Grupos finitos

Notas de clase de
Eugenio Miranda Palacios
para el curso 2010/2011
Adaptadas por Manuel Bullejos
para el curso 2020/2021

Índice

3. Subgrupos normales y Cocientes

Para hacer cocientes, en cualquier contexto algebraico, se necesitan relaciones de equivalencia que sean compatibles con las estructuras con las que estemos trabajando. Estas relaciones se suelen llamar congruencias (de grupos, anillos, módulos, etc. dependiendo del contexto en el que estemos) .

Una congruencia en un grupo G será por tanto una relación de equivalencia $\equiv$ en G compatible con la estructura de grupo, esto es:

- *Compatible con el producto*:

$$\left.\begin{array}{c} x \equiv y \\ z \equiv t \end{array}\right\} \Rightarrow xz \equiv yt.$$

- *Compatible con los inversos*:

$$x \equiv y \Rightarrow x^{-1} \equiv y^{-1}$$

Como es usual, la compatibilidad con los inversos se deduce de la compatibilidad con el producto.

$$\left.\begin{array}{c} x \equiv y \\ y^{-1} \equiv y^{-1} \end{array}\right\} \overset{\text{multiplicando}}{\Rightarrow} \left.\begin{array}{c} xy^{-1} \equiv 1 \\ x^{-1} \equiv x^{-1} \end{array}\right\} \overset{\text{multiplicando}}{\Rightarrow} x^{-1} \equiv y^{-1}.$$

Si $\equiv$ es una congruencia en G, podemos trasladar la estructura de grupo de G al conjunto de clases de equivalencia $G/\equiv$, definiendo el producto de clases como la clase del producto:

$$\bar{x} \cdot \bar{y} = \overline{xy}.$$

Las propiedades de congruencia permiten probar que esta operación está bien definida, además las propiedades del producto en G pasan al cociente $G/\equiv$. De manera que

$$G/\equiv$$

es un grupo, llamado **grupo cociente de G por la congruencia** $\equiv$. Además la proyección canónica

$$pr : G \twoheadrightarrow G/\equiv;\ x \mapsto \bar{x}$$

es un morfismo de grupos.

El **núcleo de la congruencia** será el núcleo de la proyección canónica pr y será un subgrupo $Ker(\equiv) = Ker(pr) \leq G$. Además este grupo determina totalmente a la congruencia ya que

$$x \equiv y \Leftrightarrow xy^{-1} \equiv 1 \Leftrightarrow xy^{-1} \in Ker(\equiv). \Leftrightarrow x \sim_{Ker(\equiv)} y$$

Y análogamente,

$$x \equiv y \Leftrightarrow y^{-1}x \equiv 1 \Leftrightarrow y^{-1}x \in Ker(\equiv). \Leftrightarrow x \,{}_{Ker(\equiv)}\!\sim y$$

Estos grupos tienen una propiedad muy característica que reflejamos en la siguiente

Proposición 3.1. *Dado un subgrupo $H \leq G$ son equivalentes las siguientes propiedades:*

1. *Las clases derecha coinciden con las clases izquierda, i.e. $\forall x \in G,\ xH = Hx$.*
2. *$\forall x \in G, xH \subseteq Hx$.*
3. *El único conjugado de H es el propio H, i.e. $\forall x \in G, xHx^{-1} = H$.*
4. *$\forall x \in G, xHx^{-1} \subseteq H$.*
5. *La relación ${}_H\sim$ es una congruencia.*
6. *La relación $\sim_H$ es una congruencia.*

Demostración. Probar que las cuatro primeras condiciones son equivalentes es un ejercicio sencillo, sólo hay que usar que dados subconjuntos $A \subseteq B \subseteq G$, entonces para todo $x \in G$ se tiene $xA \subseteq xB$ y $Ax \subseteq Bx$.

Veamos que 1 y 5 son equivalentes y de forma totalmente análoga se haría que 1 y 6 son equivalentes.

Si 1 es cierta, entonces

$$\left.\begin{array}{l} x\ {}_H\sim y \Leftrightarrow y^{-1}x \in H \Leftrightarrow x \in yH \\ z\ {}_H\sim t \Leftrightarrow z^{-1}t \in H \Leftrightarrow t \in zH \end{array}\right\} \Rightarrow xt \in yHzH = yzHH = yzH \Leftrightarrow xt\ {}_H\sim yz.$$

Recíprocamente, supongamos que 5 es cierta, y que $z \in xH$, entonces $x^{-1}z \in H$ y por tanto $z\ {}_H\sim x$, pongamos entonces

$$\left.\begin{array}{c} z\ {}_H\sim x \\ x^{-1}\ {}_H\sim x^{-1} \end{array}\right\} \Rightarrow zx^{-1}\ {}_H\sim xx^{-1}, = 1 \Leftrightarrow zx^{-1} \in H \Leftrightarrow z \in Hz..$$

Análogamente si $z \in xH$ deducimos que $z \in Hx$. □

Definición 3.2. Diremos que un subgrupo $H \leq G$ es normal si cumple cualquiera de las seis condiciones equivalentes dadas en la Proposición 3.1.

Si H es normal en G lo indicaremos $H \trianglelefteq G$. La normalidad no es transitiva.

Observación 3.1. El subgrupo trivial es siempre normal, $1 \trianglelefteq G$, y el total también, $G \trianglelefteq G$.

Observación 3.2. Es claro que el núcleo de cualquier morfismo de grupos $f : G \to G'$ es un subgrupo normal $Ker(f) \trianglelefteq G$ y por tanto cualquier congruencia de grupos es la congruencia asociada a un subgrupo normal.

Observación 3.3. Si $H \trianglelefteq G$ es un subgrupo normal entonces las clases por la derecha y las clases por la izquierda coinciden y por tanto los conjuntos cocientes $G/\ {}_H\sim$ y $G/\sim_H$ tambien coinciden. En este caso denotaremos

$$G/H = G/\ {}_H\sim\ = G/\sim_H$$

y lo llamaremos **grupo cociente de G sobre H**. Además, puesto que ${}_H\sim = \sim_H$ es una congruencia, la estructura de grupo de G pasa al cociente G/H y la proyección canónica $pr : G \twoheadrightarrow G/H$ es un morfismo de grupos con núcleo H.

