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:

$$hx = xh' \in xH$$

$\square$

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 $s \in S \cup S^{-1} \subseteq G$.

$\Longleftarrow$) 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 $K = \{1, (1\,2\,3), (1\,3\,2)\}$, como $[S_3 : K] = 2$, tenemos que $K \lhd S_3$:

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

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

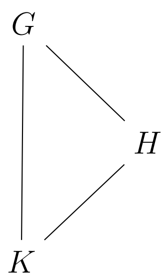
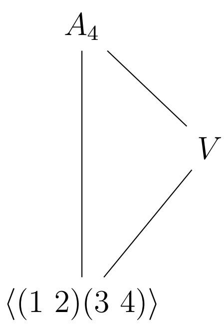


Figura 1.1: Situación descrita.

   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:

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

- 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 $A \lhd B$. $\square$

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, 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 $H = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$, tenemos que:

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

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

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.

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 $|H| \geqslant 8$, contradicción.

Proposición 1.7. *Sea G un grupo y $H < G$, entonces: H es normal 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.

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

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 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. Como $K \lhd G$, tenemos que $xK = Kx$ para todo $x \in G$, en particular para $x \in H$, con lo que $HK = KH$, lo que nos dice que $HK < G$. Además, vemos que $K \lhd HK$.
Consideramos ahora el homomorfismo resultado de componer la inclusión de H en G con la proyección al cociente G/K:

$$H \xrightarrow{i} G \xrightarrow{p} G/K$$

Con lo que:

$$Im(p \circ i) = \{(p \circ i)(h) \mid h \in H\} = \{p(h) \mid h \in H\} = \{hK \mid h \in H\} \overset{(*)}{=} HK/K$$

Calculemos el núcleo:

$$\ker(p \circ i) = \{h \in H \mid (p \circ i)(h) = K\} = \{h \in H \mid hK = K\} = \{h \in H \mid h \in K\} = H \cap K$$

Lo que nos dice que $H \cap K \lhd H$. Por el Primer Teorema de Isomorfía (aplicado a $p \circ i$):

$$\frac{H}{\ker(p \circ i)} \cong Im(p \circ i)$$

Lo que nos dice que:

$$\frac{H}{H \cap K} \cong HK/K$$

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:

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

$\square$

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:

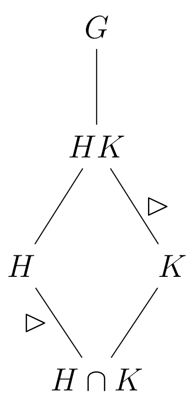


Figura 1.3: Situación del Teorema 1.10.

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 $H \nsubseteq A_n$, por lo que tenemos:

$$HA_n = S_n$$

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

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

Teorema 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):

$$\begin{aligned} p_* &: \mathcal{A} \to \mathcal{B} \\ p^* &: \mathcal{B} \to \mathcal{A} \end{aligned}$$

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 $J < G/N$, 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 $J \in \mathcal{B}$:

$$(p_* \circ p^*)(J) = p_*(\{x \in G \mid p(x) \in J\}) \stackrel{(*)}{=} J$$

Donde en $(*)$ hemos aplicado que p es sobreyectiva, por lo que si tenemos $j \in J$, existirá un $x \in G$ de forma que $p(x) = j$, 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 $xN \in G/N$, $hN \in H/N$:

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

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 φ_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:

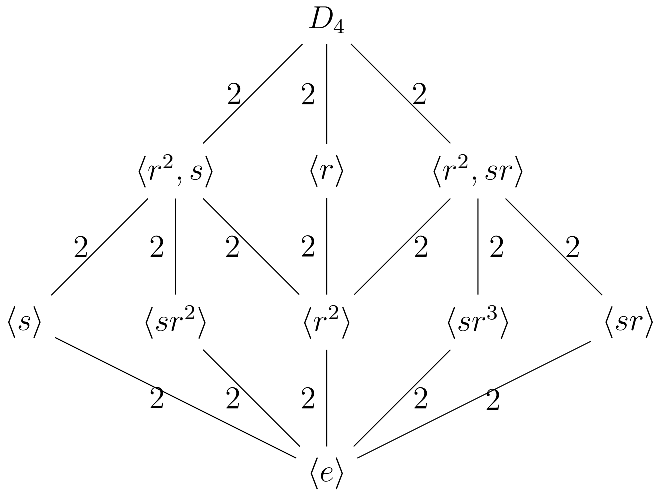
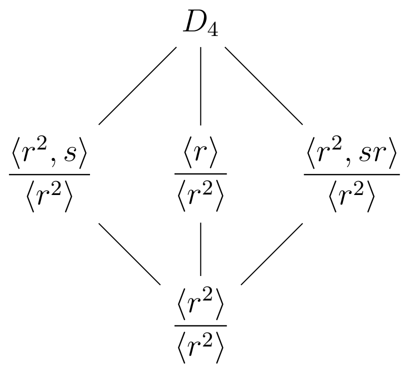
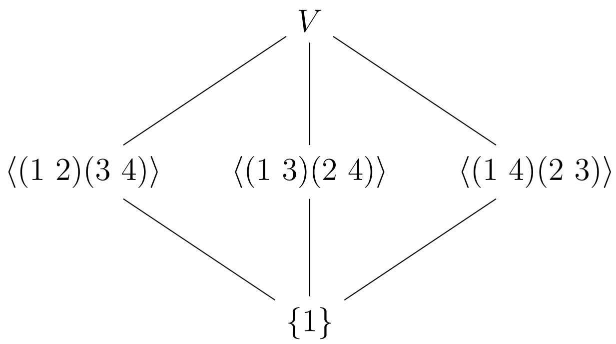


Figura 1.4: Diagrama de Hasse para los subgrupos de D_4.

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 $z = ab \in A(B \cap C)$.

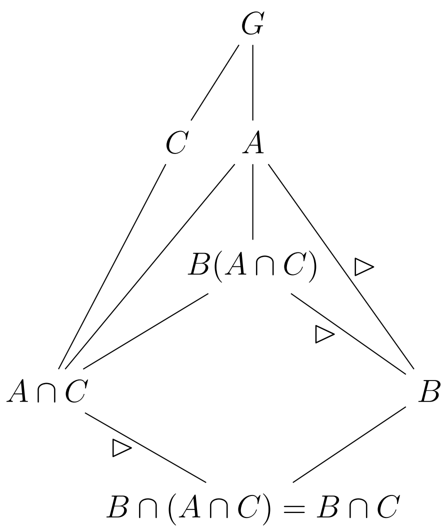
$\square$

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 $BC \lhd AC$.

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

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).

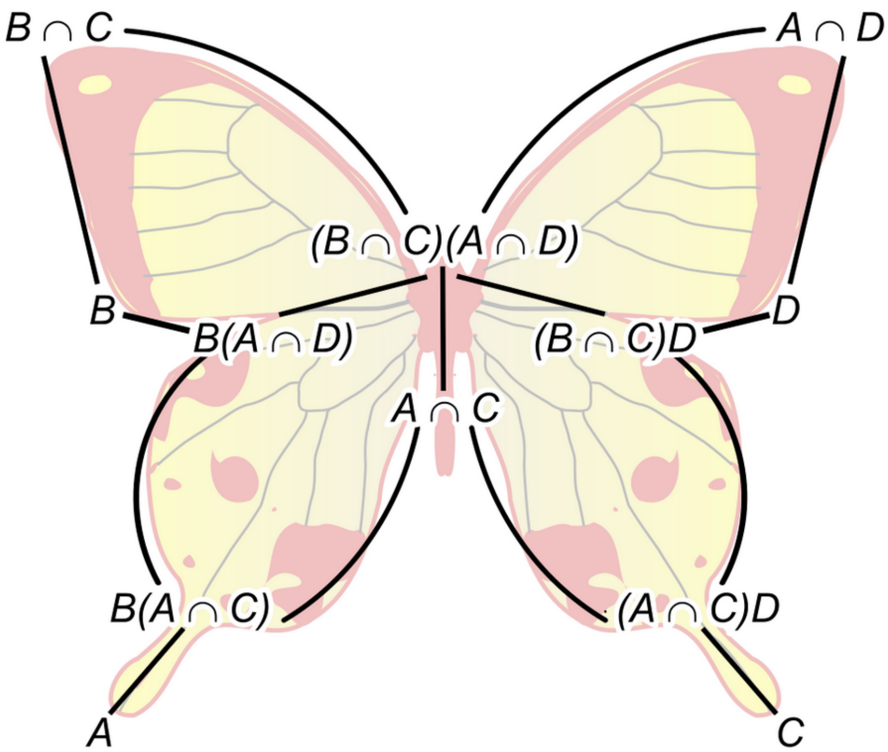


Figura 1.6: Situación del Teorema 1.14

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

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

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

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

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

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

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

Proposición 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.

$$H \underset{p_1}{\overset{i_1}{\rightleftarrows}} H \times G \underset{p_2}{\overset{i_2}{\leftrightarrows}} G$$

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. *Se tiene que:*
$$H' = Im(i_1) = \ker(p_2) = \{(h, 1) \mid h \in H\} \lhd H \times G$$
Además, $H' \cong H$*.*
5. *De la misma forma:*
$$G' = Im(i_2) = \ker(p_1) = \{(1, k) \mid k \in G\} \lhd H \times G$$
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:
   $$\begin{aligned}Im(i_1) &= \{i_1(h) \mid h \in H\} = \{(h,1) \mid h \in H\}\\ \ker(p_2) &= \{(h,k) \in H\times G \mid p_2(h,k) = 1\} = \{(h,k) \in H\times G \mid k = 1\}\\ &= \{(h,1) \in H\times G\} = \{(h,1) \mid h \in H\}\end{aligned}$$
   Para ver que $H' = \{(h,1) \mid h \in H\} \lhd H\times G$, basta ver que $x(h,1)x^{-1} \in H'$ $\forall x \in H\times G, \forall h \in H$. Para ello, sean $h' \in H$ y $(h,k) \in H\times K$, tenemos que:
   $$(h,k)(h',1)(h,k)^{-1} = (h,k)(h',1)\left(h^{-1},k^{-1}\right) = (hh'h^{-1},kk^{-1}) = (hh'h^{-1},1) \in H'$$
   Donde hemos usado que $hh'h^{-1} \in H$, por ser H un grupo.

   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:

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

Y de forma análoga a lo anterior, para ver que $G' = \{(1,k) \mid k \in G\} \lhd H \times G$, cogemos $k' \in G$ y $(h,k) \in H \times G$, donde vemos que:

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

Y finalmente, para ver que $G' \cong G$, tenemso 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, que 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:

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

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

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

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

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

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

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

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

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

Teorema 1.19. *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 $(h, k) \in H \times K$:

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

$\square$

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 $k \in K$, 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 $L \cong H \times K$. □

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.

