora qué sucede con la composición de las aplicaciones:

- Por una parte, dado $J \in \mathcal{B}$:
$$(p_* \circ p^*)(J) = p_*(\{x \in G \mid p(x) \in J\}) \overset{(*)}{=} J$$
Donde en $(*)$ hemos aplicado que p es sobreyectiva, por lo que si tenemos $yN \in J$, existirá un $x \in G$ de forma que $p(x) = yN$, luego todos los valores de J se alcanzan.

- Dado $H \in \mathcal{A}$, veamos si $H = (p^* \circ p_*)(H)$:

  $\subseteq$) Sea $h \in H$, tenemos que:
$$\{h\} = p^*(\{p(h)\}) = p^*(p_*(\{h\})) \subseteq p^*(p_*(H))$$

  $\supseteq$) Sea $x \in p^*(p_*(H))$, entonces:
$$xN = p(x) \in p_*(H) = H/N = \{hN \mid h \in H\}$$

  Por lo que $x \in H$.

Concluimos que $(p_*)^{-1} = p^*$, por lo que p_* es biyectiva y $\mathcal{A}$ es biyectivo con $\mathcal{B}$.

Veamos ahora que:
$$H \lhd G \Longleftrightarrow H/N \lhd G/N$$

$\Longrightarrow$) Sean $xN \in G/N$, $hN \in H/N$:

$$xNhN(xN)^{-1} = xNhNx^{-1}N \overset{(*)}{=} xhx^{-1}N \overset{(**)}{\in} H/N$$

Donde en $(*)$ hemos aplicado la definición del producto en el cociente y en $(**)$ hemos aplicado que $H \lhd G$, con lo que $xhx^{-1} \in H$.

$\Longleftarrow$) Ahora, sean $x \in G$ y $h \in H$:

$$xhx^{-1}N = xNhN(xN)^{-1} \in H/N$$

De donde concluimos que $xhx^{-1} \in H$, con lo que $H \lhd G$.

Finalmente, en este caso veamos que $\frac{G/N}{H/N} \cong G/H$. Para ello, consideramos las proyecciones $p_N : G \to G/N$ y $p_H : G \to G/H$. Como $N \subseteq H = \ker(p_H)$, sabemos por la Propiedad Universal del grupo cociente (Teorema 1.8) que existe un único homomorfismo $\varphi : G/N \to G/H$ que hace conmutar el siguiente diagrama:

$$\begin{tikzcd} G \arrow[r, "p_N"] \arrow[dr, "p_H"'] & G/N \arrow[d, dotted, "\varphi"] \\ & G/H \end{tikzcd}$$

Es decir, φ cumplirá que:

$$\varphi p_N = p_H$$

Si aplicamos ahora el Primer Teorema de Isomorfía sobre φ:

$$\frac{G/N}{\ker(\varphi)} \cong Im(\varphi)$$

Y basta observar que:

- Por ser p_H sobreyectiva (es una proyección), φ también será sobreyectiva, por lo que $Im(\varphi) = G/H$.
- Veamos que $\ker(\varphi) = H/N$:

  $\subseteq$) Sea $xN \in \ker(\varphi)$, entonces:

  $$H = \varphi(xN) = \varphi(p_N(x)) = p_H(x) = xH \Longrightarrow x \in H$$

  $\supseteq$) Sea $hN \in H/N$, entonces:

  $$\varphi(hN) = \varphi(p_N(h)) = p_H(h) = hH = H$$

  Por lo que $hN \in \ker(\varphi)$.

En definitiva, hemos probado que:

$$\frac{G/N}{H/N} \cong G/H$$

$\square$

Ejemplo. Recordando el retículo de subgrupos de D_4:

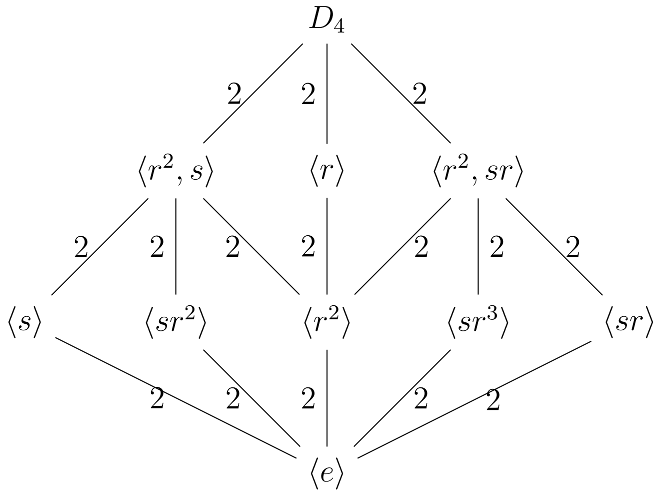
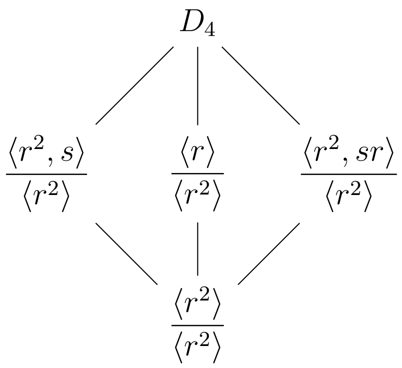
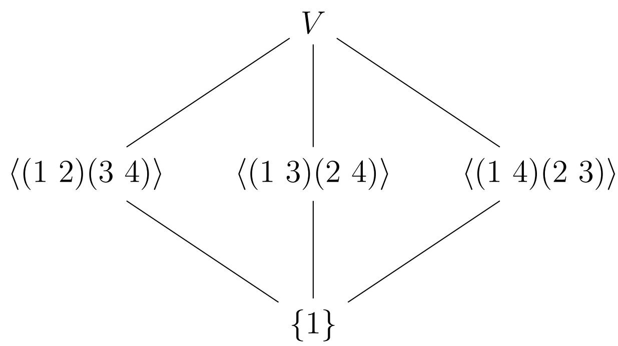


Figura 1.4: Diagrama de Hasse para los subgrupos de D_4.

Si consideramos los 5 grupos del centro del diagrama y los dividimos entre $\langle r^2\rangle$, llegamos a que el conjunto que contiene a estos es isomorfo al grupo de Klein:





Cuarto Teorema de Isomorfía

Antes de ver el Cuarto Teorema de Isomorfía, hemos de ver dos Lemas previos que nos ayudarán en su demostración:

Lema 1.12 (Ley modular o regla de Dedekind)**.** *Sea G un grupo y $A, B, C < G$ con $A < C$, entonces:*

$$A(B \cap C) = AB \cap C$$

Demostración. Por doble implicación:

$\subseteq$) Sea $z \in A(B \cap C)$, entonces existen $a \in A$ y $x \in B \cap C$ de forma que $z = ax$, con lo que $ax \in AB$ y $ax \in AC = C$ por ser $A < C$, de donde deducimos que $z = ax \in AB \cap C$.

$\supseteq$) Sea $z \in AB \cap C$, entonces:

- Por una parte, como $z \in AB$, tenemos que $\exists a \in A$ y $b \in B$ de forma que $z = ab$.
- Además, como $z \in C$, tenemos que $z = ab \in C$

Por ser $A < C$, tenemos que $a \in C$, por lo que $a^{-1} \in C$, de donde:

$$b = a^{-1}z \in C$$

Como además teniamos $b \in B$, llegamos a que $z = ab \in A(B \cap C)$.

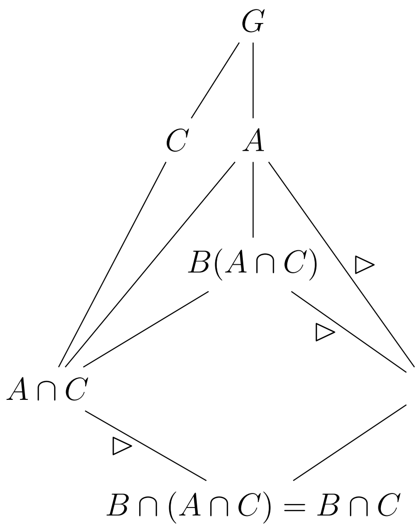
□

Observación. La hipótesis $A < C$ no es necesaria, basta con tener $A \subseteq C$.

Lema 1.13. *Sea G un grupo y $A, B, C < G$ con $B \lhd A$, entonces:*

i) $B \cap C \lhd A \cap C$ *y* ${}^{A\cap C}/_{B\cap C} \cong {}^{B(A\cap C)}/_{B}$.

ii) *Si además $C \lhd G$, entonces:* $BC \lhd AC$ *y* ${}^{AC}/_{BC} \cong {}^{A}/_{B(A\cap C)}$



Demostración. Veamos los dos apartados:

i) Aplicando el Segundo Teorema de Isomorfía sobre el diagrama (observamos el paralelogramo), tenemos el resultado de forma directa:

$${}^{A\cap C}/_{B\cap C} \cong {}^{B(A\cap C)}/_{B}$$

ii) Ahora, si $C \lhd G$ (los elementos de G conmutan con los de C), tendremos que $BC = CB$ y $AC = CA$, por lo que $BC, AC < G$. Además, como $B < A$, también tendremo que $BC < AC$. Veamos que esta última relación es normal. Para ello, sean $bc \in BC$, $ax \in AC$:

$$axbc(ax)^{-1} = axbcx^{-1}a^{-1} = axa^{-1}aba^{-1}acx^{-1}a^{-1} = (axa^{-1})(aba^{-1})(acx^{-1}a^{-1})$$

Para ver dónde está este último elemento:

- Como $x \in C$ y $C \lhd G$, $axa^{-1} \in C$.
- Como $b \in B$ y $B \lhd A$, $aba^{-1} \in B$.
- Como $c, x \in C$, tendremos $cx^{-1} \in C$ y por ser $C \lhd G$, $acx^{-1}a^{-1} \in C$.

En definitiva:

$$axbc(ax)^{-1} \in CBC = BCC = BC$$

De donde deducimos que $BC \lhd AC$. Ahora, si tenemos en mente el siguiente diagrama, podemos aplicar el Segundo Teorema de Isomorfía, ya que tenemos $A, BC < AC$ y $BC \lhd AC$.

$$\begin{tikzcd}[column sep=small]
 & AC \arrow[dl, dash] \arrow[dr, dash] & \\
A \arrow[dr, dash] & & BC \arrow[dl, dash] \\
 & BC \cap A = B(A \cap C) &
\end{tikzcd}$$

El Segundo Teorema de Isomorfía nos dice que $B(C \cap A) \lhd A$, y que:

$${}^{A}/_{B(A\cap C)} \cong {}^{AC}/_{BC}$$

$\square$

Observación. Sin embargo, el Lema anterior se podría hacer también suponiendo solo que $A, B \subseteq G$ para A y B, solo es necesario suponer que $C < G$.

A continuación, veremos el Cuarto Teorema de Isomorfía, o Teorema de Zassenhaus, para el cual conviene pensar en la Figura 1.6 (aunque en esta figura el retículo de subgrupos está al revés de a lo que estamos acostumbrados: arriba los conjuntos de menor tamaño y debajo los conjuntos mayores).

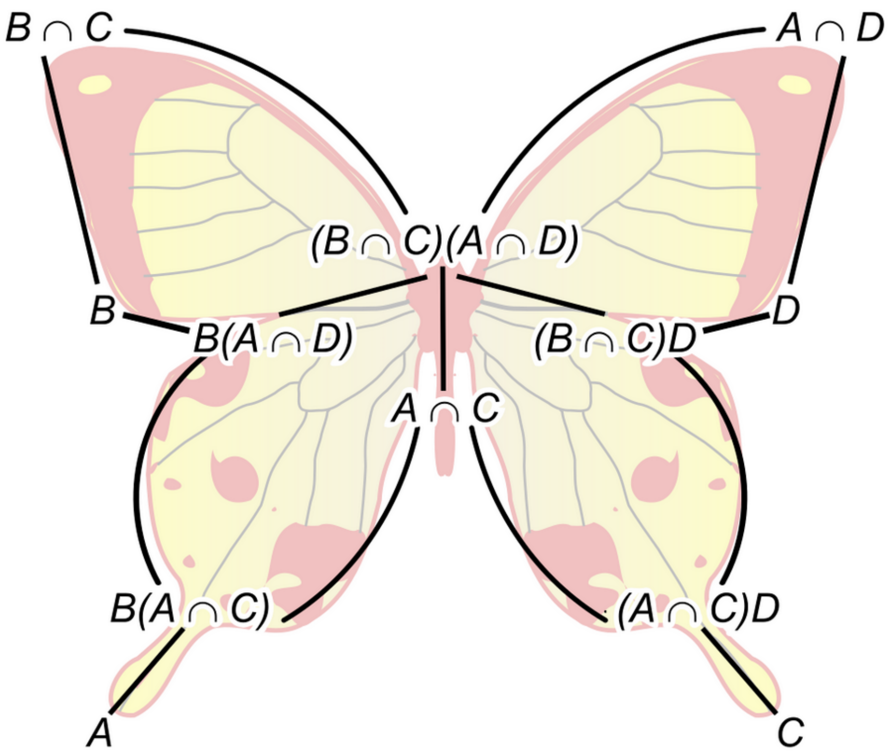


Figura 1.6: Situación del Teorema 1.14

Teorema 1.14 (Cuarto Teorema de Isomorfía para grupos)**.** *Sea G un grupo y $A_1, C_1, A_2, C_2 < G$ y $C_1 \lhd A_1$, $C_2 \lhd A_2$, entonces:*

i) $(A_1 \cap C_2)C_1 \lhd (A_1 \cap A_2)C_1$.

ii) $(A_2 \cap C_1)C_2 \lhd (A_1 \cap A_2)C_2$.

iii) ${}^{(A_1\cap A_2)C_1}/_{(A_1\cap C_2)C_1} \cong {}^{A_1\cap A_2}/_{(A_1\cap C_2)(A_2\cap C_1)} \cong {}^{(A_1\cap A_2)C_2}/_{(A_2\cap C_1)C_2}$

Demostración. Veamos cada apartado:

i) En primer lugar[2], como $C_1 \lhd A_1$, entonces los elementos de C_1 conmutarán con los de A_1, luego:

$$(A_1 \cap C_2)C_1 = C_1(A_1 \cap C_2)$$
$$(A_1 \cap A_2)C_1 = C_1(A_1 \cap A_2)$$

Por lo que ambos serán subgrupos de G. Además, como $C_2 < A_2$, tenemos ya que:

$$(A_1 \cap C_2)C_1 < (A_1 \cap A_2)C_1$$

Para ver la normalidad, sean $x \in (A_1 \cap A_2)C_1, y \in (A_1 \cap C_2)C_1$, entonces existirán elementos $a \in A_1 \cap A_2, b \in A_1 \cap C_2, c, c' \in C_1$ de forma que:

$$x = ac \qquad y = bc'$$

[2]Esta demostración se hizo en clase de otra forma usando resultados previos. Si alguien hace esta demostración de forma más sencilla que se ponga en contacto con nosotros.

Si calculamos:

$$xyx^{-1} = acbc'c^{-1}a^{-1} = (aca^{-1})(aba^{-1})(ac'a^{-1})(ac^{-1}a^{-1})$$

Veamos dónde está este elemento:

- Como $c \in C_1$, $a \in A_1 \cap A_2$ y $C_1 \lhd A_1$, $aca^{-1} \in C_1$.
- Como $b \in A_1 \cap C_2 \subseteq C_2$ y $a \in A_1 \cap A_2 \subseteq A_2$ con $C_2 \lhd A_2$, entonces $aba^{-1} \in A_1 \cap C_2$.
- Como $c', c \in C_1$, $a \in A_1 \cap A_2$ y $C_1 \lhd A_1$, $ac'a^{-1}, ac^{-1}a^{-1} \in C_1$.

En definitva:

$$xyx^{-1} \in C_1(A_1 \cap C_2)C_1C_1 = (A_1 \cap C_2)C_1C_1C_1 = (A_1 \cap C_2)C_1$$

Y concluimos que $(A_1 \cap C_2)C_1 \lhd (A_1 \cap A_2)C_1$.

ii) Es análogo, cambiando los papeles de C_1 y C_2.

iii) Para el primer isomorfismo, si tomamos:

$$\begin{aligned} G_1 &= A_1 \\ A &= A_1 \cap A_2 \\ B &= A_1 \cap C_2 \\ C &= C_1 \end{aligned}$$

Nos encontramos en las Hipótesis del Lema 1.13, ya que $A, B, C < G_1$ y $B \lhd A$, por ser $C_2 \lhd A_2$. Como además $C \lhd G_1$ por hipótesis, concluimos que:

$$AC/BC \cong A/B(A\cap C)$$

Que en nuestro caso significa:

$$(A_1\cap A_2)C_1/(A_1\cap C_2)C_1 \cong A_1\cap A_2/(A_1\cap C_2)(A_1\cap A_2\cap C_1) = A_1\cap A_2/(A_1\cap C_2)(A_2\cap C_1)$$

Para el segundo, hemos de tomar:

$$\begin{aligned} G_2 &= A_2 \\ A &= A_1 \cap A_2 \\ B &= A_1 \cap C_2 \\ C &= C_2 \end{aligned}$$

□

1.4. Producto directo

En un ejemplo del Capítulo **??** vimos que dados dos grupos H y G podíamos definir de forma sencilla una operación en $H \times G$ en función de las operaciones de H y G, que nos dotaba a $H \times G$ de estructura de grupo. A este grupo lo llamábamos grupo directo de G y H, grupo que volveremos a definir a partir de ahora y en el que nos centraremos durante esta sección.

Definición 1.4 (Producto directo)**.** Sean H y G dos grupos, definimos en el producto cartesiano $H \times G$ la operación

$$\begin{array}{rccc} \cdot : & (H \times G) \times (H \times G) & \longrightarrow & H \times G \\ & (h,k)(h',k') & \longmapsto & (hh', kk') \end{array}$$

Se verifica que $H \times G$ junto con esta operación es un grupo:

- Es claro que la operación es asociativa, por ser las respectivas operaciones de H y G asociativas.
- El elemento $(1,1) \in H \times G$ es el elemento neutro para la operación.
- Dado un elemento $(h,k) \in H \times G$, tenemos que:

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

Este grupo que hemos definido en $H \times G$ recibirá el nombre de producto directo de H y G.

Algunos autores llaman al producto directo que hemos definido producto directo externo, para diferenciarlo del producto directo interno, que luego definiremos. Sin embargo, nosotros lo llamaremos simplemente producto directo.

Proposición 1.15. *Si H y K son dos grupos finitos, entonces:*

i) $|H \times K| = |H||K|$.

ii) $O(h,k) = \text{mcm}(O(h), O(k)) \ \forall (h,k) \in H \times K$.

Demostración. Veamos las dos propiedades:

i) Se vió en Álgebra I.

ii) Como H y K son finitos, también lo será $H \times K$ y como ya vimos en la Proposición **??**, los órdenes de los elementos son finitos, por lo que el enunciado tiene todo el sentido.

Llamando $m(h,k) = \text{mcm}(O(h), O(k))$, en primer lugar vemos que:

$$(h,k)^{m(h,k)} = \left(h^{m(h,k)}, k^{m(h,k)}\right) = (1,1)$$

Donde en la primera igualdad hemos usado la definición del producto directo de H y K y en la segunda hemos usado que $O(h) \mid m(h,k)$ y que $O(k) \mid m(h,k)$.

Ahora, sea $t \in \mathbb{N} \setminus \{0\}$ de forma que $(h,k)^t = (1,1)$, tenemos entonces que $h^t = 1$ y $k^t = 1$, con lo que $O(h) \mid t$ y $O(k) \mid t$, de donde deducimos que (por definición de mínimo común múltiplo) $m(h,k) \mid t$. □

Definición 1.5 (Proyecciones e inyecciones)**.** Dados H y G dos grupos, en el producto directo de H y G podemos definir 4 aplicaciones que nos serán útiles:

1. La proyección en la primera coordenada, $p_1 : H \times G \to H$, dada por:
$$p_1(h,k) = h \qquad \forall (h,k) \in H \times G$$
2. La proyección en la segunda coordenada, $p_2 : H \times G \to G$, dada por:
$$p_2(h,k) = k \qquad \forall (h,k) \in H \times G$$
3. La inyección en la primera coordenada, $i_1 : H \to H \times G$, dada por:
$$i_1(h) = (h,1) \qquad \forall h \in H$$
4. La inyección en la segunda coordenada, $i_2 : G \to H \times G$, dada por:
$$i_2(h) = (1,k) \qquad \forall k \in G$$

Aplicaciones que podremos recordar fácilmente observando la Figura 1.7.

$$\begin{tikzcd} H \arrow[r, shift left, "i_1"] & H \times G \arrow[l, shift left, "p_1"] \arrow[r, shift right, "p_2"'] & G \arrow[l, shift right, "i_2"'] \end{tikzcd}$$

Figura 1.7: Diagrama de las proyecciones y las inyecciones.