Teorema: Si un grupo es abeliano ⇒ todo subgrupo es normal.

Observación 3.4. Los elementos de un grupo cociente G/H serán las clases derecha o izquierda de elementos de G y por tanto serán denotados por xH o Hx según nos convenga.

Como consecuencia de estas dos observaciones podemos concluir la siguiente

Proposición 3.3. *Toda congruencia es la congruencia asociada a un subgrupo normal y todo subgrupo normal es el núcleo de una congruencia.*

Y como consecuencia de esta última Proposición 3.3 tenemos

Corolario 3.4. *Un subgrupo $H < G$ es un subgrupo normal de G si y sólo si existe un homomorfismo $f : G \to G'$ tal que $H = \ker(f)$.*

Ejercicio 3.1. Dado un morfismo de grupos $f : G \to G'$ las aplicaciones $f_* : \mathcal{P}(G) \to \mathcal{P}(G')$ y $f^* : \mathcal{P}(G') \to \mathcal{P}(G)$ llevan subgrupos en subgrupos. Además f^* lleva subgrupos normales en subgrupos normales pero f_* lleva subgrupos normales en normales sólo cuando f es un epimorfismo.

3.1. Los teoremas de isomorfía

3.1.1. La propiedad universal de la proyección al cociente. El primer teorema de isomorfía

Dado un subgrupo normal $K \trianglelefteq G$ la proyección canónica $pr : G \twoheadrightarrow G/K$ tiene la siguiente propiedad universal:

> *Dar un morfismo $\bar{f} : G/K \to G'$ es equivalente a dar un morfismo $f : G \to G'$ que lleve todos los elementos de K en 1.*

Sintetizamos esta propiedad en el siguiente diagrama:

$$\begin{array}{ccccc} K & \xhookrightarrow{i} & G & \xrightarrow{pr} & G/K \\ & \searrow^{fi=1} & \downarrow{\scriptstyle \forall f} & \swarrow_{\exists! \bar{f}} & \\ & & G' & & \end{array} \qquad \bar{f}(xK) := f(x)$$

Si partimos ahora de un morfismo de grupos $f : G \to G'$ y tomamos como $K = Ker(f)$ es claro que existe $\bar{f} : G/Ker(f) \to G'; \bar{f}(xKer(f)) = f(x)$ y que es inyectiva. Por tanto esta $\bar{f}$ induce un isomorfismo $b : G/Ker(f) \to Im(f)$ que claramente hace conmutar el siguiente diagrama:

$$\begin{array}{ccc} G & \xrightarrow{pr} & G/Ker(f) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle b\cong} \\ G' & \xleftarrow{\qquad} & Im(f) \end{array} \tag{3.1}$$

Esto es lo que nos dice el primer teorema de isomorfía

Ejercicio 3.1. Dado un morfismo de grupos $f : G \to G'$ las aplicaciones $f^* : \mathcal{P}(G) \to \mathcal{P}(G')$ y $f^* : \mathcal{P}(G') \to \mathcal{P}(G)$ llevan subgrupos en subgrupos. Además f^* lleva subgrupos normales en subgrupos normales pero f_* lleva subgrupos normales en normales sólo cuando f es un epimorfismo.

Probamos :

$H \trianglelefteq G \Rightarrow f_*(H) \trianglelefteq G'$

$H \trianglelefteq G$, f^* epimorfismo $\Rightarrow f_*(H) \trianglelefteq G'$

Sea $x \in f^*(H') \Rightarrow f(x) \in H'$

$g \in G$

$gxg^{-1} \overset{??}{\in} f^*(H') \iff f(gxg^{-1}) \in H'$

$1) \to$ morfismo

$f(g)f(x)f(g^{-1}) \in H'$

Teorema 3.5 (Primer teorema de isomorfía)**.**
Dado un morfismo $f : G \to G'$ existe un isomorfismo

$$b : G/Ker(f) \xrightarrow{\cong} Im(f);\ b(xKer(f)) = f(x),$$

que hace conmutar el diagrama 3.1.

3.1.2. Subgrupos de un cociente. El tercer teorema de isomorfía

Sea $K \trianglelefteq G$ un subgrupo normal, nos ocupamos ahora de ver como son los subgrupos (normales o no) del grupo cociente G/K.

Para ello consideramos la proyección canónica $pr : G \twoheadrightarrow G/K$, y la aplicaciones inducida entre los retículos de subgrupos $pr^* : Subgr(G/K) \to Subgr(G)$ y $pr_* : Subgr(G) \to Subgr(G/K)$, que por ser pr sobreyectiva ambas llevan subgrupos normales en subgrupos normales.

Observamos primero que $pr^*(1) = Ker(pr) = K$.

Además, si $\overline{H} \leq G/K$ es un grupo cualquiera y llamamos

$$H = pr^*(\overline{H}) = \{x \in G;\ pr(x) = xK \in \overline{H}\} \leq G,$$

tenemos que H es un subgrupo de G que contiene a K (que además es normal si $\overline{H}$ lo es en G/K).