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

Teorema 1.24. *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 1.25. *Sea* $\{G_\lambda \mid \lambda \in \Lambda\}$, *entonces existe un monomorfismo*

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

1.4.3. Producto directo de una familia finita de subgrupos

Teorema 1.26 (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 1.27. *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 1.28. *Sea G un grupo y $h, k \in G$:*

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

Demostración. Veamos las dos implicaciones:

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

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

□

Teorema 1.29 (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) *$\forall h \in H$, $\forall k \in K$:*

$$hk = kh, \quad H \vee K = G, \quad H \cap K = \{1\}$$

iv) *$\forall h \in H$, $\forall k \in K$:*

$$hk = kh$$

Y para todo $g \in G$, $\exists_1 h \in H, k \in K$ tal que $g = hk$.

Demostración. Veamos las implicaciones:

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

- Primero que $HK = G$:

  $\subseteq$) Como $H, K < G$, tenemos que $HK \subseteq G$.

  $\supseteq$) 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:

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

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 $[h, k] = h(kh^{-1}k^{-1}) \in H$, por lo que:

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

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 $\alpha_1, \dots, \alpha_n \in H \cup K$ de forma que:

$$g = \alpha_1 \dots \alpha_n$$

Pero como $hk = kh$ para todo $k \in K$ y $h \in H$, podremos conmutar los elementos de forma que lleguemos a:

$$g = (h_1 \dots h_m)(k_{m+1} \dots k_n) = hk \in HK$$

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 $g = hk = \phi(h, k)$. $\square$

Ejemplo. Veamos si los siguientes ejemplos son o no un producto interno directo:

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 1.29.

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

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

Demostración. Veamos que los dos se cumplen:

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

2. Consideramos:

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

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

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

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

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

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

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

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

Por lo que:
$$\psi(\alpha, \beta)(h', k') = (\alpha(h'), \beta(k')) = (h, k)$$

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

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

De donde deducimos que:

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

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

Finalmente, veamos que ψ es un monomorfismo:

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

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

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

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

- 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.

$\square$

Teorema 1.31. *Sean H, K dos grupos finitos tales que* $\mathrm{mcd}(|H|, |K|) = 1$*, 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 1.30 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 1.30, tenemos que $H_1 \times K_1 < H \times K$, y por la definición de L que $L < H_1 \times K_1$. 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 ψ es sobreyectiva.

□

La segunda parte será utilizada en varios ejercicios.

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

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

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

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

1. *$\exists_1 H_k < G_k$ tal que $L = H_1 \times \ldots \times H_k$ para todo $L < G$.*
2. *$Aut(G_1) \times \ldots \times Aut(G_n) \cong Aut(G)$.*

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:
$$O(\overline{r}, \overline{s}) = \mathrm{mcm}(O(\overline{r}), O(\overline{s})) = \left\{ \begin{array}{l} 1 \Longleftrightarrow \overline{r} = \overline{s} = 0 \\ 2 \Longleftrightarrow \overline{r} \neq 0 \lor \overline{s} \neq 0 \end{array} \right.$$
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:
$$\mathbb{Z}_2 \oplus \mathbb{Z}_3$$
Como 2 y 3 son coprimos (se verá), podremos escribir:
$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle (\overline{1}, \overline{1}) \rangle$$
Tenemos que $O(\overline{1}, \overline{1}) = 6$, por lo que $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$.

Proposición 1.34. *Si G y H son grupos cíclicos finitos, entonces:*
$$G \oplus H \text{ es cíclico } \Longleftrightarrow \mathrm{mcd}(|G|, |H|) = 1$$

Demostración. Veamos las dos implicaciones. Para ello, supongamos que $\exists x \in G$, $y \in H$ con:
$$G = \langle x \rangle, \quad O(x) = n, \quad H = \langle y \rangle, \quad O(y) = m$$

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

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

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:

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

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

$$\text{mcd}(n, m) = \text{mcd}(O(a), O(b)) = \frac{nm}{nm} = 1$$

$\square$

Proposición 1.35. *Si $G_1, G_2, \ldots, G_n$ son n grupos cíclicos finitos, entonces:*

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

Demostración. Puede demostrarse fácilmente por inducción. $\square$

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.

1.7. Grupos cociente. Teoremas de isomorfismo. Productos

Ejercicio 1.7.1. Demostrar que si $G \leqslant S_n$, entonces $G \subseteq A_n$ o bien se tiene que $[G : G \cap A_n] = 2$. Concluir que un subgrupo de S_n consiste sólo en permutaciones pares, o bien contiene el mismo número de permutaciones pares que de impares.

Sea $G \leqslant S_n$ un subgrupo de S_n. O bien $G \subseteq A_n$ (en cuyo caso consiste sólo de permutaciones pares); o bien $\exists \sigma \in G$ tal que $\sigma \notin A_n$, es decir, $\varepsilon(\sigma) = -1$. Para ver que $[G : G \cap A_n] = 2$, hay varias posibilidades.

Opción 1: Consideramos el homomorfismo $\varepsilon : G \to \{-1, 1\}$ dado por la aplicación signatura. Calculemos su núcleo y su imagen:

$$\ker(\varepsilon) = \{\sigma \in G \mid \varepsilon(\sigma) = 1\} = A_n \cap G,$$
$$Im(\varepsilon) = \{\varepsilon(\sigma) \mid \sigma \in G\} \overset{(*)}{=} \{-1, 1\}$$

donde vamos a razonar el por qué de $(*)$. Como $1 \in G$ por ser este un grupo, entonces $1 \in Im(\varepsilon)$, y como $\exists \sigma \in G$ tal que $\varepsilon(\sigma) = -1$, entonces $-1 \in Im(\varepsilon)$. Por lo tanto, $Im(\varepsilon) = \{-1, 1\}$. Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{\ker(\varepsilon)} \cong Im(\varepsilon) \implies \frac{G}{A_n \cap G} \cong \{-1, 1\} \cong \mathbb{Z}_2.$$

Por definición de índice, se tiene que:

$$[G : A_n \cap G] = \left| \frac{G}{A_n \cap G} \right| = |\mathbb{Z}_2| = 2$$

Opción 2: Por el Teorema de Lagrange, sabemos que:

$$[S_n : A_n] = \frac{|S_n|}{|A_n|} = 2 \Longrightarrow A_n \lhd S_n$$

Aplicando el Segundo Teorema de Isomorfía a G y A_n, tenemos que:

$$\frac{G}{G \cap A_n} \cong \frac{GA_n}{A_n}$$

Veamos qué grupo es GA_n. En primer lugar, para $1 \in G$ vemos que $A_n \subset GA_n$. No obstante, como $\exists \sigma \in G$ con $\varepsilon(\sigma) = -1$, entonces $A_n \neq GA_n$, por lo que $|GA_n| > |A_n| = {}^{|S_n|}/_2$. Como $|GA_n| \mid |S_n|$, ha de ser $|GA_n| = |S_n|$, por lo que $GA_n = S_n$. Por tanto:

$$\frac{G}{G \cap A_n} \cong \frac{S_n}{A_n}$$

Por definición de índice, se tiene que:

$$[G : A_n \cap G] = \left| \frac{G}{A_n \cap G} \right| = \left| \frac{S_n}{A_n} \right| = \frac{|S_n|}{|A_n|} = 2$$

En cualquier caso, hemos visto que $[G : A_n \cap G] = 2$. Por el Teorema de Lagrange, se tiene que $|G| = 2 \cdot |G \cap A_n|$, por lo que la mitad de las permutaciones de G son pares. Como una permutación o bien es par o es impar, entonces la otra mitad ha de tener signatura impar. Por tanto, contiene el mismo número de permutaciones pares que de impares.

Ejercicio 1.7.2. Sea $\mathbb{K}$ un cuerpo.

1. Se considera la siguiente aplicación:

$$\begin{array}{rccc} \det: & \mathrm{GL}_n(\mathbb{K}) & \longrightarrow & \mathbb{K}^\times \\ & G & \longmapsto & \det(G) \end{array}$$

   Demostrar que dicha aplicación es un epimorfismo de grupos. ¿Cuál es el núcleo de este homomorfismo?

   Para comprobar que se trata de un homomorfismo, tomamos $A, B \in \mathrm{GL}_n(\mathbb{K})$ y por las propiedades de la determinante, se tiene que:

$$\det(AB) = \det(A) \cdot \det(B)$$

   Por otro lado, para cada $a \in \mathbb{K}^\times$, se considera la siguiente matriz:

$$A_a = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

   Como $\det(A_a) = a \neq 0$, entonces $A_a \in \mathrm{GL}_n(\mathbb{K})$. Como $\det(A_a) = a$, se tiene que det es sobreyectiva. Por lo tanto, det es un epimorfismo de grupos. Su núcleo es:

$$\ker(\det) = \{A \in \mathrm{GL}_n(\mathbb{K}) \mid \det(A) = 1\} = \mathrm{SL}_n(\mathbb{K})$$

2. Si $\mathbb{K}$ es un cuerpo finito con q elementos, determinar el orden del grupo $\mathrm{SL}_n(\mathbb{K})$.

   Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{\mathrm{GL}_n(\mathbb{K})}{\mathrm{SL}_n(\mathbb{K})} \cong \mathbb{K}^\times$$

   Por el Teorema de Lagrange, se tiene que:

$$|\mathrm{SL}_n(\mathbb{K})| = \frac{|\mathrm{GL}_n(\mathbb{K})|}{|\mathbb{K}^\times|} = \frac{|\mathrm{GL}_n(\mathbb{K})|}{q-1} = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{q-1}$$

Ejercicio 1.7.3. Sea $n \in \mathbb{N} \setminus \{0\}$, y sea G un grupo verificando que para todo par de elementos $x, y \in G$ se tiene que $(xy)^n = x^n y^n$. Se definen:

$$\begin{aligned} H &= \{x \in G \mid x^n = 1\}, \\ K &= \{x^n \mid x \in G\}. \end{aligned}$$

Demostrar que $H, K \lhd G$, y que $|K| = [G : H]$.