Proposición 1.16. *Se verifica que:*

1. *Las proyecciones y las inyecciones son homomorfismos de grupos.*
2. $p_1 i_1 = id = p_2 i_2$ *y las aplicaciones* $p_1 i_2$ *y* $p_2 i_1$ *son la aplicación constantemente igual a* 1.
3. *Las proyecciones son sobreyectivas y las inyecciones son inyectivas.*
4. *Si tomamos* $H' = \{(h,1) \mid h \in H\}$*, tenemos que:*
$$Im(i_1) = \ker(p_2) = H' \lhd H \times G$$
Además, $H' \cong H$.
5. *De la misma forma, si tomamos* $G' = \{(1,k) \mid k \in G\}$*, tenemos:*
$$Im(i_2) = \ker(p_1) = G' \lhd H \times G$$
Además, $G' \cong G$.
6. $H' \cap G' = \{1\}$.
7. $xy = yx$ *para todo* $x \in H'$, $y \in G'$.

Demostración. Veamos cada apartado:

1. Tenemos 4 casos:

   - Para p_1, vemos que:

     $$p_1((h,k)(h',k')) = p_1(hh',kk') = hh' = p_1(h,k)p_1(h',k') \qquad \forall (h,k),(h',k') \in H\times G$$

     Y la demostración para p_2 es análoga.

   - Para i_1, vemos que:

     $$i_1(hh') = (hh',1) = (h,1)(h',1) = i_1(h)i_1(h') \qquad \forall h,h' \in H$$

     Y la demostración es análoga para i_2.

2. Si los índices coinciden, tenemos que:

   $$\begin{aligned} (p_1 \circ i_1)(h) &= p_1(i_1(h)) = p_1(h,1) = h \qquad \forall h \in H \\ (p_2 \circ i_2)(k) &= p_2(i_2(k)) = p_2(1,k) = k \qquad \forall k \in G \end{aligned}$$

   Y si no coinciden, tenemos:

   $$\begin{aligned} (p_1 \circ i_2)(k) &= p_1(i_2(k)) = p_1(1,k) = 1 \qquad \forall k \in G \\ (p_2 \circ i_1)(h) &= p_2(i_1(h)) = p_2(h,1) = 1 \qquad \forall h \in H \end{aligned}$$

3. Para comprobar que p_1 es sobreyectiva, vemos que dada $h \in H$, tenemos que $p_1(h,1) = h$ y para ver que p_2 es sobreyectiva, dado $k \in G$, tenemos que $p_2(1,k) = k$.

   Para ver la inyectividad de i_1, si dados $h,h' \in H$ de forma que:

   $$(h,1) = i_1(h) = i_1(h') = (h',1)$$

   De donde deducimos que $h = h'$, por lo que i_1 es inyectiva. La demostración para i_2 es análoga.

4. En primer lugar:

   $$\begin{aligned} Im(i_1) &= \{i_1(h) \mid h \in H\} = \{(h,1) \mid h \in H\} \\ \ker(p_2) &= \{(h,k) \in H \times G \mid p_2(h,k) = 1\} = \{(h,k) \in H \times G \mid k = 1\} \\ &= \{(h,1) \in H \times G\} = \{(h,1) \mid h \in H\} \end{aligned}$$

   Además, la igualdad $H' = \ker(p_2)$ nos dice que $H' \lhd H \times G$, gracias a la Proposición 1.7.

   Para ver que $H' \cong H$, en el apartado 1 vimos que i_1 era un homomorfismo y aplicando 3 tenemos que, de hecho, es un monomorfismo. Como $Im(i_1) = H'$, la restricción al codominio de i_1 a su imagen nos da un isomorfismo entre H y H', con lo que $H' \cong H$.

5. Vemos que:

$$\begin{aligned} Im(i_2) &= \{i_2(k) \mid k \in G\} = \{(1,k) \mid k \in G\} \\ \ker(p_1) &= \{(h,k) \in H \times G \mid p_1(h,k) = 1\} = \{(h,k) \in H \times G \mid h = 1\} \\ &= \{(1,k) \in H \times G\} = \{(1,k) \mid k \in G\} \end{aligned}$$

La igualdad $G' = \ker(p_1)$ nos vuelve a decir que $G' \lhd H \times G$.

Y finalmente, para ver que $G' \cong G$, tenemos que i_2 es un monomorfismo, por lo que la restricción en codominio a su imagen, $Im(i_2) = G'$ nos da un isomorfismo entre G y G'.

6. La igualdad se tiene porque:

$$H' \cap G' = \{(h,k) \in H \times G \mid k = 1 \ \wedge \ h = 1\} = \{(1,1)\} = \{1\}$$

7. Sean $x \in H'$ y $y \in G'$, entonces $\exists h \in H$ y $k \in G$ de forma que $x = (h,1)$ y $y = (1,k)$, de donde:

$$xy = (h,1)(1,k) = (h,k) = (1,k)(h,1) = yx$$

□

1.4.1. Caracterización del grupo directo por isomorfismo

Teorema 1.17 (Propiedad universal del producto directo)**.** *Sea G un grupo y sean $f_1 : G \to H$, $f_2 : G \to K$ dos homomorfismos de grupos, entonces existe un único homomorfismo de grupos $f : G \to H \times K$ tal que $p_1 f = f_1$ y $p_2 f = f_2$.*
Es decir, existe un único homomorfismo f que hace conmutar el siguiente diagrama:

$$\begin{tikzcd} & G \arrow[dl, "f_1"'] \arrow[d, dashed, "f"] \arrow[dr, "f_2"] & \\ H & H \times K \arrow[l, "p_1"] \arrow[r, "p_2"'] & K \end{tikzcd}$$

Demostración. Definimos $f : G \to H \times K$ dada por:

$$f(x) = (f_1(x), f_2(x)) \qquad \forall x \in G$$

- Vemos las dos igualdades:

$$\begin{aligned} (p_1 \circ f)(x) &= p_1(f(x)) = p_1(f_1(x), f_2(x)) = f_1(x) \qquad \forall x \in G \\ (p_2 \circ f)(x) &= p_2(f(x)) = p_2(f_1(x), f_2(x)) = f_2(x) \qquad \forall x \in G \end{aligned}$$

- Para ver que f es un homomorfismo:

$$\begin{aligned} f(xy) &= (f_1(xy), f_2(xy)) = (f_1(x)f_1(y), f_2(x)f_2(y)) \\ &= (f_1(x), f_2(x))(f_1(y), f_2(y)) = f(x)f(y) \qquad \forall x, y \in G \end{aligned}$$

- Sea $g : G \to H \times K$ un homomorfismo de grupos de forma que $p_1 g = f_1$ y $p_2 g = f_2$, entonces:

$$g(x) = (p_1(g(x)), p_2(g(x))) = (f_1(x), f_2(x)) = f(x) \qquad \forall x \in G$$

  Por lo que $g = f$.

$\square$

El producto directo es único salvo isomorfismos. Es decir, si hay otro grupo que verifica la propiedad universal de grupo directo, este debe ser isomorfo al grupo directo.

Teorema 1.18. *Sea L un grupo y sean $l_1 : L \to H$, $l_2 : L \to K$ dos homomorfismos de grupos de forma que si G es un grupo y $f_1 : G \to H$ y $f_2 : G \to K$ son otros dos homomorfismos que cumplen la tesis de la propiedad universal del producto directo para L (es decir, que existe un único homomorfismo $f : G \to L$ de forma que $l_1 f = f_1$ y $l_2 f = f_2$). Entonces, tendremos que:*

$$L \cong H \times K$$

La situación es la descrita en el siguiente diagrama:

$$\begin{tikzcd}
 & L \arrow[dl, "l_1"'] \arrow[dr, "l_2"] & \\
H & & K \\
 & G \arrow[ul, "f_1"] \arrow[ur, "f_2"'] \arrow[uu, dashed, "f"] &
\end{tikzcd}$$

Demostración. En primer lugar, como $l_1 : L \to H$ y $l_2 : L \to K$ son dos homomorfismos, verifican las hipótesis de la propiedad universal del grupo cociente, por lo que existe un único homomorfismo $l : L \to H \times K$ de forma que:

$$p_1 l = l_1$$
$$p_2 l = l_2$$

$$\begin{tikzcd}
 & L \arrow[dl, "l_1"'] \arrow[dr, "l_2"] \arrow[d, dashed, "l"] & \\
H & H \times K \arrow[l, "p_1"] \arrow[r, "p_2"'] & K
\end{tikzcd}$$

Ahora, si tomamos $G = H \times K$ y consideramos $p_1 : H \times K \to H$ y $p_2 : H \times K \to K$, tenemos dos homomorfismos que por hipótesis pueden factorizarse pasando por L, es decir, existe un único homomorfismo $p : H \times K \to L$ de forma que:

$$l_1 p = p_1$$
$$l_2 p = p_2$$

$$\begin{tikzcd}
 & L \arrow[dl, bend right, "l_1"'] \arrow[dr, bend left, "l_2"] \arrow[d, dashed, bend left, "l"] & \\
H & H \times K \arrow[l, "p_1"] \arrow[r, "p_2"'] \arrow[u, dashed, bend left, "p"] & K
\end{tikzcd}$$

Para terminar la demostración, basta ver que p y l son inversos el uno del otro. Para ello, observamos que:

$$l_1 = p_1 l = l_1 p l \Longrightarrow pl = id_L$$
$$p_1 = l_1 p = p_1 l p \Longrightarrow lp = id_{H\times K}$$

Concluimos que $p^{-1} = l$, con lo que p y l son isomorfismos y $L \cong H \times K$. □

Notemos que tanto en la propiedad universal del producto directo como en su unicidad por isomorfismo solo hemos usado las proyecciones p_1 y p_2. Si consideramos resultados análogos para las inyecciones i_1 y i_2, estos seguirán siendo ciertos, teniendo que añadir una hipótesis extra:

Teorema 1.19 (Propiedad universal del producto directo 2)**.** *Sea G un grupo y $f_1 : H \to G$, $f_2 : K \to G$ dos homomorfismos de grupos verificando que:*

$$f_1(h)f_2(k) = f_2(k)f_1(h) \qquad \forall h \in H, k \in K$$

Entonces, existe un único homomorfismo de grupos $f : H\times K \to G$ tal que $fi_1 = f_1$, $fi_2 = f_2$.

$$\begin{tikzcd}
 & G & \\
H \arrow[ur, "f_1"] \arrow[r, "i_1"'] & H \times K \arrow[u, dashed, "f"] & K \arrow[ul, "f_2"'] \arrow[l, "i_2"]
\end{tikzcd}$$

Demostración. Definimos $f : H \times K \to G$ dada por:

$$f(h, k) = f_1(h)f_2(k) \qquad \forall (h, k) \in H \times K$$

- Vemos que verifica las dos igualdades:

$$(f \circ i_1)(h) = f(i_1(h)) = f(h, 1) = f_1(h)f_2(1) = f_1(h) \qquad \forall h \in H$$
$$(f \circ i_2)(k) = f(i_2(k)) = f(1, k) = f_1(1)f_2(k) = f_2(k) \qquad \forall k \in K$$

- Vemos que f es un homomorfismo, ya que dados $(h, k), (h', k') \in H \times K$:

$$\begin{aligned} f((h, k)(h', k')) = f(hh', kk') &= f_1(hh')f_2(kk') = f_1(h)f_1(h')f_2(k)f_2(k') \\ &= f_1(h)f_2(k)f_1(h')f_2(k') = f(h, k)f(h', k') \end{aligned}$$

- Sea $g : H \times K \to G$ otro homomorfismo de grupos de forma que $gi_1 = f_1$ y $gi_2 = f_2$, entonces dado $(h, k) \in H \times K$:

$$g(h, k) = g((h, 1)(1, k)) = g(h, 1)g(1, k) = g(i_1(h))g(i_2(k)) = f_1(h)f_2(k) = f(h, k)$$

□

Teorema 1.20. *Sea L un grupo y $l_1 : H \to L$, $l_2 : K \to L$ dos homomorfismos de grupos que verifican que*

$$l_1(h)l_2(k) = l_2(k)l_1(h) \qquad \forall h \in H, k \in K$$

y que para todo grupo G y para todo par de homomorfismos $f_1 : H \to G$ y $f_2 : K \to G$ tales que

$$f_1(h)f_2(k) = f_2(k)f_1(h) \qquad \forall h \in H, k \in K$$

existe un único homomorfismo $f : L \to G$ tal que $fl_1 = f_1$ y $fl_2 = f_2$, entonces:

$$L \cong H \times K$$

$$\begin{tikzcd}
& L \arrow[dd, dashed, "f"'] & \\
H \arrow[ur, "l_1"] \arrow[dr, "f_1"'] & & K \arrow[ul, "l_2"'] \arrow[dl, "f_2"] \\
& G &
\end{tikzcd}$$

Demostración. En primer lugar, por ser $l_1 : H \to L$ y $l_2 : K \to L$ dos homomorfismos de forma que $l_1(h)l_2(k) = l_2(k)l_1(h)$ $\forall h \in H, k \in K$, tenemos que existe un único homomorfismo $l : H \times K \to L$ de forma que:

$$li_1 = l_1$$
$$li_2 = l_2$$

$$\begin{tikzcd}
& L & \\
H \arrow[ur, "l_1"] \arrow[r, "i_1"'] & H \times K \arrow[u, dashed, "l"'] & K \arrow[ul, "l_2"'] \arrow[l, "i_2"]
\end{tikzcd}$$

Ahora, si tomamos $G = H \times K$ y consideramos $i_1 : H \to H \times K$ y $i_2 : K \to H \times K$, tenemos por la Proposición 1.16 que $i_1(h)i_2(k) = i_2(k)i_1(h)$ para todo $h \in H$ y para todo $k \in K$, por lo que por hipótesis tenemos que existe un único homomorfismo $i : L \to H \times K$ de forma que:

$$il_1 = i_1$$
$$il_2 = i_2$$

$$\begin{tikzcd}
& L \arrow[d, dashed, bend right, "i"'] & \\
H \arrow[ur, bend left, "l_1"] \arrow[r, "i_1"'] & H \times K \arrow[u, dashed, bend right, "l"'] & K \arrow[ul, bend right, "l_2"'] \arrow[l, "i_2"]
\end{tikzcd}$$

Basta ver que i y l son inversos el uno del otro. Para ello, observamos que:

$$l_1 = li_1 = lil_1 \Longrightarrow li = id_{H \times K}$$
$$i_2 = il_2 = ili_2 \Longrightarrow il = id_L$$

Concluimos que $i^{-1} = l$, con lo que i y l son isomorfismos y $L \cong H \times K$. $\square$

1.4.2. Producto directo de una familia de grupos

Los resultados vistos para el producto directo de dos grupos G y H puede generalizarse para el conjunto cartesiano obtenido de multiplicar una familia arbitraria de grupos. Para estudiar este caso, fijaremos la notación en un inicio: sea Λ un conjunto arbitrariamente grande, si tenemos una familia de tantos grupos como elementos hay en Λ:

$$\{G_\lambda \mid \lambda \in \Lambda\}$$

Podemos considerar el producto cartesiano de todos ellos, que denotaremos por G:

$$G = \prod\{G_\lambda \mid \lambda \in \Lambda\} = \prod_{\lambda\in\Lambda} G_\lambda$$

Proposición 1.21. *Si $\{G_\lambda \mid \lambda \in \Lambda\}$ es una familia de grupos, definimos en su producto cartesiano $G = \prod_{\lambda\in\Lambda} G_\lambda$ la operación $\cdot : G \times G \to G$ dada por:*

$$x \cdot y = z$$

De forma que la $\lambda-$ésima coordenada de z es el producto de la $\lambda-$ésima coordenadas de x por la $\lambda-$ésima coordenada de y. Se verifica que G con esta operación es un grupo.

Notación. Si $\Lambda = \{1, \ldots, n\}$, notaremos:

$$G = \prod_{\lambda\in\Lambda} G_\lambda = G_1 \times G_2 \times \ldots \times G_n$$

Si por otra parte se tiene que $G_\lambda = H$ para todo $\lambda \in \Lambda$, entonces notaremos:

$$G = \prod_{\lambda\in\Lambda} G_\lambda = H^\Lambda$$

En el caso de que Λ sea finito y tenga n elementos, notaremos H^n.

Definición 1.6 (Proyecciones e inyecciones)**.** Fijado $\lambda \in \Lambda$, definimos:

- La proyección en la $\lambda-$ésima coordenada, $p_\lambda : G \to G_\lambda$ dada por:

  $$p_\lambda(g) = g_\lambda \qquad \forall g \in G$$

  Siendo g_λ la $\lambda-$ésima coordenada de g.

- La inyección en la $\lambda-$ésima coordenada, $i_\lambda : G_\lambda \to G$ dada por:

  $$i_\lambda(x) = g \qquad \forall x \in G_\lambda$$

  Donde $g_\mu = 1\ \forall \mu \in \Lambda \setminus \{\lambda\}$ y $g_\lambda = x$.

Proposición 1.22. *Sea $\{G_\lambda \mid \lambda \in \Lambda\}$ una familia de grupos y sea $G = \prod_{\lambda\in\Lambda} G_\lambda$, se verifica:*

1. *p_λ y i_λ son homomorfismos de grupos, $\forall \lambda \in \Lambda$.*

2. *Las proyecciones son epimorfismos y las inyecciones son monomorfismos.*

3. $p_\lambda i_\lambda = id_{G_\lambda}$ *y* $(p_\lambda i_\mu)(x) = 1$ *para todo* $x \in G_\mu$, $\forall \lambda \in \Lambda, \mu \in \Lambda \setminus \{\lambda\}$.

4. $G'_\lambda = Im(i_\lambda) \cong G_\lambda$ *y es un subgrupo normal de* G.

Teorema 1.23 (Propiedad universal del producto directo)**.** *Sea* $\{G_\lambda \mid \lambda \in \Lambda\} \cup \{H\}$ *una familia de grupos y* $G = \prod_{\lambda\in\Lambda} G_\lambda$, *si tenemos una familia de homomorfismos para cada coordenada* $\{f_\lambda : H \to G_\lambda \mid \lambda \in \Lambda\}$, *entonces existe un único homomorfismo* $f : H \to G$ *de forma que* $f_\lambda = p_\lambda f$, $\forall \lambda \in \Lambda$. *Además, cualquier otro grupo que verifique esta propiedad será isomorfo a* G.

$$\begin{tikzcd} H \arrow[d, dashed, "f"] \arrow[dr, "f_\lambda"] & \\ G \arrow[r, "p_\lambda"] & G_\lambda \end{tikzcd}$$

1.4.3. Producto directo de una familia finita de subgrupos

Teorema 1.24 (Ley asociativa general)**.** *Tenemos que:*

1. *Si* G_1, G_2, G_3 *son tres grupos, entonces:*

$$(G_1 \times G_2) \times G_3 \cong G_1 \times G_2 \times G_3 \cong G_1 \times (G_2 \times G_3)$$

2. *Si* $G_1, G_2, \ldots, G_n$ *son* n *grupos, entonces si* $k \in \{1, \ldots, n-1\}$, *se tiene:*

$$\left(\prod_{j=1}^{k} G_j\right) \times \left(\prod_{j=k+1}^{n} G_j\right) \cong \prod_{j=1}^{n} G_j$$

Teorema 1.25. *Sean* $G_1, G_2, \ldots, G_n$ n *grupos y* $G = G_1 \times G_2 \times \ldots \times G_n$*:*

1. $|G| = |G_1||G_2| \cdots |G_n|$. *En particular,* G *es finito si y solo si* G_k *es finito, para todo* $k \in \{1, \ldots, n\}$.

2. $O(g_1, \ldots, g_n) = \text{mcm}(O(g_1), \ldots, O(g_n))$, $\forall (g_1, \ldots, g_n) \in G$.

1.5. Producto directo interno

El caso que nos interesará ahora será fijado un grupo G, consideramos dos subgrupos suyos, $H, K < G$ y trataremos de caracterizar cuándo $H \times K \cong G$. En cuyo caso, diremos que G es producto directo interno de H y de K.

Definición 1.7 (Conmutador)**.** Sea G un grupo, definimos sobre G la operación conmutador $[\cdot,\cdot] : G \times G \to G$ dada por:

$$[h, k] = hk(kh)^{-1} = hkh^{-1}k^{-1} \qquad \forall h, k \in G$$

Esta operación viene a decirnos cómo de abelianos son los elementos h y k que estemos considerando.