Por otro lado si $H \leq G$ es un subgrupo que contiene a K, entonce K es también normal en H y

$$pr_*(H) = H/K.$$

Teorema 3.6 (Tercer teorema de isomorfía)**.** *Si $K \trianglelefteq G$ es un subgrupo normal, la proyección canónica $pr : G \twoheadrightarrow G/K$ induce un isomorfismo entre el retículo de subgrupos de G/K y el de subgrupos de G que contienen a K*

$$Subgr(G/K) \underset{pr_*}{\overset{pr^*}{\rightleftarrows}} \{H \leq G;, K \subseteq H\}$$

$$\overline{H} \longmapsto pr^*(\overline{H})$$

$$H/K \longmapsfrom H$$

Además esta biyección lleva subgrupos normales en subgrupos normales y si $K \trianglelefteq H \trianglelefteq G$ entonces se tiene

$$\frac{G/K}{H/K} \cong G/H.$$

Demostración. Para dar el isomorfismo basta considerar el morfismo

$$f : G/K \to G/H;\ xK \mapsto xH,$$

que está bien definido por estar K contenido en H, observar que $ker(f) = H/K$ e $Im(f) = G/H$ y aplicar el primer teorema de isomorfía. □

3.1.3. El segundo teorema de Isomorfía

Spongamos ahora que tenemos dos subgrupos $H, K \leq G$ de un grupo, vamos a denotar

$$HK = \{hk; h \in H, k \in K\},$$

este conjunto claramente contiene a H yK. En general no tiene porqué ser un subgrupo de G, pero siempre está contenido en el compuesto de H yK,

$$H, K \subseteq HK \subseteq H \vee K.$$

Notar que $HH = H$.

Proposición 3.7. *Dados subgrupos $H, K \leq G$ el conjunto HK es un subgrupo de G si, y sólo si, $HK = KH$, en cuyo caso $HK = H \vee K$.*

Demostración. Si $HK \leq G$ es un subgrupo, claramente contiene a H y K y es el menor subgrupo que contiene a ambos, así para todo $h \in H$ y $k \in K$ se tiene $h, k \in HK$ y por ser subgrupo $kh \in HK$ por lo que $KH \subseteq HK$. Supongamos ahora $hk \in HK$, pongamos

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

ahora $k^{-1}h^{-1} \in KH \subseteq HK$ por lo que existirán $h_1 \in H$ y $k_1 \in K$ tal que $k^{-1}h^{-1} = h_1k_1$ entonces

$$hk = ((hk)^{-1})^{-1} = (k^{-1}h^{-1})^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH.$$

y tenemos $HK \subseteq KH$.

Recíprocamente, si $HK = KH$ entonces este conjunto claramente tiene al 1 y es cerrado para el producto ya que

$$(h_1k_1)(h_2k_2) \in (HK)(HK) = H(KH)K = H(HK)K = HHKK = HK.$$

□

Corolario 3.8. *Si $H \leq G$ y $K \trianglelefteq G$ entonces $HK = KH$ y oir tanto HK es un subgrupo de G.*

Demostración. Dado un elemento $hk \in HK$, por ser K normal, podemos escribir $hkh^{-1} = k_1 \in K$, así $hk = k_1h \in KH$. Si por el contrario partimos de $kh \in KH$, de nuevo por ser K normal, podemos escribir $h^{-1}kh = k_2 \in K$ y por tanto $kh = hk_2 \in HK$. □

Teorema 3.9 (Segundo teorema de isomorfismo)**.**

Sea G un grupo, sean H y K subgrupos de G con $K \trianglelefteq G$. Entonces: $H \cap K \trianglelefteq H$ y existe un isomorfismo

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

dado por $h(H \cap K) \mapsto hK$.

El segundo teorema de isomorfismo se conoce también como *teorema del paralelogramo*

Demostración. Consideramos la composición

$$\alpha = pi : H \xrightarrow{i} G \xrightarrow{p} G/K$$

donde i es la inclusión y p la proyección canónica. Calculamos el núcleo

$$\begin{aligned}\ker(\alpha) = \{h \in H \mid \alpha(h) = 1\} = \{h \in H \mid p(h) = hK = 1K\} \\ = \{h \in H \mid h \in K\} = H \cap K.\end{aligned}$$

Por ser un núcleo, $H \cap K = Ker(\alpha) \trianglelefteq H$.

La imagen $\mathrm{Im}(\alpha)$ del morfismo anterior es el grupo de las clases de elementos de H, luego es HK/K.

Por el primer teorema de isomoría,

$$H/(H \cap K) \cong (HK)/K \text{ con } h(H \cap K) \mapsto hK.$$

□

3.1.4. El cuarto teorema de isomorfía, Lema de Zassenhaus o de la mariposa

Comenzamos con el siguiente

Lema 3.10 (Ley modular)**.** *Dados A, B, C subgrupos de un grupo G tales que $A < C$ se verifica que $A(B \cap C) = (AB) \cap C$.*

Demostración. Todo $z \in A(B \cap C)$ se expresa como $z = ax$ con $a \in A$, $x \in B \cap C$, luego $z = ax \in B$ y $z = ax \in C$ ya que $A < C$. Por tanto $z = ax \in (AB) \cap C$.

Para todo $c \in (AB) \cap C$, $c = ab$ con $a \in A$ y $b \in B$, así que $b = a^{-1}c \in C$ y por tanto $b \in B \cap C$. Luego $c = ab \in A(B \cap C)$. □

Teorema 3.11 (Cuarto teorema de isomorfismo. Lema de Zassenhaus o de la mariposa)**.**

Dados un grupo G y subgrupos suyos H, H', K, K' tales que $H' \lhd H < G$ y $K' \lhd K < G$, entonces $K'(H' \cap K) \lhd K'(H \cap K)$, $H'(H \cap K') \lhd H'(H \cap K)$ y existen isomorfismos

$$\frac{K'(H \cap K)}{K'(H' \cap K)} \cong \frac{H \cap K}{(H \cap K')(H' \cap K)} \cong \frac{H'(H \cap K)}{H'(H \cap K')}$$

El cuarto teorema de isomorfismo se suele llamar *lema de Zassenhaus* o también *lema de la mariposa*.