Definimos en primer lugar la siguiente aplicación:

$$\begin{array}{rccc} f: & G & \longrightarrow & G \\ & x & \longmapsto & x^n \end{array}$$

Para demostrar que se trata de un homomorfismo emplearemos la propiedad dada en el enunciado $(*)$:

$$f(xy) = (xy)^n \stackrel{(*)}{=} x^n y^n = f(x)f(y) \qquad \forall x, y \in G$$

Por tanto, f es un homomorfismo. Como $\{1\}, G < G$, entonces los siguientes grupos son subgrupos de G:

$$\begin{aligned} f^*(\{1\}) &= \{x \in G \mid f(x) = 1\} = \{x \in G \mid x^n = 1\} = H = \ker(f), \\ f_*(G) &= \{f(x) \mid x \in G\} = \{x^n \mid x \in G\} = K = Im(f). \end{aligned}$$

Por tanto, tenemos que $H, K < G$. Probamos ahora que son grupos normales en G. En primer lugar, para H tomamos $x \in G$ y $h \in H$ (por lo que $h^n = 1$). Entonces:

$$(xhx^{-1})^n = xh^n x^{-1} = x \cdot 1 \cdot x^{-1} = 1 \implies xhx^{-1} \in H$$

Por tanto, $H \lhd G$. Ahora probamos que K es normal en G. Tomamos $x \in G$ y $k \in K$ (por lo que $\exists y \in G$ tal que $k = y^n$). Entonces, consideramos $xyx^{-1} \in G$ y calculamos:

$$xkx^{-1} = x(y^n)x^{-1} = (xyx^{-1})^n \in K$$

Por tanto, $K \lhd G$. Para probar que $|K| = [G : H]$, tomamos el homomorfismo f anteriormente descrito. Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{H} \cong K \implies |K| = \left|\frac{G}{H}\right| = [G : H]$$

Ejercicio 1.7.4. Para un grupo G se define su *centro* como

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

1. Demostrar que $Z(G) < G$.

   Como $Z(G) \subset G$, hay dos principales posibilidades, ambas equivalentes:

   Opción 1: Comprobamos las tres condiciones que caracterizan a los subgrupos:

   - $1 \in Z(G)$: Para todo $x \in G$, se tiene que $1x = x1 = x$.
   - $a, b \in Z(G) \implies ab \in Z(G)$: Para todo $x \in G$, se tiene que:

     $$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$$

   - $a \in Z(G) \implies a^{-1} \in Z(G)$: Para todo $x \in G$, se tiene que:

     $$a^{-1}x = (x^{-1}a)^{-1} = (ax^{-1})^{-1} = xa^{-1}.$$

Opción 2: Dados $a, b \in Z(G)$, comprobemos que $ab^{-1} \in Z(G)$:

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

En cualquier caso, $Z(G)$ es un subgrupo de G.

2. Demostrar que $Z(G) \lhd G$.

De nuevo, hay dos posibilidades:

Opción 1: Para $x \in G$. Entonces:

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

Opción 2: Empleamos la caracterización de subgrupo normal. Para $x \in G$ y $z \in Z(G)$, buscamos ver que $xzx^{-1} \in Z(G)$:

$$xzx^{-1}y = zxx^{-1}y = zy = yz = yzxx^{-1} = yxzx^{-1} \qquad \forall y \in G.$$

En ambos casos, se tiene que $Z(G) \lhd G$.

3. Demostrar que G es abeliano si, y sólo si, $G = Z(G)$.

$$G = Z(G) \iff G = \{a \in G \mid ax = xa\ \forall x \in G\} \iff ax = xa\ \forall a, x \in G \iff G \text{ es abeliano.}$$

4. Demostrar que $G/Z(G)$ es abeliano si, y sólo si, G es abeliano. Demostrar que si $G/Z(G)$ es cíclico, entonces G es abeliano.

Como $G/Z(G)$ es cíclico, entonces existe $x \in G$ tal que $G/Z(G) = \langle xZ(G)\rangle$. Como las clases de equivalencia forman una partición disjunta de G, para cada $x \in G$ existe $k \in \mathbb{Z}$ tal que $x \in x^k Z(G)$. Buscamos ahora demostrar que G es abeliano. Dados $a, b \in G$, entonces existen $p, q \in \mathbb{Z}$ tales que $a \in x^p Z(G)$ y $b \in x^q Z(G)$. Entonces, existen $z_a, z_b \in Z(G)$ tales que $a = x^p z_a$ y $b = x^q z_b$. Por tanto:

$$ab = (x^p z_a)(x^q z_b) = x^{p+q} z_a z_b = x^q z_b x^p z_a = (x^q z_b)(x^p z_a) = ba$$

Por tanto, $ab = ba$ para todo $a, b \in G$, por lo que G es abeliano.

Ejercicio 1.7.5. Determinar el centro del grupo diédrico D_4. Observar que el cociente $D_4/Z(D_4)$ es abeliano, aunque D_4 no lo sea (compárese este hecho con el tercer apartado del ejercicio anterior).

El grupo D_4 está formado por las siguientes rotaciones y reflexiones:

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

Sabemos que $Z(D_4)$ es un subgrupo normal de D_4. En primer lugar, sabemos que $1 \in Z(D_4)$. Veamos que $r^2 \in Z(D_4)$. En primer lugar, vemos que conmuta con todas las potencias de r. Veamos ahora que conmuta con el resto de elementos:

$$\begin{aligned}
r^2 s &= rsr^3 = sr^6 = sr^2 \\
r^2\ sr &= sr^2 r = sr\ r^2 \\
r^2\ sr^2 &= srr^2 r = s = sr^4 = sr^2\ r^2 \\
r^2\ sr^3 &= sr = sr^5 = sr^3\ r^2
\end{aligned}$$

Por tanto, $\{1, r^2\} \subset Z(D_4)$. Además, tenemos que:

$$\begin{aligned}
sr = r^3 s \neq rs &\Longrightarrow s, r \notin Z(D_4) \\
sr^3 = r^9 s = rs \neq r^3 s &\Longrightarrow r^3 \notin Z(D_4) \\
sr\ s = r^3 \neq r &\Longrightarrow sr \notin Z(D_4) \\
sr^3\ s = r \neq r^3 &\Longrightarrow sr^3 \notin Z(D_4)
\end{aligned}$$

Como $|Z(D_4)|$ divide a $|D_4| = 8$ y $2 \leqslant |Z(D_4)| \leqslant 3$, se tiene que $|Z(D_4)| = 2$. Por tanto,

$$Z(D_4) = \{1, r^2\}$$

Veamos que $D_4/Z(D_4)$ es abeliano. Sabemos que:

$$|D_4/Z(D_4)| = \frac{|D_4|}{|Z(D_4)|} = \frac{8}{2} = 4$$

Por tanto, $D_4/Z(D_4)$ es isomorfo a V o a C_4. Por el último apartado del ejercicio anterior, si fuese $D_4/Z(D_4)$ isomorfo a C_4, entonces D_4 sería abeliano. Como no lo es, se tiene que $D_4/Z(D_4) \cong V$. Como V es abeliano, se tiene que $D_4/Z(D_4)$ también lo es.

Ejercicio 1.7.6. Determinar el centro de los grupos S_n y A_n para $n \geqslant 2$.

Para $n = 2$, tenemos que:

$$\begin{aligned}
S_2 = \{1, (1\ 2)\} &\implies Z(S_2) = S_2 \\
A_2 = \{1\} &\implies Z(A_2) = A_2
\end{aligned}$$

Calculamos ahora $Z(S_n)$ para $n \geqslant 3$. Sea $\sigma \neq 1 \in S_n$. Entonces,$\exists i, j \in \{1, \dots, n\}$ tales que $i \neq j$ y $\sigma(i) = j$. Consideramos ahora $k \in \{1, \dots, n\}$ tal que $k \neq i, j$, y sea la permutación $\tau = (j\ k)$. Entonces:

$$\begin{aligned}
\sigma\tau(i) &= \sigma(i) = j \\
\tau\sigma(i) &= \tau(j) = k
\end{aligned}$$

Por tanto, $\sigma\tau \neq \tau\sigma$. Como σ es arbitrario, se tiene que $Z(S_n) = \{1\}$ para $n \geqslant 3$.

Trabajamos ahora con A_n. En primer lugar, para $n = 3$ tenemos que $|A_3| = 3$ primo, por lo que A_3 es cíclico y en particular abeliano. Por tanto, $Z(A_3) = A_3$.

Para $n \geqslant 4$, sea $\sigma \in A_n$ tal que $\sigma \neq 1$. Entonces, $\exists i, j \in \{1, \ldots, n\}$ tales que $i \neq j$ y $\sigma(i) = j$. Consideramos ahora $k, l \in \{1, \ldots, n\} \setminus \{i, j\}$, tal que $k \neq l$. Consideramos ahora $\tau = (j\ k\ l) \in A_n$. Entonces:

$$\sigma\tau(i) = \sigma(i) = j$$
$$\tau\sigma(i) = \tau(j) = k$$

Por tanto, $\sigma\tau \neq \tau\sigma$. Como σ es arbitrario, se tiene que $Z(A_n) = \{1\}$ para $n \geqslant 4$. Notemos que hemos tenido que imponer que $n \geqslant 4$ para que podamos elegir 4 elementos distintos.

Ejercicio 1.7.7. Determinar el centro del grupo D_n para $n \geqslant 3$.

Dado $z \in D_n$, como $D_n = \langle r, s \rangle$ entonces $z \in Z(D_n)$ si y sólo si z conmuta con r y con s. Distinguimos según los elementos de D_n:

- $1 \in Z(D_n)$ para todo $n \geqslant 3$.
- Fijado $m \in \{1, \ldots, n-1\}$, veamos si $r^m \in Z(D_n)$.

  $$r^m\ r = r^{m+1} = r\ r^m$$
  $$r^m\ s = sr^{m(n-1)} = sr^{-m} = sr^{n-m} = s\ r^m \iff r^{n-m} = r^m \overset{(*)}{\iff} n - m = m \iff n = 2m$$

  donde en $(*)$ hemos usado que $n - m, m \in \{1, \ldots, n-1\}$. Por tanto, hay que distinguir según la paridad de n:

  - Si n es impar, entonces $r^m \notin Z(D_n)$ para todo $m \in \{1, \ldots, n-1\}$.
  - Si n es par, entonces $r^{n/2} \in Z(D_n)$, y $r^m \notin Z(D_n)$ para todo $m \in \{1, \ldots, n-1\} \setminus \{n/2\}$.