Proposición 1.26. *Sea G un grupo y $h, k \in G$:*

$$hk = kh \iff [h, k] = 1$$

Demostración. Basta observar que:

$$hk = kh \iff (hk)^{-1} = (kh)^{-1} \iff [h, k] = hk(kh)^{-1} = 1$$

□

Aunque el siguiente Teorema no nos caracteriza el hecho de que el producto de dos subgrupos de un grupo sea producto directo interno, es el resultado al que comúnmente se le conoce como caracterización del producto directo interno, puesto que viene a decirnos cuándo $H \times K \cong G$ bajo un isomorfismo que se obtiene de una forma muy natural.

Por tanto, diremos que $H \times K$ con $H, K < G$ es producto directo intergo de G cuando $H \times K \cong G$ bajo el isomorfismo del siguiente Teorema:

Teorema 1.27 (Caracterización del producto directo interno)**.** *Sea G un grupo, $H, K < G$, equivalen:*

i) *La aplicación $\phi : H \times K \to G$ dada por $\phi(h, k) = hk$ es un isomorfismo.*

ii) *$H, K \lhd G$, $HK = G$ y $H \cap K = \{1\}$.*

iii) *$hk = kh \quad \forall h \in H, k \in K$, $H \vee K = G$ y $H \cap K = \{1\}$.*

iv) *$hk = kh \quad \forall h \in H, k \in K$ y para todo $g \in G$, $\exists_1 h \in H, \exists_1 k \in K$ de forma que $g = hk$.*

Demostración. Veamos las implicaciones:

$i) \Longrightarrow ii)$ Veamos las tres propiedades:

- Primero que $HK = G$:
  - $\subseteq$) $HK \subseteq G$ por definición de HK.
  - $\supseteq$) Como ϕ es sobreyectiva, dado $g \in G$, existen $h \in H$, $k \in K$ de forma que $g = \phi(h, k) = hk$, lo que nos dice que $G \subseteq HK$.
- Sea $g \in H \cap K$, entonces $g = \phi(g, 1) = \phi(1, g) = g$, pero por ser ϕ inyectiva, tenemos que $(g, 1) = (1, g)$, de donde $g = 1$.
- Finalmente, para ver que $H, K \lhd G$, basta observar que:

$$\begin{tikzcd} & G \arrow[d, bend left, "\phi^{-1}"] & \\ H & H \times K \arrow[l, "p_1"'] \arrow[r, "p_2"] \arrow[u, bend left, "\phi"] & K \end{tikzcd}$$

Para deducir:

$$\ker(p_2\phi^{-1}) = \{hk \in G \mid k = 1\} = H$$
$$\ker(p_1\phi^{-1}) = \{hk \in G \mid h = 1\} = K$$

De donde tenemos que $H, K \lhd G$ (ya que $p_2\phi^{-1}$ y $p_1\phi^{-1}$ son homomorfismos y H y K conciden con sus respectivos núcleos, ver la Proposición 1.7).

ii) $\Longrightarrow$ *iii)* Dados $h \in H$ y $k \in K$, veamos que $[h,k] = 1$, de donde deducimos que $hk = kh$:
$$[h,k] = hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$$

- Por un lado, como K es normal, tendremos que $hkh^{-1} \in K$, de donde $[h,k] = (hkh^{-1})k^{-1} \in K$.
- Por otro lado, como H es normal, tendremos también que $kh^{-1}k^{-1} \in H$, de donde $[h,k] = h(kh^{-1}k^{-1}) \in H$.

En definitiva:
$$[h,k] \in H \cap K = \{1\} \Longrightarrow hk = kh$$

Para la segunda propiedad, basta ver que:
$$G = HK \subseteq H \vee K \subseteq G$$

iii) $\Longrightarrow$ *iv)* Sea $g \in G$, veamos que se expresa como producto de un elemento de H por otro elemento de K. Para ello, como $G = H \vee K$, existirán elementos $\alpha_1, \ldots, \alpha_n \in H \cup K$ de forma que:
$$g = \alpha_1 \ldots \alpha_n$$

Pero como $hk = kh$ para todo $k \in K$ y $h \in H$, podremos conmutar los elementos de forma que lleguemos a:
$$g = (h_1 \ldots h_m)(k_{m+1} \ldots k_n) = hk \in HK$$

Para ciertos $h \in H$, $k \in K$. Para la unicidad, si $g = h_1k_1 = h_2k_2$, tenemos que:
$$h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{1\} \Longrightarrow h_2 = h_1 \wedge k_1 = k_2$$

iv) $\Longrightarrow$ *i)* Tenemos para $(h_1,k_1),(h_2,k_2) \in H \times K$ arbitrarios que:
$$\phi((h_1,k_1)(h_2,k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1,k_1)\phi(h_2,k_2)$$

De donde ϕ es un homomorfismo. La biyectividad de ϕ se debe a que dado $g \in G$, existen unos únicos $h \in H$, $k \in K$ de forma que $g = hk = \phi(h,k)$. □

Ejemplo. Veamos si los siguientes ejemplos son o no un producto interno directo, bajo el isomorfismo natural del Teorema anterior:

1. En $G = \mathbb{R}^*$, consideramos $H = \{\pm 1\}$ y $K = \{x \in \mathbb{R} \mid x > 0\}$.

   Sí es producto interno directo, ya que se verifican:

   - $G = HK$.
   - G es abeliano, luego $H, K \lhd G$.
   - $H \cap K = \{1\}$.

   Y podemos aplicar el Teorema 1.27.

2. Sean:

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \right\}$$
$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \right\}$$
$$K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \right\}$$

Dado un elemento de G, podemos escribirlo como un elemento de HK:

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ab \\ 0 & c \end{pmatrix}$$

Luego $G = HK$. Sin embargo, $hk \neq kh$ para $h \in H$ y $k \in K$, ya que:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & bc \\ 0 & c \end{pmatrix} \neq \begin{pmatrix} a & ab \\ 0 & c \end{pmatrix}$$

Por lo que G no es producto directo interno de H y de K.

3. Sea $G = \mathbb{C}^*$, consideramos $H = \{z \in \mathbb{C} \mid |z| = 1\}$ y $K = \mathbb{R}^+$. Por la forma polar de los números complejos, tenemos que $G = HK$:

$$z = \frac{z}{|z|}|z| \in HK$$

Y como G es abeliano, tenemos que $H, K \lhd G$. Además:

$$H \cap K = \{1\}$$

Veamos ahora cómo se comportan los subgrupos con el producto directo:

Proposición 1.28. *Sea G un grupo, $H, K < G$, si $H_1 < H$ y $K_1 < K$, entonces:*

1. *$H_1 \times K_1 < H \times K$.*
2. *Existe un monomorfismo $Aut(H) \times Aut(K) \to Aut(H \times K)$.*

Demostración. Veamos que los dos se cumplen:

1. $H_1 \times K_1 \subseteq H \times K$. Además, como $H_1 < H$ y $K_1 < K$, $H_1 \times K_1$ va a ser cerrado para el producto, el producto será asociativo, tendrá al elemento $(1, 1)$ como neutro y fijado un elemento $(x, y) \in H_1 \times K_1$, tendremos que $(x, y)^{-1} = (x^{-1}, y^{-1}) \in H_1 \times K_1$, de donde concluimos que $H_1 \times K_1 < H \times K$.

2. Consideramos:

$$\begin{array}{rccc} \psi : & Aut(H) \times Aut(K) & \longrightarrow & Aut(H \times K) \\ & (\alpha, \beta) & \longmapsto & \psi(\alpha, \beta) \end{array}$$

Donde $\psi(\alpha, \beta) : H \times K \to H \times K$ viene dada por:

$$\psi(\alpha, \beta)(h, k) = (\alpha(h), \beta(k)) \qquad \forall (h, k) \in H \times K$$

Veamos en primer lugar que la aplicación ψ está bien definida, es decir, que $\psi(\alpha, \beta)$ es un automorfismo siempre que $\alpha \in Aut(H)$ y $\beta \in Aut(K)$:

- Para ver que $\psi(\alpha,\beta)$ es un homomorfismo, dados $(h,k),(h',k')\in H\times K$:

$$\begin{aligned}&\psi(\alpha,\beta)((h,k)(h',k'))=\psi(\alpha,\beta)(hh',kk')=(\alpha(hh'),\beta(kk'))\\&=(\alpha(h)\alpha(h'),\beta(k)\beta(k'))=(\alpha(h),\beta(k))(\alpha(h'),\beta(k'))=\psi(\alpha,\beta)(h,k)\psi(\alpha,\beta)(h',k')\end{aligned}$$

- Para la sobreyectividad, dado $(h,k)\in H\times K$, como $\alpha\in Aut(H)$ y $\beta\in Aut(K)$ son sobreyectivas, existirán $h'\in H$, $k'\in K$ de forma que:

$$\alpha(h')=h \qquad \beta(k')=k$$

Por lo que:

$$\psi(\alpha,\beta)(h',k')=(\alpha(h'),\beta(k'))=(h,k)$$

- Para la inyectividad, sean $(h,k),(h',k')\in H\times K$ de forma que:

$$(\alpha(h),\beta(k))=\psi(\alpha,\beta)(h,k)=\psi(\alpha,\beta)(h',k')=(\alpha(h'),\beta(k'))$$

De donde deducimos que:

$$\alpha(h)=\alpha(h') \qquad \beta(k)=\beta(k')$$

Pero como α y β son inyectivas, tenemos que $h=h'$ y $k=k'$, de donde $(h,k)=(h',k')$.

Finalmente, veamos que ψ es un monomorfismo:

- Para ver que es un homomorfismo, dadas $(\alpha,\beta),(\alpha',\beta')\in Aut(H)\times Aut(K)$:

$$\psi((\alpha,\beta)(\alpha',\beta'))=\psi(\alpha\alpha',\beta\beta')\overset{(*)}{=}\psi(\alpha,\beta)\psi(\alpha',\beta')$$

Donde en $(*)$ se da la igualdad funcional, ya que para $(h,k)\in H\times K$:

$$\begin{aligned}\psi(\alpha\alpha',\beta\beta')(h,k)&=((\alpha\circ\alpha')(h),(\beta\circ\beta')(k))=(\alpha(\alpha'(h)),\beta(\beta'(k)))\\(\psi(\alpha,\beta)\psi(\alpha',\beta'))(h,k)&=\psi(\alpha,\beta)(\alpha'(h),\beta'(k))=(\alpha(\alpha'(h)),\beta(\beta'(k)))\end{aligned}$$

- Para ver que ψ es inyectiva, sean $(\alpha,\beta),(\alpha',\beta')\in Aut(H)\times Aut(K)$ de forma que:

$$\psi(\alpha,\beta)=\psi(\alpha',\beta')$$

Entonces:

$$\psi(\alpha,\beta)(h,k)=(\alpha(h),\beta(k))=(\alpha'(h),\beta'(k))=\psi(\alpha',\beta')(h,k) \quad \forall (h,k)\in H\times K$$

De donde deducimos que $\alpha=\alpha'$ y que $\beta=\beta'$, por lo que ψ es inyectiva.

□

Teorema 1.29. *Sean H,K dos grupos finitos tales que $\operatorname{mcd}(|H|,|K|)=1$, entonces:*

1. *$\forall L<H\times K$, $\exists_1 H_1<H, K_1<K$ de forma que:*

$$L=H_1\times K_1$$

Es decir, todo subgrupo de $H\times K$ se descompone de forma única como un subgrupo de H por un subgrupo de K.

2. *La aplicación $\psi : Aut(H) \times Aut(K) \to Aut(H \times K)$ de la Proposición 1.28 es un isomorfismo.*

Demostración. Veamos los dos resultados:

1. Sea $L < H \times K$, consideramos:

   $$H_1 = p_1(L) < H \qquad K_1 = p_2(L) < K$$

   Por la Proposición 1.28, tenemos que $H_1 \times K_1 < H \times K$, y por la definición de L que $L < H_1 \times K_1$, ya que si $(h,k) \in L$:

   $$\begin{aligned} h &= p_1(h,k) \in H_1 \\ k &= p_2(h,k) \in K_1 \end{aligned}$$

   Basta ver que $H_1 \times K_1 < L$.

   $$\begin{tikzcd} H \arrow[d, dash] & H \times K \arrow[l, "p_1"'] \arrow[r, "p_2"'] \arrow[d, dash] & K \arrow[d, dash] \\ H_1 & L & K_1 \end{tikzcd}$$

   Para ello, si notamos $n = |H|$ y $m = |K|$, por el Teorema de Bezout $\exists r, s \in \mathbb{Z}$ de forma que:

   $$nr + ms = 1$$

   - En primer lugar, si $h \in H_1$, por su definición y la sobreyectividad de p_1, existirá $(h,k) \in L$ de forma que $p_1(h,k) = h$, de donde:

     $$L \ni (h,k)^{ms} = (h^{ms}, k^{ms}) = \left(h^{1-nr}, 1\right) = (h,1)$$

     Por lo que: $\{(h,1) \mid h \in H_1\} \subseteq L$.
   - Ahora, si $k \in K_1$, por su definición y la sobreyectividad de p_2, existirán $(h,k) \in L$ de forma que $p_2(h,k) = k$, de donde:

     $$K \ni (h,k)^{nr} = (h^{nr}, k^{nr}) = (1, k^{1-ms}) = (1,k)$$

     Por lo que: $\{(1,k) \mid k \in K_1\} \subseteq L$.

   Sea ahora $(h,k) \in H_1 \times K_1$, tenemos que:

   $$(h,k) = (h,1)(1,k) \in L$$

   De donde $H_1 \times K_1 < L$. Finalmente, la construcción que hemos realizado nos da la unicidad, pues si existen otros subconjuntos $H_2 < H$ y $K_2 < K$ de forma que $L = H_2 \times K_2$, tendríamos que:

   $$H_2 = p_1(L) = H_1 \qquad K_2 = p_2(L) = K_1$$

2. Basta ver que $\psi : Aut(H) \times Aut(K) \to Aut(H \times K)$ es sobreyectiva, es decir, que dada $\varphi \in Aut(H \times K)$, podemos encontrar $\alpha \in Aut(H)$ y $\beta \in Aut(K)$ de forma que $\varphi = \psi(\alpha, \beta)$. Para ello, mostraremos el proceso para encontrar α y el proceso para encontrar β es análogo.

   En primer lugar, lo que hacemos es estudiar la imagen por φ del conjunto $H \times \{1\} < H \times K$. Como φ es un homomorfismo, sabemos que la imagen de $H \times \{1\}$ por φ será un subgrupo de $H \times K$, a quien llamaremos G_1:

$$G_1 = \varphi(H \times \{1\}) < H \times K$$

   Por el apartado 1, sabemos que podemos encontrar únicos $H_1 < H$ y $K_1 < K$ de forma que $G_1 = H_1 \times K_1$. Además, por ser φ biyectiva, tendremos que:

$$|H| = |H \times \{1\}| = |H_1 \times K_1| = |H_1||K_1|$$

   Veamos que $|K_1| = 1$. Para ello, si $m = |K_1| \in \mathbb{N}$:

   - De la igualdad $|H| = |H_1|m$ deducimos que m divide a $|H|$.
   - Como $m = |K_1|$ y $K_1 < K$, por el Teorema de Lagrange tenemos también que m divide a $|K|$.

   Por la definición del máximo común divisor, concluimos que m divide a $\text{mcd}(|H|, |K|) = 1$, de donde $m = 1$ y $K_1 = \{1\}$.

   Finalmente, de la igualdad $|H| = |H_1|$ concluimos que $H = H_1$. Hemos probado que:

$$\varphi(H \times \{1\}) = H \times \{1\}$$

   Definimos ahora $\alpha : H \to H$ dada por:

$$\alpha(h) = p_1(\varphi(i_1(h))) \qquad \forall h \in H$$

   Está claro que α es un homomorfismo, como composición de homomorfismos.

   - Para la sobreyectividad de α, como $\varphi(H \times \{1\}) = H \times \{1\}$, tenemos que:

$$\alpha(H) = p_1(\varphi(i_1(H))) = p_1(\varphi(H \times \{1\})) = p_1(H \times \{1\}) = H$$

   - Para la inyectividad, sean $h_1, h_2 \in H$ de forma que:

$$p_1(\varphi(h_1, 1)) = \alpha(h_1) = \alpha(h_2) = p_2(\varphi(h_2, 1))$$

     Como $\varphi(H \times \{1\}) = H \times \{1\}$, sabemos que existirán $h_1', h_2' \in H$ de forma que:

$$\varphi(h_1, 1) = (h_1', 1) \qquad \varphi(h_2, 1) = (h_2', 1)$$

     Por lo que:

$$h_1' = p_1(h_1', 1) = p_1(\varphi(h_1, 1)) = p_1(\varphi(h_2, 1)) = p_1(h_2', 1) = h_2'$$

     De donde concluimos que α es inyectiva.

De forma análoga a lo que hicimos anteriormente, puede probarse que:

$$\varphi(\{1\} \times K) = \{1\} \times K$$

Y definiendo $\beta : H \times K \to H \times K$ dada por:

$$\beta(k) = p_2(\varphi(i_2(k))) \qquad \forall k \in K$$

Tenemos que $\beta \in Aut(K)$.

Con estos dos automorfismos, veamos que $\psi(\alpha, \beta) = \varphi$:

$$\psi(\alpha, \beta)(h, k) = (\alpha(h), \beta(k)) = (p_1(\varphi(h, 1)), p_2(\varphi(1, k))) \overset{(*)}{=} \varphi(h, k) \qquad \forall (h, k) \in H \times K$$

Donde en $(*)$ hemos usado que existirán $h' \in H$ y $k' \in K$ de forma que:

$$\varphi(h, 1) = (h', 1) \qquad \varphi(1, k) = (1, k')$$

Por lo que:

$$\begin{aligned}(p_1(\varphi(h, 1)), p_2(\varphi(1, k))) &= (p_1(h', 1), p_2(1, k')) = (h', k') \\ &= (h', 1)(1, k') = \varphi(h, 1)\varphi(1, k) = \varphi(h, k)\end{aligned}$$

□

El punto 2 de este último Teorema será un resultado que usemos en numerosos ejercicios, sin considerar de forma explícita la aplicación ψ pero usando el isomorfismo $Aut(H) \times Aut(K) \cong Aut(H \times K)$ bajo las hipótesis apropiadas.

1.5.1. Producto directo interno de una familia de subgrupos

Teorema 1.30. *Sea $\{G_\lambda \mid \lambda \in \Lambda\}$ una familia de grupos de forma que para cada $\lambda \in \Lambda$ tenemos $H_\lambda < G_\lambda$, entonces:*

$$\prod_{\lambda \in \Lambda} H_\lambda < \prod_{\lambda \in \Lambda} G_\lambda$$

Teorema 1.31. *Sea $\{G_\lambda \mid \lambda \in \Lambda\}$, entonces existe un monomorfismo*

$$\prod_{\lambda \in \Lambda} Aut(G_\lambda) \longrightarrow Aut\left(\prod_{\lambda \in \Lambda} G_\lambda\right)$$

1.5.2. Producto directo interno de una familia finita de subgrupos

Teorema 1.32. *Sea G un grupo y $G_1, \ldots, G_n < G$ n subgrupos de G, definimos la aplicación $\phi : G_1 \times \ldots \times G_n \to G$ dada por:*

$$\phi(g_1, \ldots, g_n) = g_1 \cdot \ldots \cdot g_n \qquad \forall (g_1, \ldots, g_n) \in G_1 \times \ldots \times G_n$$

Son equivalentes:

i) ϕ *es un isomorfismo.*

ii) $G_k \lhd G$ $\forall k \in \{1, \dots, n\}$, $G_1 \dots G_n = G$ *y* $(G_1 \dots G_{k-1}) \cap G_k = \{1\}$ *para todo* $k \in \{2, \dots, n\}$.

iii) $g_k g_h = g_h g_k$ *para todo* $g_h \in G_h$, $g_k \in G_k$ *con* $k \neq h$, $G = G_1 \vee \dots \vee G_n$ *y* $(G_1 \dots G_{k-1}) \cap G_k = \{1\}$ *para todo* $k \in \{2, \dots, n\}$.

iv) $g_k g_h = g_h g_k$ *para todo* $g_h \in G_h$, $g_k \in G_k$ *con* $k \neq h$, *y todo elemento* $g \in G$ *se expresa de manera única como* $g = g_1 \dots g_n$ *con* $g_k \in G_k$ *para todo* $k \in \{1, \dots, n\}$.