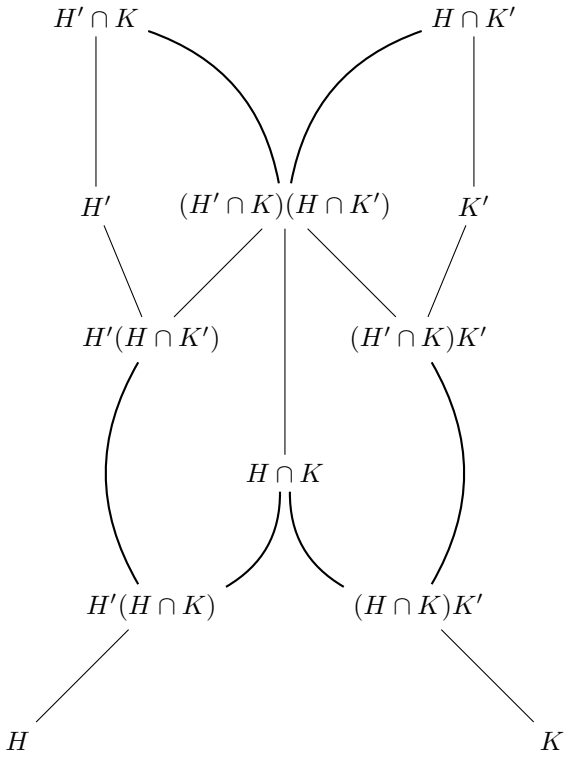
Demostración. Aplicamos el teorema 3.9 a los grupos K' y $H \cap K$. Como $K' < K$, $K' \cap (H \cap K) = H \cap K'$ y $(H \cap K')(H' \cap K) \lhd H \cap K$ ya que $K'(H \cap K)/K' \cong H \cap K / H \cap K'$, se deduce que $H \cap K' \lhd H \cap K$ y simétricamente $H' \cap K \lhd H \cap K$. En el isomorfismo anterior el subgrupo $(H \cap K')(H' \cap K)$ por la ley modular. Luego $K'(H' \cap K) \lhd K'(H \cap K)$. Aplicando el teorema del doble cociente obtenemos

$$\frac{K'(H \cap K)}{K'(H' \cap K)} \cong \frac{H \cap K}{(H' \cap K)(H \cap K')}$$

El resto sigue por simetría. □

Demostración alternativa. Basta demostrar el primer isomorfismo debido a la simetría del enunciado. Consideramos los grupos $A = K \cap H$, $B = K'(K \cap H')$. Entonces $BA = K'(K \cap H')(K \cap H) = K'(K \cap H)$ ya que $K \cap H' < K \cap H$. Además $B \cap A = (K'(K \cap H')) \cap (K \cap H) = (K'(K \cap H')) \cap H = (K' \cap H)(K \cap H')$. Aplicando el segundo teorema de isomorfismo queda el resultado buscado. □

El cuarto teorema de isomorfismo puede visualizarse en el siguiente diagrama:



3.2. Subgrupos interesantes de un grupo.

3.2.1. El centro de un grupo

Sea G un grupo y sea $x \in G$ un elemento suyo fijo. Definimos la aplicación *conjugación por* x como

$$\varphi_x : G \to G \qquad \forall g \in G,\ \varphi_x(g) = xgx^{-1}.$$

Esta aplicación es un morfismo y además se satisface que $\varphi_{xy} = \varphi_x\varphi_y$, de manera que φ_x es un automorfismo con inverso $\varphi_{x^{-1}}$ tenemos por tanto un morfismo de grupos

$$\varphi : G \to \mathrm{Aut}(G).$$

La imagen de este morfismo será llamado el *subgrupo de automorfismos interiores de* G, que denotaremos

$$\mathrm{In}(G) = Im(\varphi) = \{\varphi_x \mid x \in G\} \leq \mathrm{Aut}(G).$$

Es fácil de comprobar que para todo automorfismo $f \in \mathrm{Aut}(G)$ y para todo $x \in G$ se tiene que $f\varphi_x f^{-1} = \varphi_{f(x)}$ y por tanto $\mathrm{In}(G)$ es un subgrupo normal de $\mathrm{Aut}(G)$.

El núcleo de φ consiste en los elementos $x \in G$ tales que para todo $g \in G$ se tiene que $\varphi_x(g) = xgx^{-1} = g$ o equivalentemente $xg = gx$, este subgrupo normal de G se llamará *centro* de G y lo denotaremos

$$Z(G) = \ker(\varphi) = \{x \in G \mid xg = gx\ \forall g \in G\},$$

es decir, el conjunto de los elementos de G que conmutan con todos los elementos de G.

Evidentemente G es abeliano si y sólo si $G = Z(G)$.

En general $Z(G)$ puede ser trivial (por ejemplo para $G = S_n$, $n \geq 3$). Pero algunos tipos especiales de grupos (grupos abelianos, p-grupos, grupos nilpotentes) tienen siempre un centro no trivial. Para grupos abelianos es evidente. En los otros casos lo demostraremos más adelante.

Si aplicamos el primer teorema de isomorfía al morfismo φ tenemos:

$$G/Z(G) \cong \mathrm{In}(G).$$

3.2.2. Centralizadores y normalizadores

El concepto de centro de un grupo admite dos generalizaciones interesantes:

Definición 3.12. Sea S un subconjunto de un grupo G. Llamamos *centralizador de* S *en* G al conjunto

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

Llamamos *normalizador de* S *en* G al conjunto

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

Es fácil de comprobar que tanto el centralizador como el normalizador son subgrupos de G.

Además, si $S = H$ es un subgrupo de G, entonces H es un subgrupo normal de $N_G(H)$.

$$H \trianglelefteq N_G(H) \leq G.$$

Además $N_G(H)$ es el mayor subgrupo de G en el que H es normal y por tanto H es normal en G si, y sólo si, $N_G(H) = G$.

3.3. Presentaciones de un grupo

Dar una definición precisa de presentación de un grupo requiere una definición precisa del grupo libre y algunos resultados complejos sobre estos. En esta sección vamos a dar una aproximación al concepto de presentación de un grupo pero no vamos a ser totalmente formales, dejaremos los resultados sobre grupos libres sin demostrar. Podéis consultar [2] o [9] para tener una aproximación algo más precisa.