- Fijado $m \in \{0, \ldots, n-1\}$, veamos si $sr^m \in Z(D_n)$.

  $$sr^m\ r = sr^{m+1} = r^{(m+1)(n-1)}s = r^{mn-m+n-1}s = r^{n-m-1}s$$
  $$r\ sr^m = r\ r^{n-m}s = r^{n-m+1}s$$

  Por tanto, se necesita que $r^{n-m-1} = r^{n-m+1}$, y equivalentemente se necesita que $r^{-1} = r$, es decir, que $r^2 = 1$. Esto es cierto para $n = 2$, pero no para $n \geqslant 3$. Por tanto, $sr^m \notin Z(D_n)$ para todo $m \in \{0, \ldots, n-1\}$.

En resumen, tenemos que:

- Si n es impar, entonces $Z(D_n) = \{1\}$.
- Si n es par, entonces $Z(D_n) = \{1, r^{n/2}\}$.

Ejercicio 1.7.8. Sean H y K dos subgrupos finitos de un grupo G, uno de ellos normal. Demostrar que

$$|H||K| = |HK||H \cap K|.$$

Sean $H, K < G$, y $K \lhd G$. Entonces, por el Segundo Teorema de Isomorfía, se tiene que:

$$\frac{HK}{K} \cong \frac{H}{H \cap K}$$

Tomando índices y usando el Teorema de Lagrange, se tiene que:

$$\left|\frac{HK}{K}\right| = \frac{|HK|}{|K|} = \left|\frac{H}{H \cap K}\right| = \frac{|H|}{|H \cap K|} \Longrightarrow |H||K| = |HK||H \cap K|.$$

Si por el contrario $H \lhd G$, entonces:

$$\frac{HK}{H} \cong \frac{K}{H \cap K}$$

y de igual forma se llega a la misma conclusión.

Ejercicio 1.7.9. Sea G finito y $N \lhd G$. Probar que $G/N \cong G$ si, y sólo si, $N = \{1\}$, y que $G/N \cong \{1\}$ si, y sólo si, $N = G$.

Veamos que $G/N \cong G$ si, y sólo si, $N = \{1\}$.

$\Longrightarrow$) Supongamos que $G/N \cong G$. Entonces, por el Teorema de Lagrange, se tiene que:

$$|G| = |G/N| = \frac{|G|}{|N|} \Longrightarrow |N| = 1 \Longrightarrow N = \{1\}.$$

$\Longleftarrow$) Supongamos que $N = \{1\}$. Definimos ahora el homomorfismo siguiente:

$$\begin{array}{rccc} f: & G & \longrightarrow & G \\ & x & \longmapsto & x \end{array}$$

Tenemos que:

$$\begin{aligned} \ker(f) &= \{x \in G \mid f(x) = 1\} = \{x \in G \mid x = 1\} = \{1\} = N, \\ Im(f) &= \{f(x) \mid x \in G\} = \{x \mid x \in G\} = G \end{aligned}$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

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

Veamos ahora que $G/N \cong \{1\}$ si, y sólo si, $N = G$.

$\Longrightarrow$) Supongamos que $G/N \cong \{1\}$. Entonces, por el Teorema de Lagrange, se tiene que:

$$1 = |G/N| = \frac{|G|}{|N|} \Longrightarrow |G| = |N|$$

Como $N \leqslant G$, se tiene que $N \subset G$, y por tanto $N = G$.

$\Longleftarrow$) Supongamos que $N = G$. Entonces, definimos el homomorfismo siguiente:

$$\begin{array}{rccc} f: & G & \longrightarrow & \{1\} \\ & x & \longmapsto & 1 \end{array}$$

Entonces, tenemos que:

$$\begin{aligned} \ker(f) &= \{x \in G \mid f(x) = 1\} = \{x \in G \mid 1 = 1\} = G = N, \\ Im(f) &= \{f(x) \mid x \in G\} = \{1 \mid x \in G\} = \{1\} \end{aligned}$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{N} \cong \{1\}$$

Observación. Notemos que en las implicaciones hacia la izquierda no es necesario suponer que G es finito. Lo usaremos por tanto sin esta restricción.

Ejercicio 1.7.10. Sean G y H dos grupos cuyos órdenes sean primos relativos. Probar que si $f : G \to H$ es un homomorfismo, entonces necesariamente $f(x) = 1$ para todo $x \in G$, es decir, que el único homomorfismo entre ellos es el trivial.

Como $|G|$ y $|H|$ son primos relativos, en particular son grupos finitos. Por ser f un homomorfismo, se tiene que $f(G) < H$, luego $|f(G)| \mid |H|$. Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{\ker(f)} \cong f(G) \implies |G| = |\ker(f)| \cdot |f(G)| \Longrightarrow |f(G)| \mid |G|$$

Como $\text{mcd}(|G|, |H|) = 1$, se tiene que $|f(G)| = 1$. Como además $f(G)$ es un grupo, se tiene que $f(G) = \{1\}$. Por tanto, f es el homomorfismo trivial.

Ejercicio 1.7.11. Sean $H, K \leqslant G$, y sea $N \lhd G$ un subgrupo normal de G tal que $HN = KN$. Demostrar que

$$\frac{H}{H \cap N} \cong \frac{K}{K \cap N}.$$

Aplicamos dos veces el Segundo Teorema de Isomorfía:

- Consideramos $H, N \leqslant G$, con $N \lhd G$. Entonces, por el Segundo Teorema de Isomorfía, se tiene que:
$$\frac{HN}{N} \cong \frac{H}{H \cap N}$$
- Consideramos $K, N \leqslant G$, con $N \lhd G$. Entonces, por el Segundo Teorema de Isomorfía, se tiene que:
$$\frac{KN}{N} \cong \frac{K}{K \cap N}$$

Como $KN = HN$ y ser congruente es una relación de equivalencia, se tiene que:

$$\frac{H}{H \cap N} \cong \frac{HN}{N} = \frac{KN}{N} \cong \frac{K}{K \cap N}$$

Ejercicio 1.7.12. Sea $N \lhd G$ tal que N y G/N son abelianos. Sea H un subgrupo cualquiera de G. Demostrar que existe un subgrupo normal $K \lhd H$ tal que K y H/K son abelianos.

Por el Segundo Teorema de Isomorfía, se tiene que $K = H \cap N \lhd H$. Como $K \subset N$ y K es un grupo, entonces $K \leqslant N$. Como N es abeliano, se tiene que K también lo es. Nos falta por ver que H/K es abeliano. Por el Segundo Teorema de Isomorfía, se tiene que:

$$\frac{H}{K} \cong \frac{HN}{N}$$

Veamos ahora que $HN/N \leqslant G/N$. Como $HN \subset G$, por definición de conjunto cociente se tiene que $HN/N \subset G/N$. Como HN/N es un grupo, se tiene que $HN/N \leqslant G/N$. Como G/N es abeliano, se tiene que HN/N también lo es. Por tanto, por el Segundo Teorema de Isomorfía, se tiene que H/K es abeliano.

Ejercicio 1.7.13. Sea G un grupo finito, y sean $H, K \leqslant G$, con $K \lhd G$ y tales que $|H|$ y $[G : K]$ son primos relativos. Demostrar que $H \subseteq K$.

Por el Segundo Teorema de Isomorfía, se tiene que:

$$\frac{H}{H \cap K} \cong \frac{HK}{K}$$

Como $HK \leqslant G$, entonces $HK/K \leqslant G/K$. Por tanto $\left|\frac{H}{H\cap K}\right| = \left|\frac{HK}{K}\right|$ divide a $\left|\frac{G}{K}\right| = [G : K]$. Por otro lado:

$$\left|\frac{H}{H \cap K}\right| = \frac{|H|}{|H \cap K|} \Longrightarrow |H| = |H \cap K| \cdot \left|\frac{H}{H \cap K}\right| \Longrightarrow \left|\frac{H}{H \cap K}\right| \mid |H|$$

Como $\text{mcd}(|H|, [G : K]) = 1$, se tiene que $\left|\frac{H}{H\cap K}\right| = 1$. Por tanto, $|H| = |H \cap K|$, y como $H \cap K \subset H$, se tiene que $H \cap K = H$. Por tanto, $H \subset K$.

Ejercicio 1.7.14. Sea G un grupo.

1. Demostrar que para cada $a \in G$ la aplicación $\varphi_a : G \to G$ definida por $\varphi_a(x) = axa^{-1}$, es un automorfismo de G. φ_a se llama automorfismo interno o de conjugación de G definido por a.

   Vemos en primer lugar que está bien definida, puesto que un grupo es cerrado para inversos y productos. Por tanto, $\varphi_a(x) \in G$ para todo $x \in G$. Veamos ahora que es un isomorfismo:

   - Para ver que es un homomorfismo:

     $$\varphi_a(xy) = a(xy)a^{-1} = axa^{-1}aya^{-1} = \varphi_a(x)\varphi_a(y) \qquad \forall x, y \in G$$

   - Para ver que es inyectiva, sean $x, y \in G$ de forma que:

     $$\varphi_a(x) = axa^{-1} = aya^{-1} = \varphi_a(y)$$

     Entonces, aplicando dos veces la propiedad cancelativa, tenemos que:

     $$axa^{-1} = aya^{-1} \Longrightarrow ax = ay \Longrightarrow x = y$$

- Para ver que es sobreyectiva, sea $y \in G$, tomamos $x = a^{-1}ya$. Entonces:

$$\varphi_a(x) = \varphi_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = aa^{-1}yaa^{-1} = y$$

Concluimos que φ_a es un automorfismo de G.

2. Demostrar que la siguiente aplicación es un homomorfismo:

$$\begin{array}{rccc} \varphi : & G & \longrightarrow & \text{Aut}(G) \\ & a & \longmapsto & \varphi_a \end{array}$$

Para esto, es necesario probar que, fijados $a, b \in G$, se tiene que:

$$\varphi_{ab} = \varphi_a \circ \varphi_b$$

Tenemos que:

$$\varphi_{ab}(x) = (ab)x(ab)^{-1} = (ab)x(b^{-1}a^{-1}) = a(bxb^{-1})a^{-1} = a\varphi_b(x)a^{-1} = \varphi_a(\varphi_b(x)) \qquad \forall x \in G$$

Por tanto, $\varphi_{ab} = \varphi_a \circ \varphi_b$. Por tanto, φ es un homomorfismo de grupos.

3. Demostrar que el conjunto de automorfismos internos de G, que se denota $\text{Int}(G)$, es un subgrupo normal de $\text{Aut}(G)$.