Teorema 1.33. *Sean* $G_1, \dots, G_n$ *n grupos de forma que sus órdenes son primos relativos dos a dos, si* $G = G_1 \times \dots \times G_n$, *entonces:*

1. $\exists_1 H_k < G_k$ *tal que* $L = H_1 \times \dots \times H_k$ *para todo* $L < G$.

2. $Aut(G_1) \times \dots \times Aut(G_n) \cong Aut(G)$.

1.6. Producto directo de grupos cíclicos

Notación. Cuando hablemos del producto directo de dos grupos cíclicos, en vez de usar $\times$, usaremos como notación $\oplus$, ya que normalmente usamos la notación aditiva al trabajar con grupos cíclicos.

Ejemplo. En primer lugar, hemos de tener en cuenta que el producto directo de dos grupos cíclicos no tiene por qué ser en general un grupo cíclico. Veamos varios ejemplos de que no se cumple:

1. Supongamos que $\mathbb{Z} \oplus \mathbb{Z}$ es cíclico. En cuyo caso, tenemos que $\exists (r, s) \in \mathbb{Z} \oplus \mathbb{Z}$ de forma que:
$$\mathbb{Z} \oplus \mathbb{Z} = \langle (r, s) \rangle$$
De donde para $(1, 0) \in \mathbb{Z} \oplus \mathbb{Z}$ $\exists n \in \mathbb{Z}$ de forma que:
$$(1,0) = n(r,s) \Longrightarrow \left\{ \begin{array}{l} nr = 1 \\ ns = 0 \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} n, r \in \{\pm 1\} \\ s = 0 \end{array} \right. \Longrightarrow (r,s) = \left\{ \begin{array}{l} (-1,0) \\ (1,0) \end{array} \right.$$
Sin embargo, $(0, 1) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$, por lo que $\exists m \in \mathbb{Z}$ de forma que:
$$(0,1) = m(1,0) \Longrightarrow \left\{ \begin{array}{l} m = 0 \\ 1 = 0 \end{array} \right.$$
Contradicción, por lo que $\mathbb{Z} \oplus \mathbb{Z}$ no es cíclico.

2. Ahora, supongamos que $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ es cíclico, con lo que de la misma forma, $\exists (r, s) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$ de modo que:
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \langle (\overline{r}, \overline{s}) \rangle$$
Sin embargo:
$$O(\overline{r}, \overline{s}) = \operatorname{mcm}(O(\overline{r}), O(\overline{s})) = \left\{ \begin{array}{l} 1 \Longleftrightarrow \overline{r} = \overline{s} = 0 \\ 2 \Longleftrightarrow \overline{r} \neq 0 \vee \overline{s} \neq 0 \end{array} \right.$$

En $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ no hay elementos de orden 4, pero:

$$|\mathbb{Z}_2 \oplus \mathbb{Z}_2| = 4$$

Un grupo de orden 4 que no tiene elementos de orden 4 nunca puede ser cíclico. De hecho, tendremos que $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong V$.

3. Un ejemplo de dos grupos cíclicos cuyo producto directo es cíclico es:

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3$$

Que tiene orden $|\mathbb{Z}_2 \oplus \mathbb{Z}_3| = |\mathbb{Z}_2||\mathbb{Z}_3| = 6$. Si consideramos $(\overline{1}, \overline{1})$, tenemos que:

$$O(\overline{1}, \overline{1}) = \text{mcm}(O(\overline{1}_2), O(\overline{1}_3)) = \text{mcm}(2, 3) = 6$$

Por lo que $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle(\overline{1}, \overline{1})\rangle$. Notemos que el motivo de que esto haya sucedido es porque 2 y 3 son primos relativos.

Proposición 1.34. *Si G y H son grupos cíclicos finitos, entonces:*

$$G \oplus H \text{ es cíclico } \Longleftrightarrow \text{mcd}(|G|, |H|) = 1$$

Demostración. Veamos las dos implicaciones. Para ello, supongamos que:

$$G = \langle x\rangle, \quad O(x) = n, \quad H = \langle y\rangle, \quad O(y) = m$$

Para ciertos $x \in G$ y $y \in H$.

$\Longleftarrow$) Si $\text{mcd}(n, m) = 1$, entonces $\text{mcm}(n, m) = nm$, de donde:

$$O(x, y) = \text{mcm}(O(x), O(y)) = nm = |G||H| = |G \times H|$$

Tenemos un grupo de orden nm que contiene a un elemento de orden nm, luego $G \times H = \langle(x, y)\rangle$.

$\Longrightarrow$) Si $G \oplus H = \langle(a, b)\rangle$, entonces:

$$O(a, b) = \text{mcm}(O(a), O(b)) = nm = |G||H| = |G \times H|$$

Como $O(a) \mid n$ y $O(b) \mid m$, llegamos a que $O(a) = n$ y $O(b) = m$. Finalmente:

$$\text{mcd}(n, m) = \frac{nm}{\text{mcm}(n, m)} = \frac{nm}{nm} = 1$$

□

Corolario 1.34.1. *Si $G_1, G_2, \ldots, G_n$ son n grupos cíclicos finitos, entonces:*

$$\bigoplus_{k=1}^{n} G_k \text{ cíclico} \Longleftrightarrow \text{mcd}(|G_i|, |G_j|) = 1 \quad \forall i, j \in \{1, \ldots, n\}, i \neq j$$

Ejemplo. Aplicando esta última proposición:

- $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{30}$.
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ no es cíclico.

Ejemplo. Podemos demostrar que S_3 no es producto directo interno de subgrupos propios. Por reducción al absurdo, si fuera producto directo, como $|S_3| = 6$, tendría un subgrupo de orden 2 y otro de orden 3, ambos isomorfos a C_2 y C_3. Si tuviera dos subgrupos propios cuyo producto propio fuera él mismo, tendríamos:

$$S_3 \cong C_2 \oplus C_3 \cong C_6$$

Pero S_3 no es cíclico, hemos llegado a una contradicción.

2. Grupos resolubles

Este Capítulo trata sobre los grupos resolubles, propiedad interesante de un grupo que tendrá numerosas aplicaciones, como por ejemplo en la solución de ecuaciones con radicales. Sin embargo, la definición de grupo resoluble ha de esperar, pues primero tenemos que hacer un estudio de las "series de un grupo".

2.1. Series de un grupo

Definición 2.1 (Serie de un grupo)**.** Sea G un grupo, una serie de G es una cadena de subgrupos $G_0, G_1, \dots, G_r$ de forma que:

$$G = G_0 > G_1 > G_2 > \dots > G_r = \{1\}$$

En dicho caso, diremos que la serie tiene longitud r.

Ejemplo. En S_3, podemos considerar la serie:

$$S_3 > A_3 > \{1\}$$

Definición 2.2 (Refinamiento)**.** Sea G un grupo, si consideramos sobre él dos series:

$$G = H_0 > H_1 > \dots > H_s = \{1\} \tag{2.1}$$

$$G = G_0 > G_1 > G_2 > \dots > G_r = \{1\} \tag{2.2}$$

Diremos que (2.2) es un refinamiento de (2.1) si todo grupo que aparece en (2.1) también aparece en (2.2). Ha de ser por tanto $r \geqslant s$.

Decimos que (2.2) es un refinamiento propio de (2.1) si en (2.1) hay grupos que no aparecen en (2.2). En dicho caso, ha de ser $r > s$.

Ejemplo. En A_4, podemos considerar la serie:

$$A_4 > V > \{1\}$$

Un refinamiento propio de la misma es:

$$A_4 > V > \langle (1\ 2)(3\ 4) \rangle > \{1\}$$

Definición 2.3 (Series propia y normal)**.** Sea G un grupo, si consideramos una serie de G:

$$G = G_0 > G_1 > \dots > G_r = \{1\}$$

- Decimos que es una serie propia si todas las inclusiones entre los subgrupos son propias, es decir, si $G_{k+1} \subsetneq G_k$, para todo $k \in \{0, \ldots, r-1\}$.
- Decimos que es una serie normal si todas las relaciones de subgrupo que aparecen son de subgrupo normal, es decir, si $G_k \triangleright G_{k+1}$, para todo $k \in \{0, \ldots, r-1\}$.

  En dicho caso, lo notaremos como:

$$G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_r = \{1\}$$

Ejemplo. Todas las series anteriores eran series normales propias:

$$S_3 \triangleright A_3 \triangleright \{1\}$$
$$A_4 \triangleright V \triangleright \{1\}$$
$$A_4 \triangleright V \triangleright \langle(1\ 2)(3\ 4)\rangle \triangleright \{1\}$$

Definición 2.4 (Índices y factores de una serie)**.**
Dada una serie normal de un grupo G:

$$G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_r = \{1\}$$

- Llamamos factores de la serie a los grupos cocientes:

$$G_{k-1}/G_k \qquad \forall k \in \{1, \ldots, r\}$$

- Llamamos índices de la serie a los correspondientes órdenes de los factores.

  Si $i_k = [G_{k-1} : G_k]$ para todo $k \in \{1, \ldots, r\}$, entonces notaremos:

$$G = G_0 \overset{i_1}{\triangleright} G_1 \overset{i_2}{\triangleright} \ldots \overset{i_r}{\triangleright} G_r = \{1\}$$

Ejemplo. Por ejemplo, en la serie:

$$S_3 \triangleright A_3 \triangleright \{1\}$$

Tenemos los factores:

$$S_3/A_3 \cong C_2 \qquad A_3/\{1\} \cong A_3$$

Y los índices:

$$S_3 \overset{2}{\triangleright} A_3 \overset{3}{\triangleright} \{1\}$$

Si consideramos ahora la serie:

$$A_4 \overset{3}{\triangleright} V \overset{2}{\triangleright} \langle(1\ 2)(3\ 4)\rangle \overset{2}{\triangleright} \{1\}$$

Los factores que obtenemos son:

$$A_4/V \qquad V/\langle(1\ 2)(3\ 4)\rangle \qquad \langle(1\ 2)(3\ 4)\rangle/\{1\}$$

Definición 2.5. Sea G un grupo, si tenemos dos series normales de G:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$
$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_s = \{1\}$$

Se dice que son isomorfas si $r = s$ y existe $\sigma \in S_r$ de forma que:

$$G_{k-1}/G_k \cong H_{\sigma(k)-1}/H_{\sigma(k)} \qquad \forall k \in \{1, \ldots, r\}$$

Ejemplo. En $\mathbb{Z}/24\mathbb{Z}$ consideramos las series:

$$\mathbb{Z}/24\mathbb{Z} \rhd 2\mathbb{Z}/24\mathbb{Z} \rhd 4\mathbb{Z}/24\mathbb{Z} \rhd 8\mathbb{Z}/24\mathbb{Z} \rhd 24\mathbb{Z}/24\mathbb{Z} = \{0\}$$
$$\mathbb{Z}/24\mathbb{Z} \rhd 3\mathbb{Z}/24\mathbb{Z} \rhd 6\mathbb{Z}/24\mathbb{Z} \rhd 12\mathbb{Z}/24\mathbb{Z} \rhd 24\mathbb{Z}/24\mathbb{Z} = \{0\}$$

Que son dos series isomorfas, para la permutación $\sigma = (1\ 2\ 3\ 4)$, ya que:

$$\mathbb{Z}/24\mathbb{Z} \overset{2}{\rhd} 2\mathbb{Z}/24\mathbb{Z} \overset{2}{\rhd} 4\mathbb{Z}/24\mathbb{Z} \overset{2}{\rhd} 8\mathbb{Z}/24\mathbb{Z} \overset{3}{\rhd} 24\mathbb{Z}/24\mathbb{Z} = \{0\}$$
$$\mathbb{Z}/24\mathbb{Z} \overset{3}{\rhd} 3\mathbb{Z}/24\mathbb{Z} \overset{2}{\rhd} 6\mathbb{Z}/24\mathbb{Z} \overset{2}{\rhd} 12\mathbb{Z}/24\mathbb{Z} \overset{2}{\rhd} 24\mathbb{Z}/24\mathbb{Z} = \{0\}$$

2.1.1. Series de composición

Pasamos ya al estudio de las series que nos interesarán, que son las series de composición.

Definición 2.6 (Serie de composición)**.** Una serie de G se dice que es una serie de composición de G si es una serie normal sin refinamientos normales propios.
En una serie de composición, será usual referirnos a los factores como factores de composición, y a los índices como índices de composición.

Ejemplo. Ejemplos de series de composición son:

- Las dos series anteriores sobre $\mathbb{Z}/24\mathbb{Z}$ son series de composición, ya que los índices no permiten introducir más subgrupos a la serie.
- Anteriormente vimos que la serie $A_4 \rhd V \rhd \{1\}$ no era de composición, ya que podíamos refinarla más: $A_4 \rhd V \rhd \langle(1\ 2)(3\ 4)\rangle \rhd \{1\}$, aunque ya esta última sí que es de composición.

Por ahora, para estudiar si una serie es o no de composición, no nos queda otra que realizar un análisis exhaustivo del retículo de subgrupos del grupo que consideremos, analizando solo las inclusiones de subgrupos que sean normales, algo que mostraremos en los siguientes ejemplos.

Ejemplo. Sea $\mathbb{K}$ un cuerpo, sobre $\mathrm{GL}_2(\mathbb{K})$ consideramos las matrices triangulares superiores:

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{K}^*, b \in \mathbb{K} \right\}$$

Que tiene infinitos elementos y no es un grupo abeliano, ya que:

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

Si consideramos ahora:

$$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{K} \right\}$$

Tenemos que $T \rhd U \rhd \{1\}$ es una serie de composición.

Notemos que:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$$

Si ahora para $n > 2$ cogemos como T el conjunto de las matrices triangulares superiores y luego cogemos:

$$N = \{\text{matrices triangulares superiores con diagonal de ceros}\}$$
$$U_r = I + N^r$$

Tomando potencias los elementos van subiendo en la diagonal. Podemos considerar:

$$T \rhd U_1 \rhd U_2 \rhd \ldots \rhd U_n = I$$

Ejemplo. Tratamos de buscar cuántas series de composición hay en los siguientes grupos:

- En S_3, recordamos que el retículo de subgrupos que teníamos era:

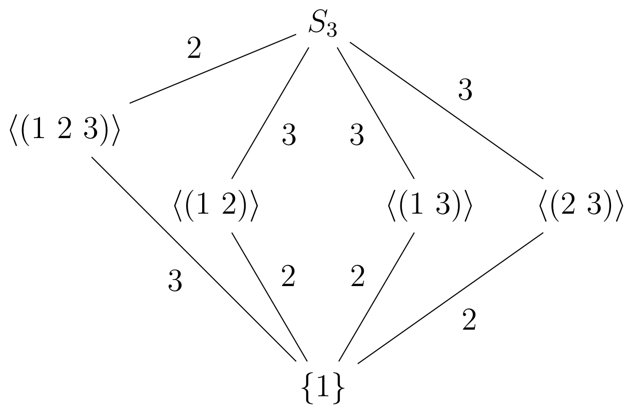


Figura 2.1: Diagrama de Hasse para los subgrupos de S_3.

  Como $A_3 = \langle(1\ 2\ 3)\rangle \lhd S_3$ (por tener índice 2) y ningún otro subgrupo de S_3 es normal salvo el trivial, la única serie de composición de S_3 es:

$$S_3 \rhd A_3 \rhd \{1\}$$

- En D_4:

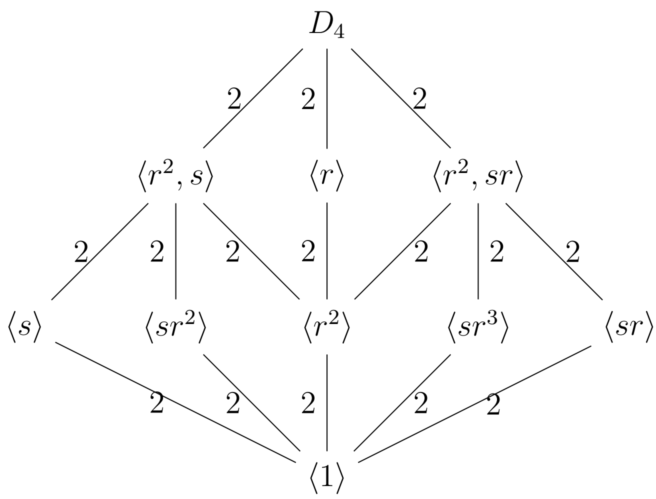
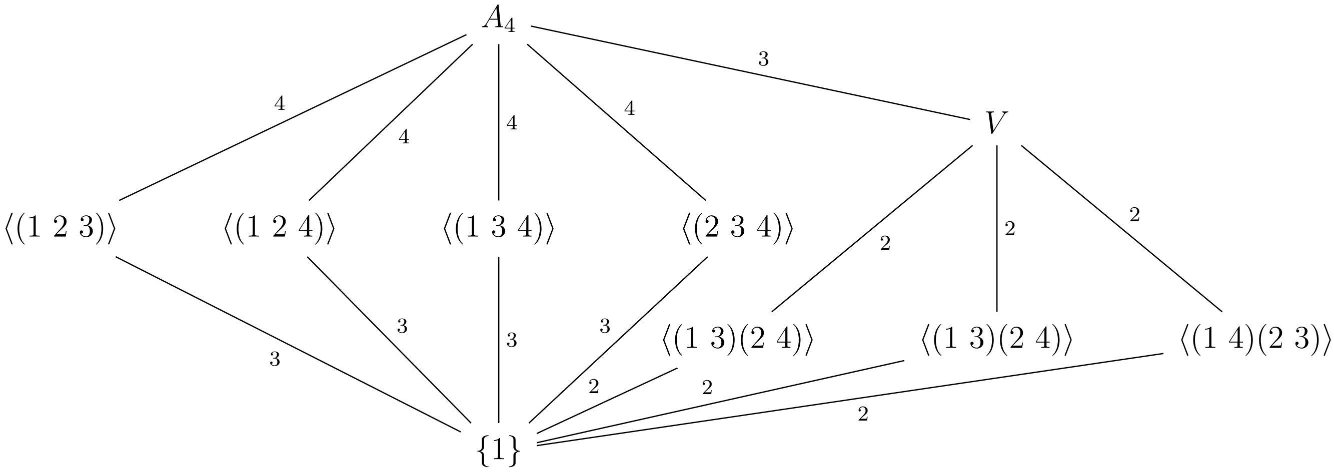


Figura 2.2: Diagrama de Hasse para los subgrupos de D_4.

Como todos los índices del grafo son 2, todas las relaciones de inclusión mostradas en el grafo en realidad son relaciones de normalidad ($\lhd$), por lo que tenemos 7 series de composición distintas (una por cada forma que tengamos de llegar desde D_4 hasta $\{1\}$ en el grafo mediante caminos descendientes):

$$\begin{gathered}
D_4 \rhd \langle r^2, s\rangle \rhd \langle s\rangle \rhd \{1\}\\
D_4 \rhd \langle r^2, s\rangle \rhd \langle sr^2\rangle \rhd \{1\}\\
D_4 \rhd \langle r^2, s\rangle \rhd \langle r^2\rangle \rhd \{1\}\\
D_4 \rhd \langle r^2, sr\rangle \rhd \langle r^2\rangle \rhd \{1\}\\
D_4 \rhd \langle r^2, sr\rangle \rhd \langle sr\rangle \rhd \{1\}\\
D_4 \rhd \langle r^2, sr\rangle \rhd \langle sr^3\rangle \rhd \{1\}\\
D_4 \rhd \langle r\rangle \rhd \langle r^2\rangle \rhd \{1\}
\end{gathered}$$

- Para A_4:

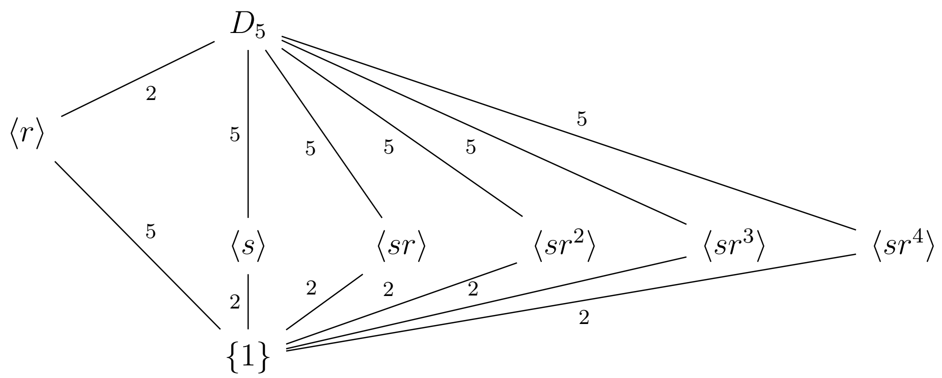


Como $V \lhd A_4$, tenemos como series de composición:

$$\begin{gathered}
A_4 \rhd V \rhd \langle (1\ 2)(3\ 4) \rangle \rhd \{1\} \\
A_4 \rhd V \rhd \langle (1\ 3)(2\ 4) \rangle \rhd \{1\} \\
A_4 \rhd V \rhd \langle (2\ 3)(2\ 3) \rangle \rhd \{1\}
\end{gathered}$$

Además, como ninguna de las relaciones $\langle (i\ j\ k) \rangle < A_4$ es normal, no tenemos más series de composición.