Definición 3.13. Dado un grupo G y un subconjunto $S \subseteq G$ diremos que S es un conjunto de generadores de G (o bien que S genera G) si $G = \langle S \rangle$.

Para ver más explícitamente que significa que S genere a G, introducimos el siguiente concepto

Definición 3.14. Una palabra en los elementos de $S \subseteq G$ es una expresión de la forma

$$w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_r^{\epsilon_r},$$

con $\epsilon_i = \pm 1$ y $r \leq 0$. Identificaremos x_i^1 con $x_i, \forall i = 0, \dots r$.

Admitimos como palabra a la palabra vacía, que es aquella en la que $r = 0$, e identificaremos a la palabra vacía con el elemento neutro $1 \in G$.

Observación 3.5. Es fácil comprobar que $\langle S \rangle$ es el subconjunto de elementos de G que se pueden poner como palabras en los elementos de S y por tanto S es un conjunto de generadores de G si todo elemento de G se puede poner como una palabra en los elementos de S.

Definición 3.15. Una palabra es reducida si en ella no aparecen secuencias del tipo xx^{-1} o $x^{-1}x$.

Observación 3.6. Simplificado secuencias del tipo xx^{-1} o $x^{-1}x$ se puede llegar desde una palabra cualquiera a una reducida, de forma que S genera G si todo elemento de G se puede escribir como una palabra reducida en S.

Definición 3.16. Diremos que los elementos de un subconjunto $S \subseteq G$ son independientes si la única palabra reducida en S que es igual a 1 es la palabra vacía.

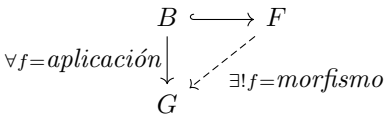
Definición 3.17. Una base para un grupo G será un subconjunto $B \subseteq G$ que generan G y cuyos elementos son independientes. Diremos que un grupo es libre si tiene una base.

Teorema 3.18. *Si F es un grupo libre, todas sus bases tienen el mismo cardinal que será un invariante del grupo llamado rango, $rg(F)$.*

Observación 3.7.

- No todo grupo es libre. Por ejemplo si G es un grupo finito, entonces todo elemento $x \in G$ tiene orden finito y por tanto la palabra $x^{o(x)}$ es una palabra reducida que es trivial y no es vacía, por tanto x no puede estar en una base de G.
- $\mathbb{Z}$ en notación aditiva o C_∞ en notación multiplicativa es libre. De rango 1.
- Un grupo libre de rango mayor que 1 no puede ser abeliano.

Teorema 3.19 (Propiedad Universal del grupo libre)**.**
Si F es un grupo libre y B es una base de F entonces dar un morfimo de F en cualquier grupo G es equivalente a dar las imágenes de los elementos en la base B, expresamos esta propiedad mediante el siguiente diagrama:



Y como corolario tenemos:

Corolario 3.20. *Dos grupos libres con el mismo rango son isomorfos.*

Los siguientes dos teoremas nos permiten establecer el concepto de presentación de un grupo.

Teorema 3.21 (Nielsen-Schreier)**.** *Todo subgrupo de un grupo libre es libre. Además, si* F *es libre de rango n todo subgrupo suyo es libre de rango menor o igual a n.*

Teorema 3.22. *Todo grupo es isomorfo a un grupo cociente de un grupo libre. Además todo grupo finito (o finitamente generado) es isomorfo a un cociente de un grupo libre de rango finito.*

Básicamente dar una presentación de un grupo es poner el grupo como un cociente de un grupo libre. Más concretamente, sea G un grupo que suponemos finito, por el Teorema 3.22 debe existir un grupo libre F de rango finito, un subgrupo normal suyo $K \trianglelefteq F$ y un morfismo $f : F \to G$ sobreyectivo que induzca un isomorfismo $\bar{f} : F/K \to G$. Podemos encontrar una base $B = \{e_1, e_2, \ldots, e_n\}$ de F y otra $B' = \{r_1, r_2, \ldots, r_s\}$ de K. Además cada r_j será una palabra en los e_i. Indiquemos esto de la siguiente forma:

$$r_j = w_i(e_1, \ldots, e_r), j = 1, \ldots, s.$$

Llamemos ahora $x_i = f(e_i), i = 1, \ldots, r$, entonces tendremos que G está generado por los x_i, $G = \langle x_1, \ldots, x_r \rangle$, y las imágenes por f de los r_j han de ser triviales, $f(r_j) = w_j(x_1, \ldots, x_r) = 1$. Estos datos determinan salvo isomorfismo a G y escribiremos:

$$G = \langle x_1, \ldots x_r;\ w_1(x_1, \ldots x_r) = 1, \ldots, w_s(x_1, \ldots x_r) = 1 \rangle.$$

Diremos que la expresión anterior es una *presentación* de G, a los elementos $x_1, \ldots x_r$ los llamaremos generadores de G y a las ecuaciones $w_1(x_1, \ldots x_r) = 1, \ldots, w_s(x_1, \ldots x_r) = 1$ las llamaremos relaciones o relatores de G.

Puesto que dar una presentación de un grupo G es poner este como un cociente de un grupo libre, utilizando las propiedades universales de los grupos libres y de los grupos cocientes tenemos el siguiente

Teorema 3.23. *(Dick)*
Dado un grupo por una presentación

$$G = \langle x_1, \ldots x_r;\ w_1(x_1, \ldots x_r) = 1, \ldots, w_s(x_1, \ldots x_r) = 1 \rangle.$$

Dar un morfismo $f : G \to H$ es equivalente a elegir elementos de H,

$$h_1 = f(x_1), \ldots, h_r = f(x_r) \in H$$

que cumplan las relaciones

$$w_1(h_1, \ldots h_r) = 1, \ldots, w_s(h_1, \ldots h_r) = 1$$

en H.