Para ello, en primer lugar es necesario ver que $\text{Int}(G) < \text{Aut}(G)$. Considerados $a, b \in G$, tenemos que:

$$\begin{aligned}(\varphi_a \circ \varphi_b^{-1})(x) &= \varphi_a\left(b^{-1}xb\right) = a\left(b^{-1}xb\right)a^{-1} = ab^{-1}xba^{-1} = \\ &= (ab^{-1})x(ab^{-1})^{-1} = \varphi_{ab^{-1}}(x) \qquad \forall x \in G\end{aligned}$$

Veamos ahora que $\text{Int}(G) \lhd \text{Aut}(G)$. Para ello es necesario ver que se tiene $f \circ \varphi \circ f^{-1} \in \text{Int}(G)$ para todo $f \in \text{Aut}(G)$ y $\varphi \in \text{Int}(G)$. Sea $f \in \text{Aut}(G)$ y $\varphi_a \in \text{Int}(G)$. Entonces, tenemos que:

$$\begin{aligned}(f \circ \varphi_a \circ f^{-1})(x) &= f\left(\varphi_a(f^{-1}(x))\right) = f\left(a(f^{-1}(x))a^{-1}\right) \\ &= f(a)f(f^{-1}(x))f(a^{-1}) = f(a)xf(a^{-1}) = \varphi_{f(a)}(x) \in \text{Int}(G)\end{aligned}$$

Por tanto, $f \circ \varphi_a \circ f^{-1} \in \text{Int}(G)$, y por tanto $\text{Int}(G) \lhd \text{Aut}(G)$.

4. Demostrar que $G/Z(G) \cong \text{Int}(G)$.

Buscamos aplicar el Primer Teorema de Isomorfía al homomorfismo φ del apartado 2. Tenemos que:

$$\begin{aligned}\ker(\varphi) &= \{a \in G \mid \varphi_a = \text{Id}_G\} = \{a \in G \mid \varphi_a(x) = x\ \forall x \in G\} \\ &= \{a \in G \mid axa^{-1} = x\ \forall x \in G\} = \{a \in G \mid ax = xa\ \forall x \in G\} = Z(G) \\ Im(\varphi) &= \{\varphi_a \mid a \in G\} = \{f \in \text{Aut}(G) \mid f(x) = axa^{-1}\ \forall x \in G\} = \text{Int}(G)\end{aligned}$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{Z(G)} \cong \text{Int}(G)$$

5. Demostrar que $\text{Int}(G) = \{\text{Id}_G\}$ si y sólo si G es abeliano.

$\Longrightarrow$) Supongamos que $\text{Int}(G) = \{\text{Id}_G\}$. Entonces, para todo $a \in G$, se tiene que:
$$\varphi_a = \text{Id}_G \Longrightarrow axa^{-1} = x \ \forall x \in G$$
Por tanto, $ax = xa \ \forall x \in G$. Como a es arbitrario, se tiene que G es abeliano.

$\Longleftarrow$) Supongamos que G es abeliano. Entonces, para todo $a \in G$, se tiene que:
$$\varphi_a(x) = axa^{-1} = aa^{-1}x = x \ \forall x \in G$$
Por tanto, $\varphi_a = \text{Id}_G$. Como a es arbitrario, se tiene que $\text{Int}(G) = \{\text{Id}_G\}$.

Ejercicio 1.7.15. Demostrar que el grupo de automorfismos de un grupo no abeliano no puede ser cíclico.

Sea G un grupo no abeliano. Por el recíproco del Ejercicio 1.7.4.4, sabemos que $G/Z(G)$ no es cíclico. Como $G/Z(G) \cong \text{Int}(G)$, se tiene que $\text{Int}(G)$ no es cíclico. Como $\text{Int}(G) < \text{Aut}(G)$ y todo subgrupo de un grupo cíclico es cíclico, se tiene que $\text{Aut}(G)$ no es cíclico.

Ejercicio 1.7.16. Demostrar que $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

Sabemos que:
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V^{\text{abs}} = \langle x, y \mid x^2 = y^2 = 1, xy = yx \rangle$$
Construimos ahora automorfismos de $\mathbb{Z}_2 \times \mathbb{Z}_2$. Sabemos que $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$.

Ejercicio 1.7.17. Demostrar que los grupos S_3, $\mathbb{Z}_{p^n}$ (con p primo) y $\mathbb{Z}$ no son producto directo internos de subgrupos propios.

1. S_3.

   Como $|S_3| = 6$, entonces sus subgrupos propios son de orden 2 y 3. Por reducción al absurdo, supongamos que $S_3 \cong K \times H$ con $K, H < S_3$. Entonces, $|S_3| = |K||H|$, y como $|K|$ y $|H|$ son divisores de 6, se tiene que $|K| = 2$ y $|H| = 3$. Por tanto, $K \cong C_2$ y $H \cong C_3$. Por tanto, $S_3 = K \times H \cong C_2 \times C_3$. Como C_2 y C_3 son cíclicos con $\text{mcd}(|C_2|, |C_3|) = 1$, se tiene que $C_2 \times C_3$ es cíclico. Por tanto, S_3 es cíclico, lo cual es una contradicción.

2. $\mathbb{Z}_{p^n}$.

   Por ser $\mathbb{Z}_{p^n}$ un grupo cíclico de orden p^n, todos sus subgrupos propios son cíclicos de orden p^k con $k \in \{1, \ldots, n-1\}$. Por tanto, por reducción al absurdo, supongamos que $\exists p, q \in \{1, \ldots, n-1\}$ tales que $\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^k} \times \mathbb{Z}_{p^q}$. Por ser $\mathbb{Z}_{p^k}$ y $\mathbb{Z}_{p^q}$ cíclicos, se tiene que $\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^q}$ es cíclico si y solo si $\text{mcd}(p^k, p^q) = 1$. Como p^k y p^q son potencias de un mismo primo, se tiene que $\text{mcd}(p^k, p^q) \geqslant p$. Por tanto, $\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^q}$ no es cíclico. Por tanto, $\mathbb{Z}_{p^n}$ no es producto directo interno de subgrupos propios.

3. $\mathbb{Z}$.

   Sabemos que todos los subgrupos de $\mathbb{Z}$ son de la forma $k\mathbb{Z}$, con $k \in \mathbb{N}$. Por tanto, por reducción al absurdo, supongamos que $\exists p, q \in \mathbb{N}$ tales que se tiene $\mathbb{Z} \cong p\mathbb{Z} \times q\mathbb{Z} \overset{(*)}{\cong} \mathbb{Z} \times \mathbb{Z}$. No obstante, $\mathbb{Z} \times \mathbb{Z}$ no es cíclico, y por tanto no es isomorfo a $\mathbb{Z}$. Por tanto, $\mathbb{Z}$ no es producto directo interno de subgrupos propios.

   En $(*)$, el isomorfismo es el siguiente (que se prueba fácilmente es es un isomorfismo):

$$\begin{array}{rccc} f: & n\mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & x/n \end{array}$$

Ejercicio 1.7.18. En cada uno de los siguientes casos, decidir si el grupo G es o no producto directo interno de los subgrupos H y K.

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

   Es directo que que $G = HK$ y $H \cap K = \{1\}$. Como $H, K < G$ y G es abeliano, se tiene que $H, K \lhd G$. Por tanto, $G \cong H \times K$.

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

3. $G = \mathbb{C}^\times$, $H = \{z \in \mathbb{C} \mid |z| = 1\}$, $K = \{x \in \mathbb{R} \mid x > 0\}$.

   Dado $z \in G$, podemos escribir:

$$z = \frac{z}{|z|} \cdot |z| \qquad \frac{z}{|z|} \in H,\ |z| \in K$$

   Por tanto, $G = HK$. Además, $H \cap K = \{1\}$, y como $H, K < G$ y G es abeliano, se tiene que $H, K \lhd G$. Por tanto, $G \cong H \times K$.

Ejercicio 1.7.19. Sean G, H y K grupos. Demostrar que:

1. $H \times K \cong K \times H$.

   Definimos el isomorfismo:

$$\begin{array}{rccc} f: & H \times K & \longrightarrow & K \times H \\ & (h,k) & \longmapsto & (k,h) \end{array}$$

   Vemos que f es un isomorfismo:

   - f es un homomorfismo:

$$\begin{aligned} f((h_1,k_1)(h_2,k_2)) &= f(h_1h_2, k_1k_2) = (k_1k_2, h_1h_2) \\ &= (k_1,h_1)(k_2,h_2) = f(h_1,k_1)f(h_2,k_2) \end{aligned}$$

   - f es inyectiva:

$$\begin{aligned} \ker(f) &= \{(h,k) \in H \times K \mid f(h,k) = (1,1)\} \\ &= \{(h,k) \in H \times K \mid (k,h) = (1,1)\} = \{(1,1)\} \end{aligned}$$

- f es sobreyectiva:
  Dado $(k,h) \in K \times H$, tomamos $(h,k) \in H \times K$. Entonces:

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

Por tanto, f es un isomorfismo.

2. $G \times (H \times K) \cong (G \times H) \times K$.
   Definimos el isomorfismo:

$$\begin{array}{rccc} f: & G \times (H \times K) & \longrightarrow & (G \times H) \times K \\ & (g,(h,k)) & \longmapsto & ((g,h),k) \end{array}$$

Vemos que f es un isomorfismo:

- f es un homomorfismo:

$$\begin{aligned} f((g_1,(h_1,k_1))(g_2,(h_2,k_2))) &= f(g_1g_2,(h_1h_2,k_1k_2)) \\ &= ((g_1g_2,h_1h_2),k_1k_2) = \\ &= ((g_1,h_1),k_1)((g_2,h_2),k_2) = \\ &= f(g_1,(h_1,k_1))f(g_2,(h_2,k_2)) \end{aligned}$$

- f es inyectiva:

$$\begin{aligned} \ker(f) &= \{(g,(h,k)) \in G \times (H \times K) \mid f(g,(h,k)) = ((1,1),1)\} \\ &= \{(g,(h,k)) \in G \times (H \times K) \mid ((g,h),k) = ((1,1),1)\} = \{(1,(1,1))\} \end{aligned}$$

- f es sobreyectiva:
  Dado $((g,h),k) \in (G \times H) \times K$, tomamos $(g,(h,k)) \in G \times (H \times K)$. Entonces:

$$f(g,(h,k)) = ((g,h),k) \qquad \forall (g,(h,k)) \in G \times (H \times K)$$

Por tanto, f es un isomorfismo.

Ejercicio 1.7.20. Dados isomorfismos de grupos $H \cong J$ y $K \cong L$, demostrar que $H \times K \cong J \times L$.