- En $D_5 = \langle r, s \mid r^5 = s^2 = 1, sr = r^4 s \rangle$ tenemos:



Solo tenemos la serie de composición:

$$D_5 \rhd \langle r \rangle \rhd \{1\}$$

Ya que D_5 no tiene más subgrupos normales, a parte del trivial.

- En el grupo de los cuaternios:

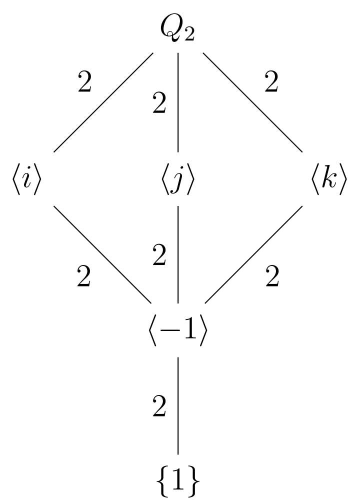


Figura 2.3: Diagrama de Hasse para los subgrupos del grupo de los cuaternios.

Como todas las aristas del grafo están numeradas con índice 2, todas las relaciones de subgrupo son normales, por lo que tenemos 3 series de composición, una por cada camino posible:

$$\begin{gathered}
Q_2 \rhd \langle i \rangle \rhd \langle -1 \rangle \rhd \{1\} \\
Q_2 \rhd \langle j \rangle \rhd \langle -1 \rangle \rhd \{1\} \\
Q_2 \rhd \langle k \rangle \rhd \langle -1 \rangle \rhd \{1\}
\end{gathered}$$

- En $S_3 \times \mathbb{Z}_2$: Por una parte, en S_3 teníamos una única serie de composición:

  $$S_3 \rhd A_3 \rhd \{1\}$$

  Y en $\mathbb{Z}_2$ la única opción a considerar es $\mathbb{Z}_2 \rhd \{0\}$. Podemos considerar ahora las series de composición resultantes de considerar todas las combinaciones:

  $$\begin{gathered}
S_3 \times \mathbb{Z}_2 \rhd S_3 \times \{0\} \rhd A_3 \times \{0\} \rhd \{(1,0)\} \\
S_3 \times \mathbb{Z}_2 \rhd A_3 \times \mathbb{Z}_2 \rhd A_3 \times \{0\} \rhd \{(1,0)\} \\
S_3 \times \mathbb{Z}_2 \rhd A_3 \times \mathbb{Z}_2 \rhd \{1\} \times \mathbb{Z}_2 \rhd \{(1,0)\}
\end{gathered}$$

  Que obtenemos primero variando algunos y luego otras. Esto es posible ya que el producto de subgrupos es subgrupo del producto, como vimos en la Proposición 1.28.

  Sin embargo, como $\text{mcd}(6,2) = 2 \neq 1$, el Teorema 1.29 no puede asegurarnos que todos los subgrupos de $S_3 \times \mathbb{Z}_2$ sean producto de subgrupos, y de hecho vamos a tener que hay subgrupos del producto que no son producto de subgrupos de cada coordenada, por lo que tendremos otra serie de composición, que tendrá la forma:

  $$S_3 \times \mathbb{Z}_2 \overset{2}{\rhd} H_1 \overset{2}{\rhd} H_2 \overset{3}{\rhd} \{1\}$$

  Con $H_1, H_2 < S_3 \times \mathbb{Z}_2$ que no especificaremos pero diremos que $H_1 \cong S_3$ y $H_2 \cong A_3$.

Definición 2.7 (Grupo simple)**.** Un grupo G se dice simple si no es trivial y no tiene subgrupos normales propios

Ejemplo. $\mathbb{Z}_3$ es un grupo simple, ya que su retículo de subgrupos es:

$$\begin{array}{c} \mathbb{Z}_3 \\ | \\ \{0\} \end{array}$$

Un resultado que veremos luego (el Teorema de Abel) nos dirá que los grupos A_n para $n \geqslant 5$ son grupos simples.

Resultados sobre series de composición

Proposición 2.1. *Un grupo abeliano finito es simple si y solo si es un grupo cíclico de orden primo.*

Demostración. Por doble implicación:

$\Longleftarrow$) Si G es cíclico de orden primo, no va a tener subgrupos propios, por lo que será simple.

$\Longrightarrow$) Si G es abeliano, entonces todos sus subgrupos serán normales. Si es simple, no tendrá subgrupos propios (ya que si no serían normales, luego no sería simple). Sea $1 \neq x \in G$, sabemos que $\langle x \rangle < G$, de donde ($\{1\} \neq \langle x \rangle$ y G no tiene subgrupos propios) $G = \langle x \rangle$, por lo que G es cíclico.

Si $|G| = nm$, entonces $\{1\} \neq \langle x^m \rangle < G$, por lo que G tendría subgrupos propios, luego no sería simple. Por tanto, $|G|$ ha de ser primo.

□

Ejemplo. Estudiando un poco el caso de grupos cíclicos infinitos, $\mathbb{Z}$ no es simple, ya que tiene subgrupos propios (que además son normales, por ser $\mathbb{Z}$ abeliano).

Proposición 2.2 (Caracterización de series de composición)**.** *Sea G un grupo, una serie normal es de composición si y solo si sus factores son grupos simples.*

Demostración. Consideramos una serie normal de longitud r:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$

Y demostraremos que la serie no es de composición si y solo si tiene un factor que no es un grupo simple:

$\Longrightarrow$) Si la serie no es de composición, podemos encontrar $H < G$ de forma que la serie:

$$G = G_0 \rhd \ldots \rhd G_{k-1} \rhd H \rhd G_k \rhd \ldots \rhd G_r = \{1\}$$

Sea un refinamiento normal propio de la serie de partida. Si consideramos la proyección al cociente de los grupos:

$$G_{k-1} \rhd H \rhd G_k$$

Llegamos a que:

$$p_*(G_{k-1}) = G_{k-1}/G_k \rhd p_*(H) = H/G_k \rhd p_*(G_k) = \{G_k\}$$

Y ninguna de estas inclusiones es una igualdad, ya que:

- Si $G_{k-1}/G_k = H/G_k$, entonces $G_{k-1} = H$ y el refinamiento anterior no era propio.
- Si $H/G_k = \{G_k\}$, entonces $H = G_k$ y el refinamiento anterior no era propio.

En definitiva, hemos encontrado un subgrupo normal propio de G_{k-1}/G_k, por lo que este factor no es un grupo simple.

$\Longleftarrow$) Si existe $k \in \{1, \ldots, r\}$ de forma que G_{k-1}/G_k no es un grupo simple, entonces dicho grupo tendrá un subgrupo propio normal suyo:

$$\{G_k\} = \{1\} \neq H \lhd G_{k-1}/G_k$$

Si usamos el Tercer Teorema de Isomorfía considerando la proyección al cociente $p_k : G_{k-1} \to G_{k-1}/G_k$, tenemos que:

$$p_k^*(H) \lhd G_{k-1}$$

Además, como $H < G_{k-1}/G_k$, tendremos que $G_k \in H$, luego:

$$G_k = \ker(p_k) = p_k^*(\{G_k\}) \subseteq p_k^*(H) \lhd G_{k-1}$$

Y por ser $G_k \lhd G_{k-1}$, deducimos que también $G_k \lhd p_k^*(H)$. Hemos encontrado un subgrupo normal de G que estaría entre G_k y G_{k-1}:

$$G = G_0 \rhd \ldots \rhd G_{k-1} \rhd p_k^*(H) \rhd G_k \rhd \ldots \rhd G_r = \{1\}$$

Además, este refinamiento de la serie normal es propio, ya que:

- Si fuese $p_k^*(H) = G_k$, tendríamos que $H = \{G_k\}$.
- Si fuese $p_k^*(H) = G_{k-1}$, tendríamos que $H = G_{k-1}/G_k$.

Ambos casos son imposibles, puesto que H era un subgrupo propio de G_{k-1}/G_k. Hemos encontrado un refinamiento normal propio de la serie de partida, por lo que esta no era de composición.

□

Proposición 2.3. *Todo grupo finito tiene una serie de composición.*

Demostración. Sea G un grupo finito, distinguimos casos:

- Si G es simple o trivial, entonces no tiene subgrupos normales propios, por lo que tiene una única serie de composición:

  $$G \rhd \{1\}$$

- Si $|G| = p$ primo, vimos en la Proposición **??** que entonces G es cíclico, y la Proposición 2.1 nos dice que G es simple, por lo que estamos en el caso anterior.

- Si $|G|$ no es primo y G no es simple, por inducción sobre $n = |G|$, suponemos que es cierto para todo grupo H con $|H| < |G|$ (observemos que el punto anterior nos sirve como caso base).

  Como G es finito, tiene un número finito de subgrupos, entre los que podemos encontrar (por ser G no simple) G_1, un subgrupo normal propio maximal[1] de G. Como $|G_1| < |G|$ (G_1 es subgrupo propio), por hipótesis de inducción tenemos una serie de composición para G_1:

  $$G_1 \rhd G_2 \rhd \ldots \rhd G_r = \{1\}$$

  Además, como G_1 era el subgrupo normal maximal de G, sabemos que no existe $H \lhd G$ con $G_1 \lhd H \lhd G$, por lo que la serie:

  $$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_r = \{1\}$$

  Es de composición. □

[1]Es decir, que no existe $G_1 \neq K \lhd G$ con $G_1 \lhd K$.

Teorema 2.4 (de Refinamiento de Schreier)**.** *Sea G un grupo, dos series normales de G tienen refinamientos isomorfos.*

Demostración. Consideramos dos series normales de G:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_{i-1} \rhd G_i \rhd \ldots \rhd G_r = \{1\} \tag{2.3}$$

$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_{j-1} \rhd H_j \rhd \ldots \rhd H_s = \{1\} \tag{2.4}$$

Fijado $i \in \{1, \ldots, r\}$, tenemos $G_i \lhd G_{i-1} < G$, y para todo $j \in \{1, \ldots, s\}$ tenemos $H_j \lhd H_{j-1} < G$, donde podemos aplicar el primer apartado del Cuarto Teorema de Isomorfía, obteniendo la siguiente relación entre los grupos:

$$G_{ij} = G_i(H_j \cap G_{i-1}) \lhd G_i(H_{j-1} \cap G_{i-1}) = G_{ij-1} \qquad \forall j \in \{1, \ldots, s\}$$

En los casos extremos (es decir, en $j = 0$ y $j = s$), tendremos:

$$\begin{aligned} G_{i0} &= G_i(H_0 \cap G_{i-1}) = G_iG_{i-1} = G_{i-1} \\ G_{is} &= G_i(H_s \cap G_{i-1}) = G_i\{1\} = G_i \end{aligned}$$

De esta forma, tenemos para todo $i \in \{1, \ldots, r\}$ que:

$$G_{i-1} = G_{i0} \rhd G_{i1} \rhd \ldots \rhd G_{is-1} \rhd G_{is} = G_i$$

Que podemos meter en todos los eslabones de la serie (2.3):

$$\begin{aligned} G = G_0 = G_{10} \rhd G_{11} \rhd \ldots \rhd G_{1s} = G_1 = G_{20} \rhd G_{21} \rhd \ldots \rhd G_{2s} = G_2 = G_{30} \rhd \ldots \\ \ldots \rhd G_{r-1s} = G_{r-1} = G_{r0} \rhd \ldots \rhd G_{rs} = G_r = \{1\} \end{aligned}$$

Obteniendo un refinamiento de longitud $r(s + 1) - (r - 1) = rs + 1$:
En cada eslabón (teníamos r) hemos metido $s + 1$ eslabones, de los que se repetían ($G_{is} = G_{i+1,0}$, para $i \in \{0, \ldots, r - 1\}$) $r - 1$ eslabones.

Si repetimos el procedimiento para la serie (2.4), fijado $j \in \{1, \ldots, s\}$, para todo $i \in \{0, \ldots, r\}$ podemos aplicar el primer apartado del Cuarto Teorema de Isomorfía, obteniendo que:

$$H_{ij} = H_j(G_i \cap H_{j-1}) \lhd H_j(G_{i-1} \cap H_{j-1}) = H_{i-1j} \qquad \forall i \in \{1, \ldots, r\}$$

En los casos extremos tendremos:

$$\begin{aligned} H_{0j} &= H_{j-1} \\ H_{rj} &= H_j \end{aligned}$$

Por lo que para todo $j \in \{1, \ldots, s\}$, tenemos:

$$H_{j-1} = H_{0j} \rhd H_{1j} \rhd \ldots \rhd H_{r-1j} \rhd H_{rj} = H_j$$

Y podemos obtener un refinamiento de (2.4) al igual que hicimos antes, metiendo la cadena superior entre cada uno de los eslabones de la serie original:

$$G = H_0 = H_{01} \rhd H_{11} \rhd \ldots \rhd H_{r1} = H_1 = H_{02} \rhd H_{12} \rhd \ldots \rhd H_{r2} = G_2 = H_{03} \rhd \ldots$$
$$\ldots \rhd H_{rs-1} = H_{s-1} = H_{0s} \rhd H_{1s} \rhd \ldots \rhd H_{rs} = H_s = \{1\}$$

Que tiene longitud $s(r+1) - (s-1) = rs + 1$, al igual que antes.

Ahora, por la segunda parte del Cuarto Teorema de Isomorfía, tenemos que:

$$\frac{G_{ij-1}}{G_{ij}} = \frac{G_i(H_j \cap G_{i-1})}{G_i(H_j \cap G_{i-1})} \cong \frac{H_j(G_{i-1} \cap H_{j-1})}{H_j(G_i \cap H_{j-1})} = \frac{H_{i-1j}}{H_{ij}}$$

Por lo que los dos refinamientos encontrados son isomorfos. □

Ejercicio. Se pide calcular un refinamiento isomorfo aplicando el método de Schreier a las dos siguientes series normales:

$$G = G_0 \rhd G_1 \rhd G_2 \rhd G_3 = \{1\}$$
$$G = H_0 \rhd H_1 \rhd H_2 = \{1\}$$

Teorema 2.5 (Jordan-Holder)**.** *Si un grupo G admite una serie de composición, cualquier serie normal puede refinarse a una serie de composición.*

Además, dos series de composición de un mismo grupo son isomorfas siempre.

Demostración. Tomamos una serie de composición de G:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$

Y también una serie normal de G:

$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_s = \{1\}$$

Por el Teorema de Schreier (la serie de composición es normal), existe un refinamiento de ambos isomorfo. Sin embargo, como la primera serie es de composición, su refinamiento coincide con ella misma. Para la segunda serie, obtendremos un refinamiento isomorfo a la primera:

$$G = \overline{G_0} \rhd \overline{G_1} \rhd \ldots \rhd \overline{G_r} = \{1\}$$

Por tanto, tendremos que:

$$G_k/G_{k+1} \cong \overline{G}_K/\overline{G}_{k+1} \qquad \forall k \in \{0, \ldots, r-1\}$$

Como la primera serie era de composición, los factores G_k/G_{k+1} son simples, y como esta propiedad se conserva por isomorfismos (compruébese), los factores $\overline{G}_k/\overline{G}_{k+1}$ también serán simples, de donde deducimos que el refinamiento de la serie normal que hemos encontrado es de composición. □

Con este último Teorema de Jordan-Holder se tiene claro ya el interés en las series de composición, ya que cada grupo admite un única (salvo isomorfismos) serie de composición.

Podemos pensar en calcular series de composición de un grupo conocida una serie de composición en un grupo isomorfo, resultado que podemos esperar que sea cierto (y que de hecho vamos a probar a continuación); sin embargo, el recíproco no es cierto en general: si tenemos dos series de composición isomorfas, una de un grupo G y otra de otro grupo K, en general G y K no van a ser isomorfos.

Ejemplo. Por ejemplo, anteriormente vimos en un ejemplo que la única serie de composición que podemos considerar en S_3 es:

$$S_3 \overset{2}{\rhd} A_3 \overset{3}{\rhd} \{1\}$$

En $\mathbb{Z}_6$, que no es isomorfo a S_3 por ser abeliano, si observamos su retículo:

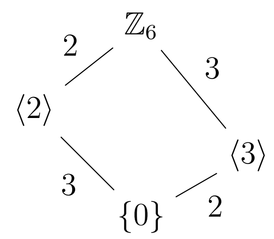


Figura 2.4: Diagrama de Hasse para los subgrupos de $\mathbb{Z}_6$.

Vemos que una serie de composición de $\mathbb{Z}_6$ es:

$$\mathbb{Z}_6 \overset{2}{\rhd} \langle 2\rangle \overset{3}{\rhd} \{0\}$$

Además, sabemos ahora por el Teorema de Jordan-Holder que $\mathbb{Z}_6$ no tiene más series de composición, ya que la otra posibilidad sería la serie:

$$\mathbb{Z}_6 > \langle 3\rangle > \{0\}$$

Pero como esta no es isomorfa a la primera y sabemos que todas las series de composición de un mismo grupo son isomorfas, sabemos que esta segunda no es de composición. Vemos finalmente que las series:

$$S_3 \overset{2}{\rhd} A_3 \overset{3}{\rhd} \{1\}$$
$$\mathbb{Z}_6 \overset{2}{\rhd} \langle 2\rangle \overset{3}{\rhd} \{0\}$$

son isomorfas. Para ello, basta ver que:

$$S_3/A_3 \cong \mathbb{Z}_2 \cong Z_6/\langle 2\rangle$$
$$A_3/\{1\} \cong A_3 \cong \mathbb{Z}_3 \cong \langle 2\rangle \cong \langle 2\rangle/\{0\}$$

Proposición 2.6. *Sean G y K dos grupos isomorfos, entonces todas las series de composición de G son isomorfas a todas las series de composición de K.*

Demostración. Como todas las series de composición de G son isomorfas entre sí y todas las series de composición de K también (por el Teorema de Jordan-Holder), basta ver que hay una serie de composición de G que es isomorfa a una serie de composición de K. Para ello, como $G \cong K$, ha de existir un isomorfismo de grupos $f : G \to K$. Sea

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$

una serie de composición de G, tendremos entonces que sus factores son de composición, luego grupos simples. □

El objetivo principal de esta asignatura es clasificar los grupos finitos. Como estos grupos van a tener series de composición cuyos factores serán grupos simples, nos centraremos en clasificar los grupos simples, para luego clasificar los grupos finitos.

La teoría de clasificación de grupos simples comenzó en 1960 y fue completada en 2004, con una demostración de 15000 páginas en lo que se conoce como el "Teorema enorme". En la demostración intervinieron matemáticos como Gorestein (1923 - 1992). Esta clasificación de los grupos simples se hizo en:

- 18 familias infinitas de grupos simples.
- 26 grupos simples, llamados grupos esporádicos.

  Como curiosidad, el grupo esporádico más pequeño tiene orden 7920 y el más grande, 10^{54}.

Cualquier grupo finito simple pertenece a una de estas 18 familias, o es isomorfo a alguno de los 26 grupos esporádicos.

Entre las 18 familias de grupos simples destacamos 2, que son las que nos interesan por ahora:

- Los grupos cíclicos de orden primo, que ya hemos demostrado que se tratan de grupos simples.
- Los grupos alternados A_n con $n \geqslant 5$.

Veremos ahora este segundo resultado, en el ya prometido Teorema de Abel.

Teorema 2.7 (de Abel)**.** *A_n es simple, para $n \geqslant 5$.*

Demostración. Sea $\{1\} \neq N \lhd A_n$, veamos que ha de ser $N = A_n$. En la Proposición **??** vimos que dado[2] $j \in X_n \setminus \{1, 2\}$, teníamos que:

$$A_n = \langle (1\ 2\ j) \rangle$$

Y la demostración terminará viendo que N contiene a un elemento de esta forma. Bajo estas hipótesis, sabemos que va a existir (por ser N finito) $1 \neq \sigma \in N$, la permutación de N que mueve menos elementos. Por ser σ par (estamos en A_n), ha de mover más de dos elementos. Veamos que mueve exactamente 3:

1. Si σ es producto de ciclos disjuntos de longitud 2: supongamos que σ mueve, al menos, los elementos x_1, x_2, x_3 (distintos entre sí), con lo que podemos escribir:

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

   Sea $\tau = (x_3\ x_4\ x_5)$ para ciertos $x_4, x_5 \in X_n$ distintos de x_1, x_2, x_3 y distintos entre sí, definimos:

   $$\sigma_1 = (x_3\ x_4\ x_5)\sigma(x_3\ x_4\ x_5)^{-1} \in N$$

   σ_1 está en N por ser $N \lhd A_n$. Si consideramos:

   $$[\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1} = \sigma_1\sigma^{-1} \in N$$

[2]Donde $X_n = \{1, 2, \ldots, n\}$.