3.4. Más sobre el Producto directo de grupos

Como vimos en la sección 1.5, dados dos grupos H y K el conjunto producto cartesiano $H \times K$ con la operación definida por componentes:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$$

tiene estructura de grupo, con elemento neutro $(1, 1)$ e inversos $(h, k)^{-1} = (h^{-1}, k^{-1})$.

De esta forma obtenemos el producto directo de H y K.

En esta sección vamos a estudiar más profundamente estos grupos.

Notemos primero que tenemos cuatro aplicaciones interesantes entre H, K y $H \times K$:

$$\begin{array}{ll} p_1 : H \times K \to H & p_1(h, k) = h \\ p_2 : H \times K \to K & p_2(h, k) = k \\ i_1 : H \to H \times K & i_1(h) = (h, 1) \\ i_2 : K \to H \times K & i_2(k) = (1, k) \end{array}$$

Estas aplicaciones reciben el nombre de *primera proyección, segunda proyección, primera inyección y segunda inyección* respectivamente. Indicamos en el siguiente Lema 3.24 propiedades de estas aplicaciones, cuyas demostraciones son rutinarias.

Lema 3.24.

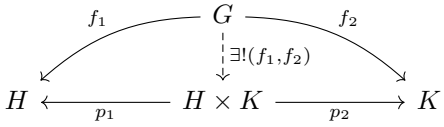
1. *Las cuatro aplicaciones anteriores son homomorfismos de grupos.*
2. $p_j i_j = Id$ *para* $j = 1, 2$*;* $p_j i_k$ *es trivial para* $j \neq k$*.*
3. p_j *es sobre e* i_j *es inyectiva para* $j = 1, 2$*.*
4. $H' = Im(i_1) = Ker(p_2) = \{(h, 1) \mid h \in H\}$ *es un subgrupo normal de* $H \times K$*, además* $H' \cong H$*.*
5. $K' = Im(i_2) = Ker(p_1) = \{(1, k) \mid k \in K\}$ *es un subgrupo normal de* $H \times K$*, además* $K' \cong K$*.*
6. $H' \cap K' = 1$*. Además,* $\forall x \in H', y \in K'$ *tenemos* $xy = yx$*.*
7. $H'K' = H \times K$*.*

La propiedad universal del producto cartesiano se extiende al contexto de grupos, de manera que el producto directo de grupos satisface la siguiente propiedad universal:

Teorema 3.25 (Propiedad universal del producto directo)**.**

Sea G un grupo arbitrario y sean $f_1 : G \to H$, $f_2 : G \to K$ dos homomorfismos de grupos cualesquiera. Existe un único homomorfismo $(f_1.f_2) : G \to H \times K$ tal que $p_1(f_1.f_2) = f_1$, $p_2(f_1.f_2) = f_2$. Indicamos esta propiedad, diciendo que

para cada f_1 y f_2 existe un único (f_1, f_2) haciendo conmutativo el siguiente diagrama:



$$(f_1, f_2)(g) := (f_1(g), f_2(g)).$$

Demostración.

1. Unicidad: Supongamos que existen algún f que verifica las condiciones del teorema. Calculemos cuanto puede valer:

$$\forall g \in G,\ f(g) = (h, k),\ h = p_1 f(g) = f_1(g),\ k = p_2 f(g) = f_2(g)$$

   Así que la única forma de definir f es $f(g) = (f_1(g), f_2(g))$.

2. Existencia: Definimos $\forall g \in G,\ (f_1, f_2)(g) = (f_1(g), f_2(g))$ por el punto anterior. Es inmediato comprobar que este es un homomorfismo y que satisface las condiciones exigidas.

□

Además la propiedad universal del producto directo lo caracteriza de forma única salvo isomorfismo, como nos indica el siguiente

Teorema 3.26. *Sea L un grupo y $l_1 : L \to H$, $l_2 : L \to K$ dos homomorfismos que verifican la propiedad:*

> *Para todo grupo G y todo par de homomorfismos $f_1 : G \to H$, $f_2 : G \to K$, existe un único homomorfismo $f : G \to L$ tal que $l_1 f = f_1$, $l_2 f = f_2$.*

Entonces $L \cong H \times K$.

Demostración. Por la propiedad universal, $\exists!(l_1, l_2) : L \to H \times K$ tal que $p_j(l_1, l_2) = l_j$, $j = 1, 2$. Por la hipótesis del presente teorema, $\exists! p : H \times K \to L$ tal que $l_j p = p_j$, $j = 1, 2$. Sustituyendo unas igualdades en otras, obtenemos:

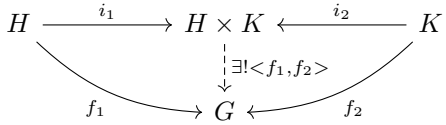
$$p_j 1_{H\times K} = p_j = l_j p = p_j(l_1, l_2)p,\ j = 1, 2 \Rightarrow (l_1, l_2)p = 1_{H\times K}$$
$$l_j 1_G = l_j = p_j(l_1, l_2) = l_j p l,\ j = 1, 2 \Rightarrow p(l_1, l_2) = 1_L$$

luego p y (l_1, l_2) son isomorfismos inversos cada uno del otro.

□

Observamos ahora que el producto directo satisface una *Segunda propiedad universal*.

Teorema 3.27. *Sea G un grupo arbitrario y sean $f_1 : H \to G$, $f_2 : K \to G$ dos homomorfismos tales que $\forall h \in H$, $\forall k \in K$, $f_1(h)f_2(k) = f_2(k)f_1(h)$. Entonces existe un único homomorfismo $f : H \times K \to G$ tal que $fi_j = f_j$, $j = 1, 2$. Indicamos esta propiedad universal mediante el siguiente diagrama:*



$$< f_1, f_2 > (h, k) := f_1(h)f_2(k).$$

Demostración.

1. Unicidad. Si $< f_1, f_2 >$ existe, satisface:

$$\begin{aligned} < f_1, f_2 > (h, k) &=< f_1, f_2 > (h, 1) < f_1, f_2 > (1, k) \\ &=< f_1, f_2 > i_1(h) < f_1, f_2 > i_2(k) = f_1(h)f_2(k) \end{aligned}$$

   luego en caso de existir es único.