Sea $f : A \to K$ y $g : B \to H$ los isomorfismos. Definimos la aplicación $h : A \times B \to K \times H$ como:

$$h(a,b) = (f(a), g(b)) \qquad \forall (a,b) \in A \times B$$

Veamos que h es un homomorfismo. Fijados $(a_1,b_1),(a_2,b_2) \in A \times B$, tenemos que:

$$\begin{aligned} h((a_1,b_1)(a_2,b_2)) &= h(a_1a_2,b_1b_2) = (f(a_1a_2), g(b_1b_2)) \\ &= (f(a_1)f(a_2), g(b_1)g(b_2)) = (f(a_1),g(b_1))(f(a_2),g(b_2)) \\ &= h(a_1,b_1)h(a_2,b_2) \qquad \forall (a_1,b_1),(a_2,b_2) \in A \times B \end{aligned}$$

Por tanto, h es un homomorfismo. Veamos ahora que es inyectiva. Para ello, tenemos que:

$$\begin{aligned}\ker(h) &= \{(a,b)\in A\times B \mid h(a,b)=(1,1)\}\\ &= \{(a,b)\in A\times B \mid (f(a),g(b))=(1,1)\} =\\ &= \{(a,b)\in A\times B \mid f(a)=1 \land g(b)=1\} =\\ &= \{(1,1)\}\end{aligned}$$

Por tanto, h es inyectiva. Veamos ahora que es sobreyectiva. Dado $(k,h)\in K\times H$, tomamos $(a,b)\in A\times B$ tales que $f(a)=k$ y $g(b)=h$ (que existe por ser f,g biyectivas). Entonces:

$$h(a,b)=(f(a),g(b))=(k,h) \qquad \forall (a,b)\in A\times B$$

Por tanto, h es sobreyectiva. Concluimos que h es un isomorfismo.

Ejercicio 1.7.21. Sean H,K,L y M grupos tales que $H\times K\cong L\times M$. ¿Se verifica necesariamente que $H\cong L$ y $K\cong M$?

Sabemos que $C_2\times C_3$ es cíclico de orden 6, luego $C_2\times C_3\cong C_6$. Además, sabemos que para todo grupo G, se tiene que $G\cong G\times\{1\}$ usando como isomorfismo la aplicación:

$$\begin{array}{rccc} f: & G & \longrightarrow & G\times\{1\}\\ & x & \longmapsto & (x,1)\end{array}$$

Por tanto, $C_2\times C_3\cong C_6\cong C_6\times\{1\}$.

No obstante, $|C_2|\neq|C_6|$ y $|C_3|\neq|1|$. Por tanto, tomando $H=C_2$, $K=C_3$, $L=C_6$ y $M=\{1\}$, se tiene que $H\times K\cong L\times M$. Sin embargo, no se verifica que $H\cong L$ y $K\cong M$.

Ejercicio 1.7.22. Demostrar que no todo subgrupo de un producto directo $H\times K$ es de la forma $H_1\times K_1$, con $H_1\leqslant H$ y $K_1\leqslant K$.

Trabajamos con el grupo directo $\mathbb{Z}_2\times\mathbb{Z}_2$. El grupo $\mathbb{Z}_2$ no tiene subgrupos propios, y por tanto los subgrupos suyos son $\{0\}$ y $\mathbb{Z}_2$. Por tanto, los subgrupos de $\mathbb{Z}_2\times\mathbb{Z}_2$ que se descomponen como producto directo de subgrupos de $\mathbb{Z}_2$ son:

- $\{0\}\times\{0\}=\{(0,0)\}$
- $\{0\}\times\mathbb{Z}_2=\{(0,0),(0,1)\}$
- $\mathbb{Z}_2\times\{0\}=\{(0,0),(1,0)\}$
- $\mathbb{Z}_2\times\mathbb{Z}_2=\{(0,0),(1,0),(0,1),(1,1)\}$

No obstante, consideramos el subgrupo de $\mathbb{Z}_2\times\mathbb{Z}_2$ dado por:

$$\langle(1,1)\rangle=\{(0,0),(1,1)\} \qquad O((1,1))=\mathrm{mcm}(2,2)=2$$

Este subgrupo no es de la forma $H_1\times K_1$, con $H_1\leqslant H$ y $K_1\leqslant K$. Por tanto, no todo subgrupo de un producto directo $H\times K$ es de la forma $H_1\times K_1$, con $H_1\leqslant H$ y $K_1\leqslant K$.

Ejercicio 1.7.23. Sean H, K dos grupos y sean $H_1 \lhd H$, $K_1 \lhd K$. Demostrar que $H_1 \times K_1 \lhd H \times K$ y que

$$\frac{H \times K}{H_1 \times K_1} \cong \frac{H}{H_1} \times \frac{K}{K_1}.$$

Como $H_1 < H$ y $K_1 < K$, se tiene que $H_1 \times K_1 < H \times K$. Veamos ahora que $H_1 \times K_1 \lhd H \times K$. Para cada $(h, k) \in H \times K$ y $(h_1, k_1) \in H_1 \times K_1$, tenemos que:

$$(h, k)(h_1, k_1)(h, k)^{-1} = (hh_1h^{-1}, kk_1k^{-1}) \in H_1 \times K_1$$

por ser $H_1 \lhd H$ y $K_1 \lhd K$. Por tanto, $H_1 \times K_1 \lhd H \times K$. Para ver el isomorfismo, consideramos la siguiente aplicación:

$$\begin{array}{rrcl} f: & H \times K & \longrightarrow & \frac{H}{H_1} \times \frac{K}{K_1} \\ & (h, k) & \longmapsto & (hH_1, kK_1) \end{array}$$

Vemos que f es un homomorfismo:

$$\begin{aligned} f((h_1, k_1)(h_2, k_2)) &= f(h_1h_2, k_1k_2) = (h_1h_2H_1, k_1k_2K_1) \\ &= (h_1H_1 \cdot h_2H_1, k_1K_1 \cdot k_2K_1) = (h_1H_1, k_1K_1)(h_2H_1, k_2K_1) \\ &= f(h_1, k_1)f(h_2, k_2) \qquad \forall (h_1, k_1), (h_2, k_2) \in H \times K \end{aligned}$$

Calculamos ahora su núcleo e imagen:

$$\begin{aligned} \ker(f) &= \{(h, k) \in H \times K \mid f(h, k) = (H_1, K_1)\} \\ &= \{(h, k) \in H \times K \mid (hH_1, kK_1) = (H_1, K_1)\} = \\ &= \{(h, k) \in H \times K \mid hH_1 = H_1 \land kK_1 = K_1\} = H_1 \times K_1 \\ Im(f) &= \left\{(hH_1, kK_1) \in \frac{H}{H_1} \times \frac{K}{K_1} \mid (h, k) \in H \times K\right\} = \\ &= \left\{(hH_1, kK_1) \in \frac{H}{H_1} \times \frac{K}{K_1} \mid h \in H \land k \in K\right\} = \frac{H}{H_1} \times \frac{K}{K_1} \end{aligned}$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{H \times K}{H_1 \times K_1} \cong \frac{H}{H_1} \times \frac{K}{K_1}$$

Ejercicio 1.7.24. Sean $H, K \lhd G$ tales que $H \cap K = \{1\}$. Demostrar que G es isomorfo a un subgrupo de $G/H \times G/K$.

Definimos la aplicación:

$$\begin{array}{rrcl} f: & G & \longrightarrow & G/H \times G/K \\ & g & \longmapsto & (gH, gK) \end{array}$$

Vemos que f es un homomorfismo:

$$\begin{aligned} f(gh) &= (ghH, ghK) = (gH, gK)(hH, hK) = \\ &= f(g)f(h) \qquad \forall g, h \in G \end{aligned}$$

Calculamos su núcleo:

$$\begin{aligned}\ker(f) &= \{g \in G \mid f(g) = (H, K)\}\\ &= \{g \in G \mid (gH, gK) = (H, K)\} =\\ &= \{g \in G \mid gH = H \wedge gK = K\} = H \cap K = \{1\}\end{aligned}$$

Por tanto, tenemos que:

$$\frac{G}{\ker(f)} \cong \frac{G}{\{1\}} \cong G$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$G \cong \frac{G}{\ker(f)} \cong Im(f)$$

Como $G < G$ y f es un homomorfismo, se tiene que $Im(f) < G/H \times G/K$. Por tanto, G es isomorfo a $Im(f)$, que es un subgrupo de $G/H \times G/K$.

Ejercicio 1.7.25. Sean $H, K \lhd G$ tales que $HK = G$. Demostrar que

$$\frac{G}{H \cap K} \cong \frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{H} \times \frac{G}{K}.$$

La demostración no es directa, y la dividiremos en dos partes. Por un lado, demostraremos la primera relación de isomofía, y posteriormente veremos la segunda.

Por el Segundo Teorema de Isomorfía, tenemos que $H \cap K \lhd H, K$. Veamos ahora que $H \cap K \lhd G$. Para ello, tomamos $g \in G$ y $x \in H \cap K$. Como $G = HK$, tenemos que $g = hk$ con $h \in H$ y $k \in K$. Entonces:

$$\begin{aligned}gxg^{-1} &= (hk)x(hk)^{-1} = (hk)x(k^{-1}h^{-1}) =\\ &= h(kxk^{-1})h^{-1} \overset{(*)}{=} h\widetilde{k}h^{-1} \overset{(**)}{\in} H \cap K\end{aligned}$$

donde $(*)$ se cumple porque $H \cap K \lhd K$, por lo que $kxk^{-1} = \widetilde{k} \in K$ y $(**)$ se cumple porque $H \cap K \lhd H$, por lo que $h\widetilde{k}h^{-1} \in H$. Por tanto, $H \cap K \lhd G$, y el primer cociente tiene sentido.

Definimos la aplicación:

$$\begin{array}{rccc} f: & G & \longrightarrow & \frac{H}{H\cap K} \times \frac{K}{H\cap K} \\ & g & \longmapsto & (h(H \cap K), k(H \cap K)) \end{array}$$

Veamos que está bien definida, puesto que la descomposición no tiene por qué ser única. Sean $k_1, k_2 \in K$ y $h_1, h_2 \in H$ tales que $g = k_1h_1 = k_2h_2$. Entonces, en primer lugar vemos que $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$. Por tanto:

- $h_1 = k_1^{-1}k_2h_2$, con $k_1^{-1}k_2 \in K \cap K$ y $h_2 \in H$, por lo que $h_1(H \cap K) = h_2(H \cap K)$.
- $k_1 = k_2h_1^{-1}h_2$, con $h_1^{-1}h_2 \in H \cap H$ y $k_2 \in K$, por lo que $k_1(H \cap K) = k_2(H \cap K)$.