- Supongamos que σ mueve a x_5, en cuyo caso:

$$\sigma = (x_1\ x_2)(x_3\ x_4)(x_5\ \sigma(x_5))\dots$$
$$\sigma_1 = (x_1\ x_2)(x_3\ \sigma(x_5))(x_4\ x_5)\dots$$

  Con lo que:

$$[\tau, \sigma] = (x_3\ \sigma(x_5))(x_4\ x_5)(x_3\ x_4)(x_5\ \sigma(x_5))$$

  Luego $[\tau, \sigma]$ deja fijos a x_1 y x_2 y mueve a los mismos que movía σ. Por ello, $[\tau, \sigma] \in N$ y $[\tau, \sigma]$ mueve menos elementos que σ, contradicción, que viene de suponer que σ mueve a x_5.
- Si suponemos que σ no mueve a x_5:

$$\sigma_1 = (x_1\ x_2)(x_4\ x_5)$$

  Tenemos:

$$[\tau, \sigma] = (x_3\ x_5\ x_4)$$

  Que mueve menos elementos que σ, contradicción.

Por tanto, σ no puede ser producto de transposiciones, ya que llegamos a contradicciones.

2. Si σ tiene un ciclo de longitud mayor o igual que 3 en el que mueve a x_1, x_2 y x_3:

$$\tau = (x_3\ x_4\ x_5)$$
$$\sigma_1 = \tau\sigma\tau^{-1} \in N$$

Supongamos que σ mueve más de 3 elementos, por lo que mueve al menos (por ser una permutación par) 5. En dicho caso:

$$\sigma_1 = (x_1\ x_2\ x_4\ \dots) \neq \sigma$$

Por lo que:

$$[\tau, \sigma] = \sigma_1\sigma^{-1} \in N$$

Y $[\tau, \sigma]$ deja fijos a los mismos que σ y a x_2. En dicho caso, tenemos que $[\tau, \sigma]$ mueve menos que σ.

En definitiva, concluimos que σ contiene a un ciclo de longitud 3, a saber: $(i\ j\ k)$, todos ellos elementos distintos.

- Si $i, j, k, 1, 2$ son todos distintos:

$$(1\ i)(2\ j)(i\ j\ k)(1\ i)(2\ j) = (1\ 2\ k) \in N$$

- Si $i = 1$ y $j, k, 2$ fueran distintos, $\exists h$ distinto de los anteriores de forma que:

$$(2\ j)(k\ h)(1\ j\ k)(2\ j)(k\ h) = (1\ 2\ h) \in N$$

- Si $i = 2$ y $j, k, 1$ fueran distintos, $\exists h$ distintos de los anteriores de forma que:

$$\dots = (1\ 2\ h) \in N$$

En definitiva, N contiene al generador de A_n, de donde:

$$N = \langle (1\ 2\ j) \rangle = A_n$$

□

2.2. Grupos resolubles

Antes de pasar con la definición de grupos resolubles, hemos de respasar ciertos conceptos relacionados con la operación de conmutador que ya definimos sobre los elementos de G, recordamos que era la aplicación $[\cdot,\cdot] : G \times G \to G$ dada por:

$$[x, y] = xy(yx)^{-1} = xyx^{-1}y^{-1} \qquad \forall x, y \in G$$

2.2.1. Preliminares

Sobre el conmutador solo vimos la Proposición 1.26, que nos decía que dados dos elementos h, k de un grupo G:

$$hk = kh \iff [h, k] = 1$$

Proposición 2.8. *Sea G un grupo y $x, y \in G$, se verifican:*

i) $[x, y]^{-1} = [y, x]$.

ii) $z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}]$, $\forall z \in G$.

Demostración. Veamos cada apartado:

i) Basta con ver:

$$[x, y][y, x] = xy(yx)^{-1}yx(xy)^{-1} = xy(xy)^{-1} = 1$$

ii) Sea $z \in G$, basta aplicar la definición del conmutador:

$$\begin{aligned} z[x, y]z^{-1} &= zxy(yx)^{-1}z^{-1} = zxy(x^{-1}y^{-1}z^{-1}) \\ [zxz^{-1}, zyz^{-1}] &= zxz^{-1}zyz^{-1}(zyz^{-1}zxz^{-1})^{-1} = zxyz^{-1}(zx^{-1}y^{-1}z^{-1}) \\ &= zxy(x^{-1}y^{-1}z^{-1}) \end{aligned}$$

□

Proposición 2.9. *Sea G un grupo, el conjunto:*

$$\langle [x, y] \mid x, y \in G \rangle$$

es un subgrupo normal de G.

Demostración. Llamando Λ a dicho conjunto, para ver que es un subgrupo, si $a, b \in \Lambda$, entonces $\exists n, m \in \mathbb{Z}$ de forma que:

$$a = ([x, y])^n \qquad b = ([x, y])^m$$

En dicho caso:

$$ab^{-1} = ([x, y])^n([x, y])^{-m} = ([x, y])^{n-m}$$

Con $n - m \in \mathbb{Z}$, por lo que $ab^{-1} \in \Lambda$, de donde $\Lambda < G$.

Ahora, para ver que $\Lambda \lhd G$, sea $a \in \Lambda$, existirán $n \in \mathbb{Z}$, $x, y \in G$ de forma que $a = ([x, y])^n$. Sea $z \in G$:

- Si $n = 1$:
$$z[x,y]z^{-1} = [zxz^{-1}, zyz^{-1}] \in \Lambda$$
- Si $n = -1$:
$$z([x,y])^{-1}z^{-1} = z[y,x]z^{-1} = [zyz^{-1}, zxz^{-1}] \in \Lambda$$
- Supuesto para $n-1$, para n:
$$z([x,y])^n z^{-1} = z[x,y]z^{-1}z([x,y])^{n-1}z^{-1} = (z[x,y]z^{-1})(z([x,y])^{n-1}z^{-1})$$
Con $z[x,y]z^{-1} \in \Lambda$ por ser $[x,y] \in \Lambda$ y $z([x,y])^{n-1}z^{-1} \in \Lambda$ por hipótesis de inducción. Como $\Lambda < G$, concluimos que $z([x,y])^n z^{-1} \in \Lambda$. Escribiendo $m = -n$:
$$\left(z([x,y])^m z^{-1}\right)^{-1} = z^{-1}([x,y])^{-m}z \in \Lambda$$
Por ser $\Lambda < G$, concluimos que $z([x,y])^m z^{-1} \in \Lambda$.

En definitiva, $\Lambda \lhd G$. □

Definición 2.8 (Subgrupo conmutador)**.** Sea G un grupo, llamamos subgrupo conmutador de G al subgrupo:
$$[G,G] = \langle [x,y] \mid x,y \in G \rangle$$
Observemos que como $hk = kh \iff [h,k] = 1$, este grupo está generado por los conmutadores de los elementos que no conmutan entre sí:
$$[G,G] = \langle [x,y] \mid xy \neq yx \rangle$$

Proposición 2.10. *Sea G un grupo, $G/[G,G]$ es abeliano. Más aún, es el menor subgrupo normal de G que hace que el cociente sea abeliano. Es decir, si $N \lhd G$:*
$$G/N \text{ es abeliano} \iff [G,G] < N$$
$G/[G,G]$ recibe el nombre de grupo abelianizado de G.

Demostración. Si demostramos la doble implicación, como $[G,G] < [G,G]$, tendremos que $G/[G,G]$ es abeliano, por lo que solo tenemos que probar esto:

$\Longrightarrow$) Si consideramos la proyección al cociente $p : G \to G/N$, sea $a \in [G,G]$, entonces existirán $n \in \mathbb{Z}$ y $x,y \in G$ de forma que:
$$a = ([x,y])^n$$
Si calculamos la imagen de a por p (que recordamos que es un homomorfismo):
$$\begin{aligned} p(a) = (p([x,y]))^n = \left(p\left(xy(yx)^{-1}\right)\right)^{-1} &= (p(xy))^n (p(yx))^{-n} \\ &\overset{(*)}{=} (p(x))^n (p(y))^n (p(y))^{-n} (p(x))^{-n} = 1 \end{aligned}$$
Donde en $(*)$ hemos usado que G/N es abeliano. Tenemos que $a \in \ker(p) = N$.

$\Longleftarrow$) Sean $x, y \in G$, entonces:

$$xy(yx)^{-1} = [x, y] \in [G, G] < N$$

Pero:

$$(xN)(yN) = xyN = yxN = (yN)(xN) \Longleftrightarrow xy(yx)^{-1}N = N$$

Por lo que $(xN)(yN) = (yN)(xN)$, para todos $x, y \in G$.

$\square$

Corolario 2.10.1. *Si G es un grupo:*

$$G \text{ abeliano} \Longleftrightarrow [G, G] = \{1\}$$

Demostración. Como $G \cong G/\{1\}$:

$$G \text{ abeliano} \Longleftrightarrow G/\{1\} \text{ abeliano} \Longleftrightarrow [G, G] < \{1\} \Longleftrightarrow [G, G] = \{1\}$$

$\square$

Ejercicio. Se pide comprobar que:

$$[A_3, A_3] = \{1\}$$
$$[S_3, S_3] = A_3$$
$$[A_4, A_4] = V$$

2.2.2. Definición

Definición 2.9 (Serie derivada)**.** La serie derivada de un grupo G es la cadena de subgrupos normales:

$$G = G^0 \rhd G' \rhd G'' \rhd \ldots \rhd G^{(k)} \rhd \ldots$$

Donde:

$$G^{(k+1)} = [G^{(k)}, G^{(k)}]$$

De esta forma, el subgrupo $G' = [G, G]$ recibe el nombre de subgrupo derivado de G, o primer derivado de G.

Un grupo G se dice resoluble si existe un índice k de forma que $G^{(k)} = \{1\}$. Es decir, la serie derivada de G alcanza el $\{1\}$.

Ejemplo. Veamos que:

- Si G es abeliano, entonces G es resoluble:

$$G' = [G, G] = \{1\}$$

Por lo que la serie derivada es:

$$G \rhd G' = \{1\}$$

- S_3 es resoluble:

$$\begin{aligned} S_3' &= [S_3, S_3] = A_3 \\ S_3'' &= A_3' = [A_3, A_3] = \{1\} \end{aligned}$$

Y la serie derivada es:

$$S_3 \rhd A_3 \rhd \{1\}$$

- A_4 es resoluble:

$$\begin{aligned} A_4' &= [A_4, A_4] = V \\ A_4'' &= V' = [V, V] = \{1\} \end{aligned}$$

Y la serie derivada es:

$$A_4 \rhd V \rhd \{1\}$$

- S_4 es resoluble, ya que $S_4' = [S_4, S_4] = A_4$ y ya tenemos la serie de A_4:

$$S_4 \rhd A_4 \rhd V \rhd \{1\}$$

En general, si G es un grupo cuyo grupo derivado es resoluble, entonces G será resoluble.

- A_5 no es resoluble:

$$A_5' = [A_5, A_5] \neq \{1\}$$

Ya que A_5 no es abeliano, pero como A_5 es simple, no tiene subgrupos normales propios, con lo que $A_5' = A_5$. La serie derivada será:

$$A_5 \rhd A_5 \rhd A_5 \rhd \dots$$

En general, ningún grupo no abeliano y simple es resoluble.

- S_n no es resoluble para $n \geqslant 5$, ya que:

$$[S_n, S_n] = A_n \qquad \forall n \geqslant 3$$

Y como ya vimos lo que le pasa a A_n para $n \geqslant 5$, la serie derivada de S_n será:

$$S_n \rhd A_n \rhd A_n \rhd \dots$$

Teorema 2.11 (Caracterización de grupos resolubles para grupos finitos)**.**
Si G es un grupo finito, son equivalentes:

i) *G es resoluble.*

ii) *G tiene una serie normal con factores abelianos.*

iii) *Los factores de composición de G son cíclicos de orden primo.*

iv) *G tiene una serie normal con factores cíclicos.*

Demostración. Veamos todas las implicaciones:

$i) \Longrightarrow ii)$ Si G es resoluble, la serie derivada será de la forma:

$$G = G^0 \rhd G' \rhd \ldots \rhd G^{(r)} = \{1\}$$

Que es una serie normal con factores abelianos, ya que los factores son de la forma:

$$G^{(k-1)}/G^{(k)} = G^{(k-1)}/\left[G^{(k-1)}, G^{(k-1)}\right]$$

Que ya vimos en la Proposición 2.10 que siempre era un grupo abeliano.

$ii) \Longrightarrow iii)$ Si tenemos una serie normal con factores abelianos:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_s = \{1\}$$

Por el Teorema de Jordan-Holder, podemos refinarla a una serie de composición, donde nos fijaremos ahora en lo que pasa entre dos eslabones de la serie original:

$$\ldots \rhd G_r \rhd H_{r1} \rhd H_{r2} \rhd \ldots \rhd H_{rs} \rhd G_{r+1} \rhd \ldots$$

Por hipótesis los factores son abelianos, es decir, los grupos:

$$G_{k-1}/G_k \qquad \forall k \in \{1, \ldots, s\}$$

son abelianos. Por consiguiente, como todo subgrupo de un grupo abeliano también es abeliano, tenemos que los siguientes cocientes también son abelianos:

$$H_{r1}/G_{r+1} \quad H_{r2}/G_{r+1} \quad \cdots \quad H_{rs}/G_{r+1} \quad < \quad G_r/G_{r+1}$$

Por tanto, los factores:

$$\begin{aligned}
G_r/H_{r1} &\cong \frac{G_r/G_{r+1}}{H_{r1}/G_{r+1}} \\
H_{r1}/H_{r2} &\cong \frac{H_{r1}/G_{r+1}}{H_{r2}/G_{r+1}} \\
&\vdots \\
H_{rs-1}/H_{rs} &\cong \frac{H_{rs-1}/G_{r+1}}{H_{rs}/G_{r+1}}
\end{aligned}$$

Son abelianos, por ser isomorfos a un cociente de un grupo abeliano. En definitiva, todos los factores de composición son abelianos, finitos y simples (por ser factores de composición), luego son cíclicos de orden primo, por la Proposición 2.1.

$iii) \Longrightarrow iv)$ Como las series de composición son, en particular, series normales, cualquier[3] serie de composición de G será normal con factores cíclicos.

[3]Gracias al Teorema de Jordan-Holder.

iv) $\Longrightarrow$ *i)* Consideramos una serie normal con factores cíclicos (luego abelianos):

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}$$

Veamos que $G^{(k)} < G_k$, para todo $k \in \{1, \ldots, r\}$: como G_{k-1}/G_k es abeliano por ser un factor, entonces por la Proposición 2.10:

$$[G_{k-1}, G_{k-1}] = G^{(k)} < G_k$$

En particular:

$$G^{(r)} < G_r = \{1\}$$

Y tenemos ya que la serie derivada alcanza el mínimo:

$$G = G^0 \rhd G' \rhd \ldots \rhd G^{(r)} = \{1\}$$

Por lo que G es resoluble.

□

Ejemplo. Aplicaciones del Teorema son:

- Vimos ya que S_4 era resoluble, veámoslo de otra forma:

  $$S_4 \rhd A_4 \rhd V \rhd \{1\}$$

  Es una serie normal con factores cíclicos abelianos:

  $$S_4/A_4 \qquad A_4/V \qquad V/\{1\}$$

- En D_n:

  $$D_n \rhd \langle r \rangle \rhd \{1\}$$

  Es una serie normal con factores cíclicos abelianos, luego D_n es resoluble.

Una estrategia muy usada a la hora de comprobar si un grupo es resoluble o no es buscar si nuestro grupo tiene un subgrupo normal resoluble que haga que el cociente sea resoluble, con lo que podemos aplicar el tercer apartado de la siguiente Proposición:

Proposición 2.12. *Se verifica que:*

i) *Todo subgrupo de un grupo resoluble es resoluble.*

ii) *Todo cociente de un grupo resoluble es resoluble.*

iii) *Si $N \lhd G$ y N y G/N son resolubles, entonces G es resoluble.*

Demostración. Veamos cada una:

i) Supongamos que la serie derivada de G es:

$$G = G^0 \rhd G' \rhd G'' \rhd \ldots \rhd G^{(r)} = \{1\}$$

Si $H < G$, entonces $H^{(k)} < G^{(k)}$ para todo $k \in \{1, \ldots, r\}$. Como tenemos que $G^{(r)} = \{1\}$, tendremos que $H^{(r)} = \{1\}$, por lo que H es resoluble.

ii) Supuesto que G es resoluble con la serie anterior, consideramos $N \lhd G$. Por inducción, tendremos que:

$$\left({}^{G}\!/\!_{N}\right)^{(k)} = {}^{G^{(k)}N}\!/\!_{N}$$

Y como $G^{(r)} = \{1\}$, entonces:

$$\left({}^{G}\!/\!_{N}\right)^{(r)} = \{1\} \Longrightarrow G/N \text{ resoluble}$$

iii) Si $N \lhd G$ y G/N son resolubles: por ser G/N resoluble, entonces $\exists s$ de forma que:

$${}^{G^{(s)}N}\!/\!_{N} = \left({}^{G}\!/\!_{N}\right)^{(s)} = \{1\}$$

En dicho caso:

$$G^{(s)} < N$$

Y como N es resoluble, $\exists t$ de forma que $N^{(t)} = \{1\}$. En dicho caso:

$$G^{(s+t)} < N^{(t)} = \{1\}$$

□

Para concluir los resultados sobre grupos resolubles, veamos qué pasa con el producto de grupos resolubles:

Corolario 2.12.1. *Cualquier producto finito de grupos resolubles es resoluble.*

Demostración. Suponiendo que G_1 y G_2 son resolubles, cada uno tendrá su serie derivada. Tenemos:

$$G_2 \cong \{1\} \times G_2 < G_1 \times G_2$$

Con $\{1\} \times G_2$ resoluble por ser isomorfo a G_2. Además, $\{1\} \times G_2 \lhd G_1 \times G_2$. Busquemos el cociente:

$${}^{G_1 \times G_2}\!/\!_{\{1\} \times G_2} \cong G_1$$

Que es resoluble, por lo que usando el apartado 3 de la Proposición superior, concluimos que $G_1 \times G_2$ es resoluble.

Por hipótesis de inducción, fijada una coordenada, movemos todas las demás. □

3. $G-$conjuntos y p-grupos

Definición 3.1. Sea G un grupo y X un conjunto no vacío, una acción[1] de G sobre X es una aplicación:

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

Que verifica:

i) $ac(1,x) = x \quad \forall x \in X$.

ii) $ac(g, ac(h,x)) = ac(gh,x) \quad \forall x \in X, \quad \forall g,h \in G$.

En dicho caso, diremos que G actúa[2] (o que opera) sobre X.

Si G actúa sobre X, diremos que este conjunto X es el $G-$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 notación, 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>:
$$\begin{array}{rrcl} ac: & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & x \end{array}$$

2. Si tenemos una acción $ac : G \times X \to X$ y $H < G$, podemos considerar la <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 $X = \{1, \ldots, n\}$ y $G = S_n$, la acción natural de S_n sobre X será la acción $ac : S_n \times X \to X$ dada por:

$$ac(\sigma, k) = {}^{\sigma}k = \sigma(k) \qquad \forall \sigma \in S_n, k \in X$$

Proposición 3.1. *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* $\text{Perm}(X)$.

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:
$$\begin{array}{rccl} \phi : & G & \longrightarrow & \text{Perm}(X) \\ & g & \longmapsto & \phi(g) \end{array}$$
Donde $\phi(g)$ es una aplicación $\phi(g) : X \longrightarrow X$ dada por:
$$\phi(g)(x) = {}^{g}x \qquad \forall x \in X$$
Veamos en primer lugar que ϕ está bien definida, es decir, que $\phi(g) \in \text{Perm}(X)$ para cada $g \in G$. Para ello, veamos antes que ϕ cumple:
  - $\phi(1) = id_X$, ya que la aplicación $x \mapsto ac(1, x)$ es la aplicación identidad en X, por ser ac una acción de G sobre X.
  - $\phi(g)\phi(h) = \phi(gh)$, ya que al evaluar en cualquier $x \in G$:
  $$(\phi(g)\phi(h))(x) = \phi(g)(\phi(h)(x)) = \phi(g)({}^{h}x) = {}^{g}({}^{h}x) \overset{(*)}{=} {}^{gh}x = \phi(gh)(x)$$
  Donde en $(*)$ hemos usado que ac es una acción de G sobre X.