2. Definimos la aplicación $< f_1, f_2 >: H \times K \to G$ así: $< f_1, f_2 > (h, k) = f_1(h)f_2(k)$. Se comprueba de inmediato que $< f_1, f_2 >$ es un homomorfismo (para lo cual hace falta la condición impuesta) y se verifica la conmutatividad del diagrama.

□

Esta segunda propiedad universal también determina de manera única al producto directo:

Teorema 3.28. *Sea L un grupo y $l_1 : H \to L$, $l_2 : K \to L$ dos homomorfismos tales que $\forall h \in H$ y $\forall k \in K$, $l_1(h)l_2(k) = l_2(k)l_1(h)$ y que verifican la propiedad:*

> *Para todo grupo G y todo par de homomorfismos $f_1 : H \to G$, $f_2 : K \to G$ tales que $\forall h \in H$ y $\forall k \in K$, $f_1(h)f_2(k) = f_2(k)f_1(h)$ existe un único homomorfismo $f : L \to G$ tal que $fl_1 = f_1$, $fl_2 = f_2$.*

Entonces $L \cong H \times K$.

Demostración. Idéntica a la del teorema 3.26, invirtiendo el sentido de las flechas.

□

Vamos ahora a caracterizar el producto directo de forma interna, de manera que hablaremos de *Producto directo interno de grupos.*

Sea G un grupo y H, K subgrupos suyos. Siempre podemos definir una aplicación

$$\phi : H \times K \to G;\ \phi(h, k) = hk$$

pero esta aplicación no tiene que ser homomorfismo ni tampoco biyectiva. Existen unas condiciones equivalentes entre sí:

Teorema 3.29 (Caracterizaciones del producto directo)**.**

Sea G un grupo, $H, K \leq G$. Las cuatro condiciones siguientes son equivalentes:

1. *La anterior aplicación ϕ es un isomorfismo.*
2. *$H, K \trianglelefteq G$, $HK = G$ y $H \cap K = 1$.*
3. *$\forall h \in H \ \forall k \in K \Rightarrow hk = kh$, $H \vee K = G$ y $H \cap K = 1$.*
4. *$\forall h \in H \ \forall k \in K \Rightarrow hk = kh$, y $\forall g \in G \ \exists_1 h \in H \ \exists_1 k \in K$ tales que $g = hk$.*

Demostración. La hacemos en ciclo:

$1 \Rightarrow 2$)

ϕ es sobre, luego $\forall g \in G \ \exists h \in H, k \in K$ tales que $g = \phi(h,k) = hk$ y $G = HK$.

Sea $g \in H \cap K$. Entonces $g = \phi(g,1) = \phi(1,g)$. Como ϕ es inyectiva, $(g,1) = (1,g)$ y por tanto $g = 1$.

$H = Ker(p_2\phi^{-1}) \trianglelefteq G$ y $K = Ker(p_1\phi^{-1}) \trianglelefteq G$.

$2 \Rightarrow 3$)

$\forall h \in K, \ \forall k \in K \ [h,k] = hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K = 1$ ya que $H, K \trianglelefteq G$.

$3 \Rightarrow 4$)

$\forall g \in G, \ x = h_1k_1 \cdots h_nk_n$. Como los elementos de H y K conmutan, $g = (h_1 \cdots h_n)(k_1 \cdots k_n) = hk$.

Sea $g = h_1k_1 = h_2k_2$. Entonces $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = 1$, luego $h_1 = h_2$ y $k_1 = k_2$.

$4 \Rightarrow 1$)

ϕ es biyectiva porque cada $g \in G$ se expresa de manera única como $g = hk$. Por otra parte, $\phi[(h_1,k_1)(h_2,k_2)] = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1,k_1)\phi(h_2k_2)$ y ϕ es un homomorfismo.

□

Definición 3.30. Un grupo G verificando las condiciones del teorema anterior se llama *producto directo interno* de los subgrupos H y K.

Lema 3.31. *Sean $H_1 \leq H$, $K_1 \leq K$. Entonces:*

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

Demostración.

1. El producto cartesiano $H_1 \times K_1$ es un subconjunto de $H \times K$. Es inmediato comprobar que es cerrado para el producto, la unidad y el inverso.

2. Definimos una aplicación $\psi : Aut(H) \times Aut(K) \to Aut(H \times K)$ por la regla $\psi(\alpha, \beta)(h, k) = (\alpha(h), \beta(k))$. Se comprueba fácilmente que ψ está bien definida y que s un monomorfismo.

□

No todo subgrupo de $H \times K$ es de la forma $H_1 \times K_1$, ni el monomorfismo ψ es sobre. Pero existe un caso particular importante en el que sí se verifican estas dos condiciones:

Teorema 3.32. *Sean H, K dos grupos finitos tales que $m.c.d(|H|, |K|) = 1$. Entonces:*
$\forall L \leq H \times K \ \exists_1 H_1 \leq H, \exists_1 K_1 < K$ *tales que* $L = H_1 \times K_1$.

Demostración.
Sean $H_1 = p_1(L)$, $K_1 = p_2(L)$. Evidentemente, $L \leq H_1 \times K_1$. Veamos la inversa: $\forall h \in H_1 \ \exists (h, k) \in L$. Sean $n = |H|$, $m = |K|$. Por el teorema de Bezout, $\exists r, s \in \mathbb{Z}$ tales que $mr + ns = 1$. Entonces $L \ni (h, k)^{mr} = (h^{mr}, k^{mr}) = (h^{1-ns}, 1) = (h, 1)$. Similarmente $\forall k \in K$, $(1, k) \in L$. Luego $\forall (h, k) \in H_1 \times K_1$, $(h, k) = (h, 1)(1, k) \in L$, y por tanto $H_1 \times K_1 \leq L$.

□

Lo que hemos hecho para dos grupos, se puede hacer para una familia arbitraria de grupos.