Por tanto, f está bien definida. Veamos que es un homomorfismo. Dados $g_1, g_2 \in G$, $\exists h_1, h_2 \in H$ y $k_1, k_2 \in K$ tales que $g_1 = h_1k_1$ y $g_2 = h_2k_2$. Entonces:

$$\begin{aligned}
f(g_1g_2) &= f(h_1k_1h_2k_2) = \\
&= (h_1h_2(H\cap K), k_1k_2(H\cap K)) = \\
&= (h_1(H\cap K), k_1(H\cap K))(h_2(H\cap K), k_2(H\cap K)) \\
&= f(g_1)f(g_2) \qquad \forall g_1, g_2 \in G
\end{aligned}$$

Calculamos su núcleo:

$$\begin{aligned}
\ker(f) &= \{g \in G \mid f(g) = (H\cap K, H\cap K)\} \\
&= \{g = hk \in G \mid (h(H\cap K), k(H\cap K)) = (H\cap K, H\cap K)\} = \\
&= \{g = hk \in G \mid h(H\cap K) = H\cap K \wedge k(H\cap K) = H\cap K\} = \\
&= \{g = hk \in G \mid h, k \in H\cap K\} \stackrel{(*)}{=} H\cap K
\end{aligned}$$

donde $(*)$ se cumple porque la inclusión $\ker f \subseteq H\cap K$ se cumple por ser $H\cap K$ cerrado para el producto; mientras que la inclusión $H\cap K \subseteq \ker f$ se cumple tomando $g = g \cdot 1$.

Veamos ahora que es sobreyectiva. Dado $(h(H\cap K), k(H\cap K)) \in \frac{H}{H\cap K} \times \frac{K}{H\cap K}$, tomamos $g = hk \in G$. Entonces:

$$f(g) = f(hk) = (h(H\cap K), k(H\cap K)) \qquad \forall g \in G$$

Por tanto, f es sobreyectiva. Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{H\cap K} \cong \frac{H}{H\cap K} \times \frac{K}{H\cap K}$$

Llegamos a este punto, tan solo nos falta probar que:

$$\frac{H}{H\cap K} \times \frac{K}{H\cap K} \cong \frac{G}{H} \times \frac{G}{K}$$

Para ello, aplicamos en primer lugar dos veces el Segundo Teorema de Isomorfía.

- $H, K < G$ y $K \lhd G$:
$$\frac{G}{K} \cong \frac{H}{H\cap K}$$
- $H, K < G$ y $H \lhd G$:
$$\frac{G}{H} \cong \frac{K}{H\cap K}$$

Por tanto, tenemos que:

$$\frac{H}{H\cap K} \times \frac{K}{H\cap K} \cong \frac{G}{K} \times \frac{G}{H}$$

Como $G/H \times G/K \cong G/K \times G/H$, tenemos que:

$$\frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{K} \times \frac{G}{H} \cong \frac{G}{H} \times \frac{G}{K}$$

Por tanto, se cumple la segunda relación de isomorfía. Concluimos que:

$$\frac{G}{H \cap K} \cong \frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{H} \times \frac{G}{K}$$

Ejercicio 1.7.26. Demostrar que si G es un grupo que es producto directo interno de subgrupos H y K, y $N \lhd G$ tal que $N \cap H = \{1\} = N \cap K$, entonces N es abeliano.

Ejercicio 1.7.27. Dar un ejemplo de un grupo G que sea producto directo interno de dos subgrupos propios H y K, y que contenga a un subgrupo normal no trivial N tal que $N \cap H = \{1\} = N \cap K$. Concluir que para $N \lhd H \times K$ es posible que se tenga

$$N \neq (N \cap (H \times \{1\})) \times (N \cap (\{1\} \times K)).$$

Ejercicio 1.7.28. Sea G un grupo finito que sea producto directo interno de dos subgrupos H y K tales que $\mathrm{mcd}(|H|, |K|) = 1$. Demostrar que para todo subgrupo $N \leqslant G$ se verifica que $N = (N \cap H) \times (N \cap K)$.

Ejercicio 1.7.29. Sea G un grupo y sea $f : G \to G$ un endomorfismo idempotente (esto es, verificando que $f^2 = f$) y tal que $Im(f) \lhd G$. Demostrar que

$$G \cong Im(f) \times \ker(f).$$

Sea la siguiente aplicación:

$$\begin{array}{rccc} \varphi : & Im(f) \times \ker(f) & \longrightarrow & G \\ & (x, y) & \longmapsto & xy \end{array}$$

Veamos que φ es un isomorfismo. Para ello, previamente veremos que para todo $x \in Im(f)$, se tiene que $f(x) = x$. Dado $x \in Im(f)$, existe $y \in G$ tal que $f(y) = x$. Entonces:

$$f(x) = f(f(y)) = f^2(y) \overset{(*)}{=} f(y) = x$$

donde en $(*)$ se cumple porque f es idempotente.

Homomorfismo

Veamos que φ es homomorfismo. Para cada $(x_1, y_1), (x_2, y_2) \in Im(f) \times \ker(f)$, tenemos que:

$$\varphi((x_1, y_1)(x_2, y_2)) = \varphi(x_1 x_2, y_1 y_2) = x_1 x_2 y_1 y_2$$
$$\varphi(x_1, y_1)\varphi(x_2, y_2) = (x_1 y_1)(x_2 y_2) = x_1 y_1 x_2 y_2$$

Veamos que $x_2 y_1 = y_1 x_2$. Es decir, que dados $x \in Im(f)$ y $y \in \ker(f)$, tenemos que $xy = yx$. Como $Im(f) \lhd G$, y $\ker f \subset G$, tenemos que $yxy^{-1} \in Im(f)$. Por lo visto anteriormente, $f(yxy^{-1}) = yxy^{-1}$. Aplicando que f es un homomorfismo (estamos demostrando que φ lo es, pero sabemos que f lo es), tenemos que:

$$yxy^{-1} = f(yxy^{-1}) = f(y)f(x)f(y^{-1}) = f(y)xf(y)^{-1} \overset{(*)}{=} 1x1 = x \Longrightarrow yx = xy$$

donde en $(*)$ se cumple porque $y \in \ker(f)$ y $x \in Im(f)$.

Por tanto, φ es un homomorfismo.

Inyectividad

Veamos que φ es inyectiva. Para ello, sean $(x_1, y_1), (x_2, y_2) \in Im(f) \times \ker(f)$ tales que $\varphi(x_1, y_1) = \varphi(x_2, y_2)$. Entonces:

$$x_1y_1 = x_2y_2 \Longrightarrow x_2^{-1}x_1 = y_2y_1^{-1} \in \ker(f) \cap Im(f)$$

Veamos ahora que $\ker(f) \cap Im(f) = \{1\}$. Sea $x \in \ker(f) \cap Im(f)$. Como $x \in \ker(f)$, tenemos que $f(x) = 1$, y como $x \in Im(f)$, $f(x) = x$. Entonces $1 = f(x) = x$, por lo que $x = 1$. Por tanto, $\ker(f) \cap Im(f) = \{1\}$, por lo que:

$$\begin{aligned} x_2^{-1}x_1 = 1 &\Longrightarrow x_1 = x_2 \\ y_2y_1^{-1} = 1 &\Longrightarrow y_1 = y_2 \end{aligned}$$

Por tanto, φ es inyectiva.

Sobreyectividad

Veamos ahora que es sobreyectiva. Dado $g \in G$, tomamos $x = f(g) \in Im(f)$ e $y = f(g^{-1})g$. Veamos en primer lugar que $y \in \ker(f)$:

$$f(y) = f(f(g^{-1})g) = f(f(g^{-1}))f(g) = f^2(g^{-1})f(g) = f(g^{-1})f(g) = f(g^{-1}g) = f(1) = 1$$

Por tanto, $y \in \ker(f)$. Veamos ahora que $\varphi(x, y) = g$. Entonces:

$$\varphi(x, y) = \varphi(f(g), f(g^{-1})g) = f(g)f(g^{-1})g = f(gg^{-1})g = f(1)g = 1g = g$$

Por tanto, φ es sobreyectiva.

Concluimos que φ es un isomorfismo. Por tanto, $G \cong Im(f) \times \ker(f)$.

Ejercicio 1.7.30. Sea S un subconjunto de un grupo G. Se llama *centralizador* de S en G al conjunto

$$C_G(S) = \{x \in G \mid xs = sx \ \forall s \in S\}$$

y se llama *normalizador* de S en G al conjunto

$$N_G(S) = \{x \in G \mid xS = Sx\}.$$

1. Demostrar que $N_G(S) \leqslant G$.

   Comprobamos las tres condiciones:

- $1 \in N_G(S)$, ya que $1S = S1 = S$.
- Sea $x, y \in N_G(S)$. Entonces $xS = Sx$ y $yS = Sy$. Entonces:

  $$(xy)S = x(yS) = x(Sy) = (xS)y = (Sx)y = S(xy)$$

  Por tanto, es cerrado para el producto.
- Sea $x \in N_G(S)$, $xS = Sx$. Entonces:

  $$xS = Sx \Longrightarrow S = x^{-1}Sx \Longrightarrow Sx^{-1} = x^{-1}S \Longrightarrow x^{-1} \in N_G(S)$$

  Por tanto, es cerrado para inversos.

2. Demostrar que $C_G(S) \lhd N_G(S)$.

   Veamos en primer lugar que $C_G(S) \leqslant N_G(S)$. Para ello, vemos en primer lugar que $C_G(S) \subseteq N_G(S)$. Fijado $x \in C_G(S)$, tenemos que $xs = sx$ para todo $s \in S$, por lo que:
   $$xS = \{xs \mid s \in S\} = \{sx \mid s \in S\} = Sx$$

   Comprobamos ahora las tres condiciones para ser subgrupo:

   - $1 \in C_G(S)$, ya que $1s = s = s1$.
   - Sea $x, y \in C_G(S)$. Entonces $xs = sx$ y $ys = sy$. Entonces:

     $$(xy)s = x(ys) = x(sy) = (xs)y = (sx)y = s(xy)$$

     Por tanto, es cerrado para el producto.
   - Sea $x \in C_G(S)$, $xs = sx$. Entonces:

     $$xs = sx \Longrightarrow S = x^{-1}Sx \Longrightarrow Sx^{-1} = x^{-1}S \Longrightarrow x^{-1} \in C_G(S)$$

     Por tanto, es cerrado para inversos.