  Ahora, veamos que dado $g \in G$, la aplicación $\phi(g)$ es biyectiva (es decir, está en $\text{Perm}(X)$), 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 $\phi(g) \in \text{Perm}(X)$, para todo $g \in G$ y la aplicación ϕ está bien definida.

  Además, por las dos propiedades anteriores, tenemos que ϕ es un homomorfismo de grupos.

- Sea $\phi : G \to \text{Perm}(X)$ 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:
$$\begin{aligned} ac(1, x) &= \phi(1)(x) = x \qquad \forall x \in X \\ ac(g, ac(h, x)) &= \phi(g)(\phi(h)(x)) = \phi(gh)(x) = ac(gh, x) \qquad \forall x \in X, \quad \forall g, h \in G \end{aligned}$$

□

Definición 3.2 (Representación por permutaciones)**.** Sea G un grupo y X un conjunto no vacío, si tenemos una acción de G sobre X, el homomorfismo ϕ dado por esta acción según la Proposición 3.1 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, dadas 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 una acción $ac : G \times X \to X$ sobre un grupo G y un conjunto no vacío X que tiene asociada una representación por permutaciones ϕ, entonces la acción por restricción $ac : H \times X \to X$ tendrá asociada como representación por permutaciones el homomorfismo $\phi_H : H \to X$ 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 3.2 (Cayley)**.** *Todo grupo finito es isomorfo a un subgrupo de un grupo de permutaciones.*

Demostración. Sea G un grupo finito, consideramos la acción por traslación:

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

Y su representación por permutaciones, $\phi : G \to \text{Perm}(G)$ dado por:

$$\phi(g)(h) = gh \qquad \forall g \in G, \forall h \in G$$

Como la acción por traslación es una acción fiel, tendremos que $\ker(\phi) = \{1\}$ y aplicando el Primer Teorema de Isomorfía sobre ϕ, obtenemos que:

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

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

Ejemplo. Podemos considerar las traslaciones de G sobre conjuntos especiales:

- La acción por traslación de G sobre $\mathcal{P}(G)$ será $ac : G \times \mathcal{P}(G) \to \mathcal{P}(G)$ dada por:
$$ac(g,A) = gA = \{ga \mid a \in A\} \subseteq G \qquad \forall A \in \mathcal{P}(G)$$
- Podemos también considerar la acción por traslación en el cociente por las clases laterales por la izquierda[3]: si $H < G$, consideramos el cociente de G sobre H por la izquierda y la acción $ac : G \times G/_H\sim \to G/_H\sim$ dada por:
$$ac(g, xH) = {}^g(xH) = gxH = \{gxh \mid h \in H\}$$

6. La <u>acción por conjugación</u> se define como $ac : G \times G \to G$ dada por:

$$ac(g,h) = {}^gh = ghg^{-1}$$

Que es una acción, ya que:

$$\begin{array}{ll} {}^1h = 1h1^{-1} = h & \forall h \in G \\ {}^g({}^hl) = g\,{}^hlg^{-1} = ghlh^{-1}g^{-1}ghl(gh)^{-1} = {}^{gh}l & \forall g,h,l \in G \end{array}$$

El homomorfismo asociado es:

$$\phi : G \to \text{Perm}(X)$$
$$\phi(g)(h) = ghg^{-1} \qquad \forall g,h \in G$$

Y a $\phi(g)$ lo llamábamos (en el ej 14 de la relación 4, φ_g) <u>automorfismo interior definido por G</u>, con imagen:

$$Im(\phi) = Int(G)$$

El núcleo en este caso es:

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

[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.

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:

$$ac(g, A) = {}^g A = gAg^{-1} = \{gag^{-1} \mid a \in A\} \subseteq G \qquad \forall A \in \mathcal{P}(G)$$

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:

$$ac(g, H) = {}^g H = gHg^{-1} < G$$

Ya que en la Proposición 1.1 vimos que gHg^{-1} era un subgrupo de G, al que llamaremos subgrupos conjugado de G.

3.1. Órbitas de un elemento

Definición 3.3 (Órbita)**.** Sea G un grupo y X un $G-$conjunto, definimos en X una relación de equivalencia $\sim$ dada por:

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

La clase de equivalencia de cada $x \in X$ se llama órbita de x, denotada por:

$$Orb(x) = \{y \in X \mid y = {}^g x, g \in G\}$$

Tenemos de esta forma que el conjunto cociente $X/\sim$ es el conjunto de las órbitas.

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 del H:

$$\begin{aligned}
Orb(1) &= \{k \in X \mid \exists \sigma \in H \text{ con } \sigma(k) = 1\} = \{1, 2, 3\} \\
Orb(2) &= \{1, 2, 3\} \\
Orb(3) &= \{1, 2, 3\} \\
Orb(4) &= \{4\}
\end{aligned}$$

  Donde pensamos en $Orb(k)$ como en los elementos de X desde los que podemos llegar a k con una permutación de H.

- 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 3.4. 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 3.5 (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 isontropía.

Proposición 3.3. *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 ${}^1 x = x$ 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:

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

  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 $gh \in Stab_G(x)$.

$\square$

Ejemplo. Si nuevamente sobre $X = \{1, 2, 3, 4\}$ volvemos a considerar la acción natural de S_4 sobre X:

- En $H = \langle(1\ 2\ 3)\rangle$:

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

- 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 3.4. *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, $G/_{Stab_G(x)}\sim$. Podemos considerar la aplicación $\phi : G/_{Stab_G}x \longrightarrow Orb(x)$ dada por:
$$\phi(gStab_G(x)) = {}^g x \qquad \forall g \in G$$

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

- Veamos que es sobreyectiva: sea $y \in Orb(x)$, vemos que $\exists g \in G$ 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 $gStab_G(x) = g'Stab_G(x)$.

□

Observación. La demostración es cierta sin suponer que G sea un grupo finito, salvo para concluir que $|Orb(x)|$ es un divisor de $|G|$.

Ejemplo. En el ejemplo de antes:

- Tenemos:
$$|Orb(1)| = \{1, 2, 3\}$$
  Y también que:
$$[H : Stab_H(1)] = \frac{|H|}{|Stab_H(1)|} \Longrightarrow |Stab_H(1)| = 1$$

Proposición 3.5. *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:
$$Stab_G(y) = gStab_G(x)g^{-1}$$

Para ello:

$\subseteq$) Sea $h \in Stab_G(x)$:
$${}^{ghg^{-1}} y = {}^{gh}\left({}^{g^{-1}} y\right) = {}^{gh} x = {}^{g}\left({}^{h} x\right) = {}^{g} x = y$$

Entonces, $ghg^{-1} \in Stab_G(y)$, por lo que $gStab_G(y)g^{-1} \subseteq Stab_G(y)$.

$\supseteq$) Sea ahora $h \in Stab_G(y)$:
$${}^{g^{-1}hg} x = x \Longrightarrow g^{-1}Stab_G(y)g \subseteq Stab_G(x)$$

Y multiplicando por g y g^{-1} tenemos la otra inclusión:
$$Stab_G(y) \subseteq gStab_G(x)g^{-1}$$

□

Definición 3.6. Sea G un grupo y X un $G-$conjunto, un elemento $x \in X$ se dice que es <u>fijo</u> 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 3.6. *Sea G un grupo y X un $G-$conjunto, si $x \in X$, entonces:*
$$x \in Fix(X) \Longleftrightarrow Orb(x) = \{x\} \Longleftrightarrow Stab_G(x) = G$$

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 $g \in G$, notamos $y = {}^g x$, pero entonces tenemos que:

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

Por lo que $y \in Orb(x) = \{x\}$, 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 $x \in Fix(X)$.

□

Observemos que si X es finito, $X/\sim = \{Orb(x_1), \ldots, Orb(x_n)\}$:

$$\begin{aligned} |X| = \sum_{k=1}^{n} |Orb(x_k)| = |Fix(X)| + \sum_{x_k \notin Fix(X)} |Orb(x_k)| \\ = |Fix(X)| + \sum_{x_k \notin Fix(X)} [G : Stab_G(x_k)] \end{aligned}$$

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

3.1.1. 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 ${}^g h = gh = k$.

$$\begin{aligned} Stab_G(h) &= \{g \in G \mid gh = {}^g h = h\} = \{1\} \qquad \forall h \in G \\ Fix(G) &= \{h \in G \mid gh = {}^g h = h \quad \forall g \in G\} = \emptyset \end{aligned}$$

3.1.2. 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 conjungos y vemos propiedades de estos que nos ayudarán a entender la acción.

Definición 3.7 (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 3.8 (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 3.7. *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:

$$\begin{aligned} xs = sx &\Longrightarrow xsx^{-1} = s \\ ys = sy &\Longrightarrow s = y^{-1}sy \qquad \forall s \in S \end{aligned}$$

  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 3.8. *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 $K < G$, $K \subseteq N_G(H) \Longleftrightarrow K < N_G(H)$. □

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:

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

Es la clase de conjugación de h en G (relación 4, ejercicio 30).

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

Centralizador de G en h (mismo ejercicio).

$$|Cl_G(h)| = [G : C_G(h)]$$

Y en el caso finito:

$$[G : C_G(h)] = \frac{|G|}{|C_G(h)|}$$

Por lo que $|Cl_G(h)|$ será un divisor de $|G|$.

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

Ejemplo. Calcular las clases de conjugación de D_4:

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} = \{s^i r^j \quad i = 0, 1 \; j = 0, 1, 2, 3\}$$

$$\begin{aligned} Cl_{D_4}(1) &= \{s^i r^j 1 (s^i r^j)^{-1}\} = \{1\} \\ Cl_{D_4}(r) &= \{s^i r^j r (s^i r^j)^{-1}\} = \{s^i r^j r r^{-j} s^{-i}\} = \{s^i r s^i\} = \{r, srs\} = \{r, r^3\} \\ Cl_{D_4}(r^2) &= \{s^i r^2 s^i\} = \{r^2\} \\ Cl_{D_4}(s) &= \{s, sr^2\} \\ Cl_{D_4}(sr) &= \{sr, sr^3\} \end{aligned}$$

$$|G| = |Z(G)| + \sum_{h \notin Z(G), h \in \Gamma} |Cl_G(h)| = |Z(G)| + \sum_{h \notin Z(G), h \in \Gamma} [G : Cl_G(h)]$$

(Γ indica que cogemos un elemento de cada clase) Es la fórmula de las clases de conjugación de G. Esta fórmula podemos generalizarla para cualquier subgrupo normal $H \lhd G$, en la fórmula de clases generalizada:

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

Donde Γ son las órbitas con más de un elemento (C_G es el centralizador de G).

3.1.3. Acción por conjugación sobre subgrupos

Sea G un grupo, la acción por conjugación sobre sus subgrupos viene definida[4] por $ac : G \times Subg(G) \to Subg(G)$ dada por:

$$ac(g, H) = {}^gH = gHg^{-1} \qquad \forall g \in G, \qquad \forall H \in Subg(G)$$

Veamos que:

$$Orb(H) = \{K \in Subg(G) \mid \exists g \in G \text{ con } gHg^{-1} = {}^gH = K\} = \{gHg^{-1} \mid g \in G\}$$

Es decir, la órbita de un subgrupo está formado por todos sus conjugados.

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

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

Esto se debe a que:

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

Donde la última equivalencia se tiene gracias a la Proposición 1.2, 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:

$$Fix(Subg(G)) = \{H < G \mid gHg^{-1} = {}^gH = H \quad \forall g \in G\} = \{H < G \mid H \lhd G\}$$

Coincide con el conjunto de subgrupos normales de G.

Si G es finito:

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

El número de grupos conjugados es un divisor de $|G|$.

3.2. $p-$grupos

Definición 3.9 ($p-$grupo)**.** Si p es un número primo, un grupo G se dice que es un $p-$grupo si todo elemento tiene orden una potencia de p.

Si G es un grupo, diremos que $H < G$ es un $p-$subgupo de G si H es un $p-$grupo.

Ejemplo. $\mathbb{Z}_8$ es un ejemplo de $2-$grupo.

Teorema 3.9 (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 subgrupo de orden p que será un $p-$subgrupo.*

[4] está bien definida gracias a la Proposición 1.1

Demostración. Si consideramos:

$$X = \{(a_1, a_2, \dots, a_p) \in G^p \mid a_1 a_2 \dots a_p = 1\}$$

Si $|G| = n$, entonces $|X| = n^{p-1}$, ya que elegimos libremente las $p-1$ primeras coordenadas (variación con repetición) y la última viene condicionada.

Sea $\sigma = (1\ 2\ \dots\ p) \subseteq S_p$ y:

$$H = \langle \sigma \rangle = \{1, \sigma, \dots, \sigma^{p-1}\} \subseteq S_p$$

Consideramos también la acción natural $ac : H \times X \to X$ dada por:

$$ac(\sigma^k, (a_1, a_2, \dots, a_p)) = \left(a_{\sigma^k(1)}, a_{\sigma^k(2)}, \dots, a_{\sigma^k(p)}\right) \qquad \forall k \in \{0, \dots, p-1\}$$

Veamos que:

$$|Orb(a_1, \dots, a_p)| = [H : Stab_H(a_1, \dots, a_p)] = \frac{|H|}{|Stab_H(a_1, \dots, a_p)|}$$

De donde tenemos que $|Orb(a_1, \dots, a_p)|$ es un divisor de $|H|$. En dicho caso, $|Orb(a_1, \dots, a_p)|$ será 1 o p, por ser $|H| = p$.

Sean r el número de órbitas con un elemento y s el número de órbitas con p elementos, entonces:

$$|X| = r + sp = n^{p-1}$$

Veamos ahora cómo son los elementos de $Orb(a_1, \dots, a_p)$:

$$Orb(a_1, \dots, a_p) = \{(a_1, \dots, a_p), (a_2, \dots, a_p, a_1), \dots, (a_p, a_1, \dots, a_{p-1})\}$$

La órbita será unitaria si y solo si $a_1 = a_2 = \dots = a_p$. Además, sabemos de la existencia de órbitas con un elemento ($r \geqslant 1$), como $Orb(1, 1, \dots, 1)$. Busquemos más: por hipótesis, $p \mid n$ y además $r = n^{p-1} - sp$, de donde $p \mid r$, por lo que $r \geqslant 2$ (ya que lo divide un primo).

En conclusión, $\exists a \in G \setminus \{1\}$ de forma que $Orb(a, a, \dots a)$ es unitaria, de donde $a^p = 1$, por lo que $O(a) = p$. Tenemos que $\langle a \rangle$ es un $p-$subgrupo de orden p. □

Corolario 3.9.1. *Sea G un grupo finito y p un número primo:*

$$G \textit{ es un } p\textit{−grupo} \iff \exists n \in \mathbb{N} \textit{ con } |G| = p^n$$

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 divie 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 $r = 1$ y $q = p$.

De esta forma, el único primo que divide a $|G|$ es p, luego $|G| = p^n$, para algún $n \in \mathbb{N}$. □

Si consideramos el centro de un $p-$grupo:

Teorema 3.10 (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, G no es trivial.
- Si G es no abeliano, entonces $Z(G) < G$ y por la fórmula anterior de las clases:

  $$p^n = |G| = |Z(G)| + \sum_{h \notin Z(G), h \in \Gamma} [G : C_G(h)]$$

  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 Γ.

  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 $|Z(G)| \geqslant p$.

□

Corolario 3.10.1. *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 (relación 4 ejercicio 4). En dicho caso, G coincide con su centro, $G = Z(G)$, luego $p^n = p^{n-1}$, <u>contradicción</u>.

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.
- Si $|Z(G)| = p$, no puede ser.
- Falta que $|Z(G)| = p^2$, luego $Z(G) = G$.

□

Este corolario nos dice que todos los grupos de orden p^2 son resolubles, por ser abelianos.

Teorema 3.11. *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 $p^l||G|$, 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 de orden divisible por p^k que sea de la forma $p^k m$ con $m < r$, es decir, $\exists H < G$ con $|H| = p^k$, veamos qué ocurre con G:

    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 $|K|$. Usando la Segunda Hipótesis de inducción, tendremos $H < K < G$ 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:

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

      Y como p divide a todos los $[G : C_G(h)]$, 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 $K \lhd G$ y podemos considerar el conjunto cociente G/K, con orden:

      $$|G/K| = \frac{|G|}{|K|} = \frac{|G|}{p}$$

      De donde $p^{k-1} \mid |G/K|$.
      Por la Primera Hipótesis de inducción, existe otro $L < G/K$ con $|L| = p^{k-1}$. Por el Tercer Teorema de Isomorfía, sabemos que $\exists K \lhd H < G$ de forma que:

      $$L = H/K$$

      De donde:

      $$|H| = |H/K||K| = p^{k-1}p = p^k$$

$\square$

Ejemplo. Por ejemplo, si G es un grupo de la forma $|G| = 24 = 2^3 \cdot 3$, tendremos un subgrupo de orden 2, otro de orden 4 y otro de orden 8.

3.2.1. $p-$subgrupos de Sylow

En 1872, un noruego llamado Peter LM Sylow (1832-1918) definió unos grupos y llegó a unos resultados sobre ellos.

Definición 3.10 ($p-$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 $|H| = p^k$.

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 $|Q| = 3$.

Corolario 3.11.1 (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.*

Demostración. Es evidente a partir del Teorema 3.11. $\square$

Observación. Si G es un grupo y p es un número primo con:

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

Y P es un $p-$grupo de Sylow con $P < H < G$, entonces usando la fórmula de los índices:

$$[G : P] = [G : H][H : P]$$

En dicho caso, $[H : P] \mid [G : P] = m$, por lo que p no dividirá a $[H : P]$. Además:

$$[G : H] \mid [G : P] \Longrightarrow p \nmid [G : H]$$

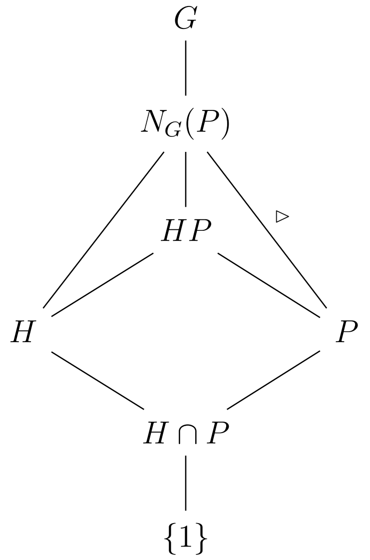
Es decir, si encontramos un grupo que contiene a P como subgrupo, p no dividirá a dichos índices.

Al siguiente Lema también le llaman Segundo Teorema de Sylow, aunque nos reservamos este nombre para el resultado que se demustra a partir del Lema.

Lema 3.12. *Si P es un $p-$subgrupo de Sylow de un grupo finito G y H es un $p-$subgrupo de de $N_G(P)$, entonces H está contenido en P.*

Es decir, los $p-$subgrupos del normalizador de un $p-$subgrupo de Sylow están contenidos en diho subgrupo.