Sea $\{G_\lambda \mid \lambda \in \Lambda\}$ una familia arbitraria de grupos y sea $G = \prod_\lambda G_\lambda$ su producto cartesiano. Definimos una operación interna en G por componentes: $\forall g, h \in G, (gh)_\lambda = g_\lambda h_\lambda$.

Es fácil comprobar que G con la operación recién definida tiene estructura de grupo al que llamaremos *producto directo* de la familia de grupos G_λ.

Si $\Lambda = \{1, \ldots, n\}$ es finito, escribimos $G = G_1 \times \cdots \times G_n$. Y si todos los productos G_λ son el mismo grupo H, escribimos $G = H^\Lambda$ ($G = H^n$ si es finito) y lo llamamos *potencia directa* de H.

Tenemos *aplicaciones canónicas*, pra todo $\lambda \in \Lambda$,

$$\begin{array}{ll} p_\lambda : G \to G_\lambda, & p_\lambda(g) = g_\lambda \\ i_\lambda : G_\lambda \to G, & i_\lambda x = g \end{array}$$

donde $g_\mu = x$ si $\mu = \lambda$, $g_\mu = 1$ en otro caso.

Estas aplicaciones son las *proyecciones* y las *inyecciones* respectivamente.

Lema 3.33.

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

2. $\forall \lambda \in \Lambda$, $p_\lambda i_\lambda = 1_{G_\lambda}$. *Para* $\lambda \neq \mu$, $p_\lambda i_\mu$ *es trivial.*

3. $\forall \lambda \in \Lambda$, p_λ *es sobre y* i_λ *es inyectiva.*

4. $G'_\lambda = Im(i_\lambda) \cong G_\lambda$ *es normal en* G.

Teorema 3.34 (Propiedad universal del producto directo)**.**
Sea $\{G_\lambda \mid \lambda \in \Lambda\}$ *una familia de grupos y sea* $G = \prod_\lambda G_\lambda$ *su producto directo, con proyecciones* $p_\lambda : G \to G_\lambda$. *Para cualquier familia de homomorfismos de grupos (con el mismo conjunto de índices)* $\{f_\lambda : H \to G_\lambda\}$ *existe un único homomorfismo* $(f_\lambda)_\Lambda : H \to G$ *tal que* $\forall \lambda, f_\lambda = p_\lambda (f_\lambda)_\Lambda$. *Además, cualquier otro grupo que verifique esta propiedad es isomorfo a* G.

El teorema dice que existe un único $(f_\lambda)_\Lambda$ que hace conmutativos todos los diagramas:

$$\begin{array}{ccc} H & & \\ {\scriptstyle \exists!(f_\lambda)_\Lambda}\downarrow & \searrow^{f_\lambda} & \\ \prod_\lambda G_\lambda & \xrightarrow{p_\lambda} & G_\lambda \end{array} \qquad (f_\lambda)_\Lambda(h) := (f_\lambda(h))_\Lambda.$$

Veamos algunas propiedades específicas para productos de un número finito de grupos. Empezamos con una ley asociativa:

Teorema 3.35.

1. *Sean* G_1, G_2, G_3 *tres grupos arbitrarios. 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. *Sean* $G_1, \ldots, G_n$ *grupos. Para todo* $k = 1, \ldots, n-1$ *se verifica:*
$$(\prod_1^k G_\lambda) \times (\prod_{k+1}^n G_\lambda) \cong \prod_1^n G_\lambda.$$

Veamos ahora cual es la relación entre órdenes de grupos y el orden de su producto:

Teorema 3.36. *Sean* $G_1, \ldots, G_n$ *grupos cualesquiera y sea* $G = G_1 \times \cdots \times G_n$.

1. $|G| = |G_1| \cdots |G_n|$. *En particular,* G *es finito si y sólo si todos los* G_λ *son finitos.*

2. $\forall (g_1, \ldots, g_n) \in G$, $o((g_1, \ldots, g_n)) = m.c.m.(o(g_1), \ldots, o(g_n))$.

También podemos caracterizar el producto directo de una forma interna.

Sea G un grupo y $G_1, \ldots, G_n$ subgrupos suyos. Siempre podemos definir una aplicación
$$\phi : G_1 \times \ldots \times G_n \to G$$
así: $\phi(g_1, \ldots, g_n) = g_1 \cdots g_n$ (el producto en G). En general, ϕ no es homomorfismo ni sobre ni inyectiva. Pero como en el caso $n = 2$, tenemos:

Teorema 3.37. *Las siguientes condiciones son equivalentes:*

1. *La aplicación ϕ es un isomorfismo*
2. *Para $\lambda = 1, \ldots, n$, $G_\lambda \trianglelefteq G$, $G_1 \cdots G_n = G$ y $(G_1 \cdots G_{i-1}) \cap G_i = 1$ para $i = 2, \ldots, n$.*
3. *Para $\lambda \neq \mu$ $g_\lambda \in G_\lambda$ y $g_\mu \in G_\mu$, $g_\lambda g_\mu = g_\mu g_\lambda$; $G = G_1 \vee \cdots \vee G_n$ y $(G_1 \cdots G_{i-1}) \cap G_i = 1$ para $i = 2, \ldots, n$.*
4. *Para $\lambda \neq \mu$ $g_\lambda \in G_\lambda$ y $g_\mu \in G_\mu$, $g_\lambda g_\mu = g_\mu g_\lambda$; todo elemento $g \in G$ se expresa de manera única como $g = g_1 \cdots g_n$ donde $g_\lambda \in G_\lambda$*

De forma análoga al caso 2, tenemos

Teorema 3.38. *Sea $G_1, \ldots, G_n$ una familia finita de grupos finitos tales que sus órdenes son primos relativos dos a dos. Sea $G = \prod_1^n G_\lambda$. Entonces:*
$\forall L < G \ \exists_1 H_\lambda < G_\lambda$ *tales que* $L = H_1 \times \cdots \times H_n$.