   Comprobamos ahora que $C_G(S) \lhd N_G(S)$. Para ello, tomamos $x \in N_G(S)$ y $y \in C_G(S)$, y veamos que $xyx^{-1} \in C_G(S)$. Para ello, tomamos $s \in S$, y como $x \in N_G(S)$, tenemos que $xS = Sx$, por lo que $sx = xs'$ con $s' \in S$ y por tanto $x^{-1}sx \in S$. Entonces:

   $$yx^{-1}sx = x^{-1}sxy \Longrightarrow xyx^{-1}s = sxyx^{-1} \Longrightarrow xyx^{-1} \in C_G(S)$$

3. Demostrar que si $S \leqslant G$ entonces $S \lhd N_G(S)$.

   Sea $s \in S$. Veamos que $s \in N_G(S)$, es decir que $sS = Ss$.

   $\subset$) Sea $x \in sS$. Entonces, $\exists s' \in S$ tal que $x = ss'$. Entonces, como $ss'(s^{-1}) \in S$, tenemos que:
   $$x = ss' = ss'(s^{-1})s \in Ss$$

   $\supset$) Sea $x \in Ss$. Entonces, $\exists s' \in S$ tal que $x = s's$. Entonces, como $(s^{-1})s's \in S$, tenemos que:
   $$x = s's = ss^{-1}s's \in sS$$

Por tanto, $S \subset N_G(S)$. Como $S \subset N_G(S)$ y $S, N_G(S) < G$, tenemos que $S < N_G(S)$. Veamos ahora que $S \lhd N_G(S)$. Para ello, tomamos $x \in N_G(S)$ y $s \in S$, y veamos que $xsx^{-1} \in S$. Entonces:

$$xsx^{-1} \overset{(*)}{=} s'xx^{-1} = s' \in S$$

donde en $(*)$ hemos empleado que $x \in N_G(S)$, por lo que $xS = Sx$.

Ejercicio 1.7.31. Sea G un grupo y H y K subgrupos suyos con $H \subseteq K$. Entonces demostrar que H es normal en K si y sólo si $K < N_G(H)$. (Así, el normalizador $N_G(H)$ queda caracterizado como el mayor subgrupo de G en el que H es normal.)

$\Longrightarrow$) Sea $H \lhd K$, y veamos que $K \subset N_G(H)$. Como $H \lhd K$, tenemos que $kH = Hk$ para todo $k \in K$, luego $K \subset N_G(H)$. Como además $K, N_G(H) < G$, tenemos que $K < N_G(H)$.

$\Longleftarrow$) Sea $K < N_G(H)$, luego $K \subset N_G(H)$. Entonces, para todo $k \in K$, tenemos que $kH = Hk$. Por tanto, $H \lhd K$.

Ejercicio 1.7.32. Sea G un grupo.

1. Demostrar que $C_G(Z(G)) = G$ y que $N_G(Z(G)) = G$.

   Veamos en primer lugar que $C_G(Z(G)) = G$.

   $\subset$) Sea $x \in C_G(Z(G))$, luego trivialmente $x \in G$.

   $\supset$) Sea $x \in G$, luego $xz = zx$ para todo $z \in Z(G)$. Por tanto, $x \in C_G(Z(G))$.

   Veamos ahora que $N_G(Z(G)) = G$.

   $\subset$) Sea $x \in N_G(Z(G))$, luego trivialmente $x \in G$.

   $\supset$) Sea $x \in G$, luego $xz = zx$ para todo $z \in Z(G)$. Por tanto, $xZ(G) = Z(G)x$, luego $x \in N_G(Z(G))$.

   Análogamente, también podríamos haber usando que $G = C_G(Z(G))$ y $C_G(Z(G)) \lhd N_G(Z(G))$.

2. Si G es un grupo y $H < G$ ¿Cuándo es $G = N_G(H)$? ¿Y cuándo es $G = C_G(H)$?

   Por el ejercicio anterior, que nos caracteriza el normalizador, sabemos que:

   $$G = N_G(H) \Longleftrightarrow H \lhd G$$

   Por otro lado, sabemos que $C_G(H) = G$ si y sólo si $H \subset Z(G)$.

3. Si $H \leqslant G$ con $|H| = 2$, demostrar que $N_G(H) = C_G(H)$. Deducir que $H \lhd G$ si y sólo si $H \subset Z(G)$.

   Si $|H| = 2$, entonces $H = \{1, h\}$ con $h \in G \setminus \{1\}$, luego $h = h^{-1}$. Veamos que $N_G(H) = C_G(H)$.

   $\subset$) Sea $x \in N_G(H)$, luego $xH = Hx$. Como $xh \in Hx$, entonces hay dos opciones:

- $xh = 1$, luego $x = h^{-1}$. Por tanto, $xh = h^{-1}h = 1 = hh^{-1} = hx$.
- $xh = h$, luego $x = 1$. Por tanto, $xh = 1h = h = h1 = hx$.

En cual caso, $xh = hx$, luego $x \in C_G(H)$.

$\supset$) Como $C_G(H) \lhd N_G(H)$, se tiene.

Demostramos ahora que $H \lhd G$ si y sólo si $H \subset Z(G)$.

$\Longrightarrow$) Como $H \lhd G$, por el apartado anterior tenemos que $G = N_G(H)$. Como acacaba de ver que $N_G(H) = C_G(H)$, tenemos que $G = C_G(H)$. Por tanto, para todo $x \in G$, tenemos que $xh = hx$ para todo $h \in H$. Por tanto, $H \subset Z(G)$.

$\Longleftarrow$) Como $H \subset Z(G)$, tenemos que $C_G(H) = G$. Por tanto, se tiene que $N_G(H) = C_G(H) = G$, luego $H \lhd G$.

Ejercicio 1.7.33. Sea G un grupo arbitrario. Para dos elementos $x, y \in G$ se define su *conmutador* como el elemento

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

Observación. (El conmutador recibe tal nombre porque $[x, y]yx = xy$.)

Como $[x, y]^{-1} = [y, x]$, el inverso de un conmutador es un conmutador. Sin embargo el producto de dos conmutadores no tiene porqué ser un conmutador. Entonces se define el *subgrupo conmutador* o (primer) *subgrupo derivado* de G, denotado $[G, G]$, como el subgrupo generado por todos los conmutadores de G.

1. Demostrar que, $\forall a, x, y \in G$, se tiene que $a[x, y]a^{-1} = [axa^{-1}, aya^{-1}]$.

$$[axa^{-1}, aya^{-1}] = axa^{-1}aya^{-1}ax^{-1}a^{-1}ay^{-1}a^{-1} = axyx^{-1}y^{-1}a^{-1} = a[x, y]a^{-1}$$

2. Demostrar que $[G, G] \lhd G$.

   Tenemos que:

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

   Como $[x, y] \in G$ para todo $x, y \in G$ y $[G, G]$ es un grupo, tenemos que $[G, G] < G$. Veamos que $[G, G] \lhd G$. Para ello, tomamos $g \in G$ y $z \in [G, G]$. Entonces, como $z \in [G, G]$, tenemos que:

$$z = [x_1, y_1] \cdots [x_n, y_n] \qquad x_i, y_i \in G \ \forall i = 1, \dots, n$$

   Entonces:

$$\begin{aligned} gzg^{-1} &= g[x_1, y_1] \cdots [x_n, y_n]g^{-1} = \\ &= g[x_1, y_1]g^{-1}g[x_2, y_2]g^{-1} \cdots g[x_n, y_n]g^{-1} = \\ &= [gx_1g^{-1}, gy_1g^{-1}] \cdots [gx_ng^{-1}, gy_ng^{-1}] \in [G, G] \end{aligned}$$

3. Demostrar que el grupo cociente $G/[G,G]$, que se representa por G^{ab}, es un grupo abeliano (que se llama el abelianizado de G).

   Dados $x, y \in G$, hemos de ver que $x[G,G]y[G,G] = y[G,G]x[G,G]$. Usando el producto en el cociente, hemos de ver que:
   $$xy[G,G] = yx[G,G]$$
   Consideramos ahora $[y^{-1}, x^{-1}] \in [G,G]$. Entonces:
   $$xy[y^{-1}, x^{-1}] = xyy^{-1}x^{-1}yx = yx$$
   Por tanto, $xy[G,G] = yx[G,G]$, luego $G/[G,G]$ es abeliano.

4. Demostrar que G es abeliano si y sólo si $[G,G] = 1$.

   $\Longrightarrow$) Si G es abeliano, entonces:
   $$\begin{aligned}[G,G] &= \langle [x,y] \mid x,y \in G\rangle = \langle xyx^{-1}y^{-1} \mid x,y \in G\rangle = \\ &= \langle xx^{-1}yy^{-1} \mid x,y \in G\rangle = \langle 1 \mid x,y \in G\rangle = \{1\}\end{aligned}$$
   $\Longleftarrow$) Si $[G,G] = 1$, entonces dados $x, y \in G$, tenemos que $[x,y] = 1$, luego:
   $$1 = [x,y] = xyx^{-1}y^{-1} = xy(yx)^{-1} \Longrightarrow xy = yx$$
   Por tanto, G es abeliano.

5. Sea $N \lhd G$. Demostrar que el grupo cociente G/N es abeliano si y sólo si $[G,G] < N$ (así que el grupo $[G,G]$ es el menor subgrupo normal de G tal que el cociente es abeliano).

   $\Longrightarrow$) Sea G/N abeliano, y consideramos la proyección en el cociente:
   $$\begin{array}{rccc} p: & G & \longrightarrow & G/N \\ & g & \longmapsto & gN \end{array}$$
   Sabemos que p es un homomorfismo. Dados $x, y \in G$, tenemos que:
   $$p([x,y]) = p(xyx^{-1}y^{-1}) = p(x)p(y)p(x)^{-1}p(y)^{-1} = 1$$
   Por tanto, por ser p un homomorfismo, tenemos que $p([G,G]) = \{1\}$, luego $[G,G] \subseteq \ker p = N$. Por tanto, como además $[G,G]$ es un grupo, se tiene que $[G,G] < N$.

   $\Longleftarrow$) Sea $[G,G] < N$. Sean ahora $x, y \in G$, y buscamos ver que $xyN = yxN$. Tenemos que:
   $$xy[y^{-1}, x^{-1}] = xyy^{-1}x^{-1}yx = yx$$
   Como $[y^{-1}, x^{-1}] \in [G,G] < N$, tenemos que $xyN = yxN$. Por tanto:
   $$(xN)(yN) = xyN = yxN = (yN)(xN)$$
   Por tanto, G/N es abeliano.

Ejercicio 1.7.34.

1. Calcular el subgrupo conmutador de los grupos S_3, A_4, D_4 y Q_2.

2. Demostrar que, para $n \geqslant 3$, el subgrupo conmutador de S_n es A_n y que éste es el único subgrupo de S_n de orden ${}^{n!}/_{2}$.