Demostración. Como $P \lhd N_G(P)$ y $H < N_G(P)$, tenemos que $HP < N_G(P)$ y $H \cap P < H$. Estamos en la situación:



Por el Segundo Teorema de Isomorfía:

$$HP/P \cong H/H \cap P$$

Ahora, si $r = [HP : P] = [H : H \cap P]$, entonces $p \nmid r$. Ahora, como $r = [H : H \cap P]$ y como H es un $p-$subgrupo, $p^k \mid r$ para cierto $k \in \mathbb{N}$ (como es un $p-$grupo, tendremos $k > 0$). Como $p \nmid r$ (por la observación anterior) y $p^k \mid r$, entonces $r = 1$, de donde $HP = P$ y $H < P$. □

Teorema 3.13 (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:

$$ac(g, P) = {}^gP = gPg^{-1} \in S$$

Sea $P_1 \in S$, estudiemos su órbita y su estabilizador:

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

Tenemos:

$$|Orb(P_1)| = [G : N_G(P_1)]$$
$$P_1 < N_G(P_1) < G_1$$
$$[G : P_1] = [G : N_G(P_1)][N_G(P_1) : P_1]$$

Por lo que $|Orb(P_1)|$ divide a $[G : P_1] = m$. En definitiva:

$$\text{mcd}(|Orb(P_1)|, p) = 1$$

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 $P_1 \in S$, $H \times Orb(P_1) \to Orb(P_1)$, dada por:

$$ac(h, P) = {}^hP = hPh^{-1} \in Orb(P_1)$$

Tendremos:

$$Stab_H(P) = \{h \in H \mid hPh^{-1} = P\} = H \cap N_G(P) < H$$

Además, también tendremos que $H \cap N_G(P) < P$, ya que si H es un $p-$subgrupo de $N_G(P)$, entonces $H < P$. En definitiva:

$$Stab_H(P) = H \cap N_G(P) < H \cap P < H \cap N_G(P)$$

De donde tenemos que $N_G(P) = H \cap P$. Usando la fórmula de la órbita:

$$|Orb(P_1)| = \sum_P [H : Stab_H(P)] = \sum_P [H : H \cap P]$$

De donde cada sumando divide a $|H|$ con H un $p-$subgrupo de P, por lo que $|H|$ es una potencia de p. Sin embargo, como $p \nmid |Orb(P_1)|$ (su máximo común divisor era 1), ha de existir un grupo $P \in Orb(P_1)$ (notemos que P es un $p-$subgrupo de Sylow. De hecho, P es un conjugado de P_1) de forma que:

$$[H : H \cap P] = 1$$

Por lo que $H \cap P = H$ y $H < P$.

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, antes vimos (el lema) que si $H = P_2 < G$, entonces H está contenido en un subgrupo de Sylow, por lo que $\exists P$, un $p-$subgrupo de Sylow, conjugado de P_1 (por *i)*) de forma que $P_2 < P$, pero $|P| = |P_2|$, luego $P_2 = P$.

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:

$$n_p = |S| = |Orb(P_1)| = [G : N_G(P_1)]$$

Por lo que $n_p \mid m$.

Si en el apartado i) tomamos $H = P_1$ (el de la demostración anterior):

$$n_p = |Orb(P_1)| = \sum_P [P_1 : P_1 \cap P]$$

Por lo que $[P_1 : P_1 \cap P] = 1$ y los demás eran múltiplos de p, deducimos que $n_p \equiv 1 \mod p$.

$\square$

Ejemplo. Vamos a calcular grupos de Sylow:

- En $C_n = \langle x \mid x^n = 1\rangle$ para cierto $n \in \mathbb{N}$, 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:

  - $2-$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.

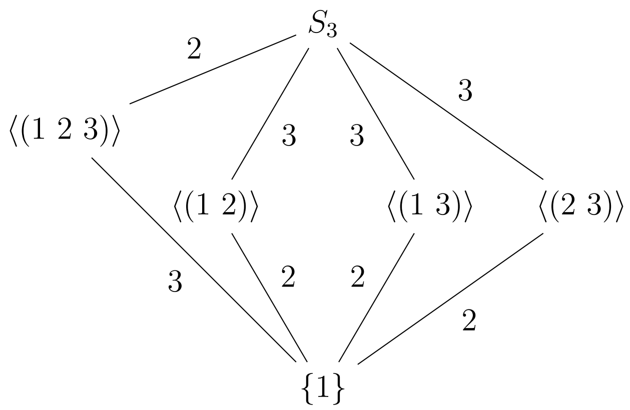


Figura 3.1: Diagrama de Hasse para los subgrupos de S_3.

  como los 3 subgrupos de la derecha son conjugados entre sí (compruébese), tendremos que $n_2 = 3$.

  - Los $3-$subgrupos de Sylow será un subgrupo de orden 3 de S_3, que será el único que hay: $\langle(1\ 2\ 3)\rangle = A_3 \lhd S_3$.

    Si queremos verlo por el Segundo Teorema de Sylow:

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

- En A_4, tenemos $|A_4| = 12 = 2^3 \cdot 3$. Tendremos:
  - $2-$subgrupo de Sylow de orden 4. Busquemos por el Segundo Teorema de Sylow:

$$\left.\begin{array}{r} n_2 \mid 3 \\ n_2 \equiv 1 \mod 2 \end{array}\right\} \Longrightarrow n_2 \in \{1, 3\}$$

    Concluimos que $n_2 = 1$, de donde el $2-$subgrupo de Sylow es V, que era normal en A_4.
  - $3-$subgrupo de Sylow de orden 3:

$$\left.\begin{array}{r} n_3 \mid 4 \\ n_3 \equiv 1 \mod 3 \end{array}\right\} \Longrightarrow n_3 \in \{1, 4\}$$

    Y serán los subgrupos de A_4 generados por los $3-$ciclos.
- En S_4, $|S_4| = 24 = 2^3 \cdot 3$:
  - Para los $2-$subgrupos:

$$\left.\begin{array}{r} n_2 \mid 3 \\ n_2 \equiv 1 \mod 2 \end{array}\right\} \Longrightarrow n_2 \in \{1, 3\}$$

    Si suponemos que $n_2 = 1$, sea Q un grupo con $|Q| = 8$ que sea el $2-$subgrupo de Sylow. En dicho caso, todas las trasposiciones deben estar contenidas en Q (por ser de orden 2), pero todas las trasposiciones generan a S_4, luego $Q = S_4$, contradicción.
    Por tanto, tenemos $n_2 = 3$, tenemos 3 $2-$subgrupos de Sylow: Q_1, Q_2 y Q_3. El grupo de Klein V es un $2-$subgrupo, y es normal en S_4. Por tanto, va a estar contenido en algún Q_k ($k \in \{1, 2, 3\}$). Supongamos que $V < Q_1$. Como todos ellos son conjugados, $\exists \alpha, \beta \in S_4$ de forma que:

$$\begin{aligned} Q_2 &= \alpha Q_1 \alpha^{-1} \\ Q_3 &= \beta Q_1 \beta^{-1} \end{aligned}$$

    Y si multiplicamos (como $V \lhd S_4$):

$$\begin{aligned} V = \alpha V \alpha^{-1} < \alpha Q_1 \alpha^{-1} = Q_2 \\ V = \beta V \beta^{-1} < \beta Q_1 \beta^{-1} = Q_3 \end{aligned}$$

    De donde deducimos que $V < Q_k$ para todo $k \in \{1, 2, 3\}$. Los Q_k contendrán a V y a alguna transposición:

$$\begin{aligned} Q_1 &= V\langle(1\ 2)\rangle \\ Q_2 &= V\langle(1\ 3)\rangle \\ Q_3 &= V\langle(1\ 4)\rangle \end{aligned}$$

  - Para los $3-$subgrupos de Sylow:

$$\left.\begin{array}{r} n_3 \mid 8 \\ n_3 \equiv 1 \mod 3 \end{array}\right\} \Longrightarrow n_3 \in \{1, 4\}$$

Los subgrupos de orden 4 de S_4 son:

$$\langle (1\ 2\ 3)\rangle, \langle (1\ 2\ 4)\rangle, \langle (1\ 3\ 4)\rangle, \langle (2\ 3\ 4)\rangle$$

Que son los 3−subgrupos de Sylow.

Corolario 3.13.1. *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. Por doble implicación:

$\Longrightarrow$) Si P es el único, como todos los conjugados de P son subgrupos de Sylow, tendremos que:

$$gPg^{-1} = P \qquad \forall g \in G$$

Que era la caracterización de subgrupo normal de G.

$\Longleftarrow$) Supuesto que $P \lhd G$, sea Q otro $p-$subgrupo de Sylow, como P y Q han de ser conjugados, sabemos que $\exists g \in G$ de forma que $gPg^{-1} = Q$, pero por ser $P \lhd G$, tenemos también que $P = gPg^{-1}$, luego:

$$P = gPg^{-1} = Q$$

□

Ejemplo. Todo grupo de orden 35 es resoluble.

Demostración. Sea G un grupo con $|G| = 35 = 5 \cdot 7$, vemos que:

$$\left.\begin{array}{r} n_7 \mid 5 \\ n_7 \equiv 1 \mod 5 \end{array}\right\} \Longrightarrow n_7 = 1$$

En dicho caso, tenemos un único 7−subgrupo de Sylow $H < G$, que además es normal y tendrá orden 7. 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:

$$|G/H| = 5$$

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 exitir $H \lhd G$ y ser H y G/H resolubles. □

Se puede demostrar de forma análoga que ciertos grupos de cierto orden son siempre resolubles.

Teorema 3.14. *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 1.32), vimos que G era producto directo interno de todos ellos (los llamaremos H_i con $i \in \{1, \ldots, n\}$) si y solo si:

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

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

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

□

Observación. Notemos que cualquier grupo abeliano finito es producto directo interno de sus subgrupos de Sylow, ya que en cualquier grupo abeliano los subgrupos son normales.

4. 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 estos grupos según su orden (para cada orden tendremos una clasificación), salvo isomorfismos.

Serán de especial relevancia varios resultados que ya hemos visto:

- $C_n \times C_m \cong C_{nm} \iff \mathrm{mcd}(n,m) = 1$, en la Proposición 1.34.
- Si $|G| = p_1^{n_1} \dots p_k^{n_k}$ y G tenía un único P_i p_i-subgrupo de Sylow para cada $i \in \{1, \dots, k\}$, entonces $G \cong P_1 \times P_2 \times \dots \times P_k$.

Como trabajaremos con subgrupos abelianos, recordamos que la notación que usábamos para el producto directo de grupos abelianos era $\oplus$.

Teorema 4.1 (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 $\beta_1 \geqslant \beta_2 \geqslant \dots \geqslant \beta_t \geqslant 1$ de forma que:

$$\beta_1 + \beta_2 + \dots + \beta_t = n \quad y \quad A \cong C_{p^{\beta_1}} \oplus C_{p^{\beta_2}} \oplus \dots \oplus C_{p^{\beta_t}}$$

Además, esta expresión es única, es decir, si existen $\alpha_1 \geqslant \alpha_2 \geqslant \dots \geqslant \alpha_s \geqslant 1$ de forma que:

$$\alpha_1 + \alpha_2 + \dots + \alpha_s = n \quad y \quad A \cong C_{p^{\alpha_1}} \oplus C_{p^{\alpha_2}} \oplus \dots \oplus C_{p^{\alpha_s}}$$

entonces $s = t$ y $\alpha_k = \beta_k$, para todo $k \in \{1, \dots, t\}$.

Observación. Notemos que lo que estamos haciendo es tomar particiones de n de la forma β_i, y este Teorema nos dice que el $p-$grupo puede escribirse de forma única salvo isomorfismos como producto de ciertos subgrupos cíclicos.

Es decir, existen tantos $p-$grupos abelianos de orden p^n como particiones tengamos del número n.

Ejemplo. Por ejemplo:

- Grupos abelianos finitos de orden $8 = 2^3$, tenemos como particiones:

$$3 \Longrightarrow A \cong C_8$$
$$1,2 \Longrightarrow A \cong C_4 \oplus C_2$$
$$1,1,1 \Longrightarrow A \cong C_2 \oplus C_2 \oplus C_2$$

- Los grupos abelianos finitos de orden $81 = 3^4$, tenemos como particiones:

$$A \cong C_{81}$$
$$A \cong C_{27} \oplus C_3$$
$$A \cong C_9 \oplus C_9$$
$$A \cong C_9 \oplus C_3 \oplus C_3$$
$$A \cong C_3 \oplus C_3 \oplus C_3 \oplus C_3$$

Teorema 4.2 (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:

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

Donde para cada $i \in \{1, \dots, k\}$ tenemos:

$$n_{i1} \geqslant n_{i2} \geqslant \dots \geqslant n_{it_i} \geqslant 1$$
$$n_{i1} + n_{i2} + \dots + n_{it_i} = r_i$$

Y la descomposición es única salvo el orden.

Esta última recibe el nombre de descomposición cíclica primaria, y a los $p_i^{n_{ij}}$ con $i \in \{1, \dots, k\}$ y $j \in \{1, \dots t_i\}$ se les llama divisores elementales de A.

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 $P_1, P_2, \dots, P_k$ el conjunto de todos sus $p-$subgrupos de Sylow, de forma que $|P_i| = p_i^{r_i}$, para todo $i \in \{1, \dots, k\}$. Como cada P_i es un p_i-subgrupo abeliano finito, aplicando el Teorema 4.1, podemos escribir:

$$P_i = \bigoplus_{j=1}^{t_i} C_{p_i^{n_{ij}}} \qquad \forall i \in \{1, \dots, k\}$$

De donde tenemos la expresión de la tesis.
A cada P_i con $i \in \{1, \dots, k\}$ lo llamaremos componente p_i-primaria de A. □

Ejemplo. Si tenemos un subgrupo finito abeliano A con $|A| = 360 = 2^3 \cdot 3^2 \cdot 5$, veamos los divisores elementales:

Div. elementales	Descomp. 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	$C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$

Serían todas las descomposiciones cíclicas primarias de A. Es decir, A será isomorfo a cualquiera de esos.

Sin embargo, si recordamos la Proposición 1.34, esto nos llevará a la descomposición cíclica, donde observaremos por ejemplo que:

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

Ahora, usaremos que:

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

Teorema 4.3 (Descomposición cíclica de un grupo abeliano finito)**.**
Si A es un grupo abeliano finito, entonces:

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

Donde los d_i son enteros positivos de forma que:

$$d_1 d_2 \ldots d_t = |A|$$

Y $d_i \mid d_j$ para cada $j \leqslant i$. Además, la descomposición es única salvo el orden, para cada partición.

Demostración. Supuesto que $|A| = p_1^{r_1} \ldots p_k^{r_k}$, si usamos la descomposición que nos da el Teorema 4.2:

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

Para ciertos:

$$\begin{gathered}
n_{i1} \geqslant n_{i2} \geqslant \ldots \geqslant n_{it_i} \geqslant 1 \\
n_{i1} + n_{i2} + \ldots + n_{it_i} = r_i
\end{gathered}$$

Sea $t = \text{máx}\, t_1, t_2, \ldots, t_k$, si $t_i < l \leqslant t$, tendremos entonces que $n_{il} = 0$.

Lo que estamos haciendo es dada una partición, como por ejemplo la $\{2, 2^2, 3^2, 5\}$, denotar por t_i al número de particiones de cada número y por n_{ij} a los exponentes de cada una de las particiones, construyendo la tabla:

$$\left\{ \begin{array}{c|cc} t_1 & n_{11} & n_{12} \\ t_2 & n_{21} & n_{22} \\ t_3 & n_{31} & n_{32} \end{array} \right.$$

De esta forma, tenemos:

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

Y A es la suma directa de los cíclicos con órdenas las entradas de las columnas. Si tomamos el producto por columnas obtenemos la cíclica primaria y si la hacemos por filas la que estamos interesados:

$$\begin{aligned} d_1 &= p_1^{n_{11}} p_2^{n_{21}} \ldots p_k^{n_{k1}} \\ &\vdots \\ d_t &= p_1^{n_{1t}} p_2^{n_{2t}} \ldots p_k^{n_{kt}} \end{aligned}$$

Efectivamente, tendremos que:

$$d_1 d_2 \ldots d_t = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k} = |A|$$

Como $n_{ij} \geqslant n_{ij+1}$, tendremos entonces que $d_i \mid d_j$, para todo $j \leqslant i$. Además, tendremos que:

$$\begin{aligned} C_{d_1} &\cong C_{p_1^{n_{11}}} \oplus C_{p_2^{n_{21}}} \oplus \ldots \oplus C_{p_k^{n_{k1}}} \\ &\vdots \\ C_{d_t} &\cong C_{p_1^{n_{1t}}} \oplus C_{p_2^{n_{2t}}} \oplus \ldots \oplus C_{p_k^{n_{kt}}} \end{aligned}$$

De donde $A \cong C_{d_1} \oplus C_{d_2} \oplus \ldots \oplus C_{d_t}$. La unicidad viene de la unicidad dada por la descomposición del Teorema 4.2. □

Los d_i reciben el nombre de factores invariantes.

Ejemplo. Sea A un grupo abeliano finito con $|A| = 360 = 2^3 \cdot 3^2 \cdot 5$:

- Para la partición $\{2^3, 3^2, 5\}$, tenemos que:

  $$A \cong C_8 \oplus C_9 \oplus C_5$$

  Los factores invariantes serán:

  $$d_1 = 2^3 \cdot 3^2 \cdot 5$$

  Por lo que la descomposición cíclica 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:

  $$\begin{pmatrix} 2^2 & 3^2 & 5 \\ 2 & 1 & 1 \end{pmatrix}$$

  Por lo que tendremos (los productos de las filas):

  $$\begin{aligned} d_1 &= 2^2 \cdot 3^2 \cdot 5 = 180 \\ d_2 &= 2 \cdot 1 \cdot 1 = 2 \end{aligned}$$

  Y la descomposición cíclica es:

  $$A \cong C_{180} \oplus C_2$$

- Para la descomposición $\{2, 2, 2, 3^2, 5\}$, tenemos:

$$A \cong C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5$$

Y tendremos $t = 3$:

$$\left(\begin{array}{cccc} d_1 = & 2 & 3^2 & 5 \\ d_2 = & 2 & 1 & 1 \\ d_3 = & 2 & 1 & 1 \end{array}\right)$$

Por lo que:

$$A \cong C_{90} \oplus C_2 \oplus C_2$$

- Para $\{2^3, 3, 3, 5\}$:

$$A \cong C_8 \oplus C_3 \oplus C_3 \oplus C_5$$

Y tenemos:

$$\begin{pmatrix} 2^3 & 3 & 5 \\ 1 & 3 & 1 \end{pmatrix}$$

Y la descomposición cíclica será:

$$A \cong C_{120} \oplus C_3$$

- Para $\{2^2, 2, 3, 3, 5\}$:

$$A \cong C_4 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$$

Y tenemos:

$$\begin{pmatrix} 2^2 & 3 & 5 \\ 2 & 3 & 1 \end{pmatrix}$$

Por lo que tenemos la descomposición cíclica:

$$A \cong C_{60} \oplus C_6$$

- Para $\{2, 2, 2, 3, 3, 5\}$:

$$A \cong C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$$

Tenemos:

$$\begin{pmatrix} 2 & 3 & 5 \\ 2 & 3 & 1 \\ 2 & 1 & 1 \end{pmatrix}$$

Y:

$$A \cong C_{30} \oplus C_6 \oplus C_2$$

En el caso particular de que todos los primos tengan exponente 1:

Corolario 4.3.1. *Si A es un grupo abeliano finito con $|A| = p_1p_2 \ldots p_k = n$, entonces salvo isomorfismo, el único grupo abeliano de orden n es el cíclico C_n.*

Demostración. Utilizando el Teorema 4.2, 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:

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

□

Ejemplo. Sea A un grupo abeliano finito con $|A| = 580 = 2^2 \cdot 3^2 \cdot 5$, buscamos clasificarlo según la descomposición cíclica:

Descomposición	desc. cíclica primaria	factores invariantes	desc. cíclica
$\{2^2, 3^2, 5\}$	$C_4 \oplus C_9 \oplus C_5$	$2^2 \cdot 3^2 \cdot 5 = 180$	C_{180}
$\{2, 2, 3^2, 5\}$	$C_2 \oplus C_2 \oplus C_9 \oplus C_5$	$d_1 = 2 \cdot 9 \cdot 5 = 90$ $d_2 = 2$	$C_{90} \oplus C_2$
$\{2^3, 3, 3, 5\}$	$C_4 \oplus C_3 \oplus C_3 \oplus C_5$	$d_1 = 2^2 \cdot 3 \cdot 5 = 60$ $d_2 = 3$	$C_{60} \oplus C_3$
$\{2, 2, 3, 3, 5\}$	$C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$	$d_1 = 2 \cdot 3 \cdot 5 = 30$ $d_2 = 2 \cdot 3 = 6$	$C_{30} \oplus C_6$

Ejemplo. Listar los órdenes de todos los elementos de un grupo de orden 8. Sea A un grupo abeliano finito de orden 8, entonces lo podemos clasificar en:

- C_8:
  - Los elementos $\{1, 3, 5, 7\}$ tienen orden 8.
  - $O(0) = 1$.
  - $O(2) = {}^{8}/_{\text{mcd}(2,8)} = 4 = O(6)$.
  - $O(4) = 2$.
- $C_4 \oplus C_2$, 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 son: $\{1, 2, 4\}$:
  - $O(0, 0) = 1$.
  - $O(0, 1) = 2$.
  - $O(1, b) = 4 = O(3, b)$, $\forall b \in C_2$
  - $O(2, b) = 2$, $\forall b \in C_2$.
- $C_2 \oplus C_2 \oplus C_2$, los órdenes son $\{1, 2\}$ y todos tienen orden 2 salvo el elemento $(0, 0, 0)$.