Capítulo 10
Productos de grupos

En este capítulo vamos a investigar la construcción del producto directo y semidirecto de grupos. Este es un modo de construir un grupo G a partir de dos grupos H y K. Luego, en §10.3 vamos a definir la noción de extensión de un grupo por otro. Resulta que los productos directos y semidirectos son casos muy especiales de extensiones. En §10.4 vamos a probar que todo grupo abeliano finitamente generado es isomorfo a un producto de grupos cíclicos. Finalmente, la sección §10.5 presenta un ejemplo muy importante de grupos abelianos finitamente generados: el grupo de puntos racionales de una curva elíptica.

10.1 Productos directos

10.1.1. Definición. Para dos grupos H y K su **producto directo** (o simplemente **producto**) es el conjunto

$$H \times K := \{(h,k) \mid h \in H, k \in K\}$$

dotado de la operación

$$(h_1,k_1) \cdot (h_2,k_2) := (h_1h_2, k_1k_2).$$

Ya que H y K son grupos, $H \times K$ es también un grupo. La identidad es $(1_H, 1_K)$ y los elementos inversos son $(h,k)^{-1} = (h^{-1}, k^{-1})$.

De la misma manera, para una familia de grupos $(H_i)_{i\in I}$, se define el producto

$$\prod_{i\in I} H_i := \{(h_i)_{i\in I} \mid h_i \in H_i\}$$

respecto a la operación

$$(h_i)_{i\in I} \cdot (h'_i)_{i\in I} := (h_i \cdot h'_i)_{i\in I}.$$

Si A y B son grupos abelianos, está claro que el producto $A \times B$ es también un grupo abeliano. En general, si $(A_i)_{i\in I}$ es una familia de grupos abelianos, entonces su producto $\prod_{i\in I} A_i$ es abeliano.

10.1.2. Ejemplo. Para el producto

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0),(0,1),(1,0),(1,1)\}$$

la tabla de adición viene dada por

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Recordemos la tabla de multiplicación del grupo

$$V := \{\mathrm{id}, (1\ 2)\ (3\ 4), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3)\}.$$

$\circ$	id	$(1\ 2)\ (3\ 4)$	$(1\ 3)\ (2\ 4)$	$(1\ 4)\ (2\ 3)$
id	id	$(1\ 2)\ (3\ 4)$	$(1\ 3)\ (2\ 4)$	$(1\ 4)\ (2\ 3)$
$(1\ 2)\ (3\ 4)$	$(1\ 2)\ (3\ 4)$	id	$(1\ 4)\ (2\ 3)$	$(1\ 3)\ (2\ 4)$
$(1\ 3)\ (2\ 4)$	$(1\ 3)\ (2\ 4)$	$(1\ 4)\ (2\ 3)$	id	$(1\ 2)\ (3\ 4)$
$(1\ 4)\ (2\ 3)$	$(1\ 4)\ (2\ 3)$	$(1\ 3)\ (2\ 4)$	$(1\ 2)\ (3\ 4)$	id

Podemos convencernos a simple vista de que

$$V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

▲

10.1.3. Ejemplo. ¿Cuándo el producto de dos grupos cíclicos finitos es también cíclico? Para un elemento $(a, b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tenemos

$$\begin{aligned}\operatorname{ord}(a,b) = \min\{k \mid k\cdot(a,b) = (k\cdot a, k\cdot b) = (0,0)\} &= \min\{k \mid k \mid \operatorname{ord} a,\ k \mid \operatorname{ord} b\} \\ &= \operatorname{mcm}(\operatorname{ord} a, \operatorname{ord} b) = \frac{\operatorname{ord} a \cdot \operatorname{ord} b}{\operatorname{mcd}(\operatorname{ord} a, \operatorname{ord} b)}.\end{aligned}$$

Luego, el grupo $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ es cíclico si y solamente si este posee un elemento de orden

$$|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = mn.$$

Este elemento tiene que ser de la forma (a, b) donde a es un generador de $\mathbb{Z}/m\mathbb{Z}$ (es decir, $\operatorname{ord} a = m$) y b es un generador de $\mathbb{Z}/n\mathbb{Z}$ (es decir, $\operatorname{ord} a = n$) y además necesitamos tener $\operatorname{mcd}(m, n) = 1$. Entonces, el producto de dos grupos cíclicos es también cíclico si y solamente si los ordenes de grupos son coprimos:

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z} \iff \operatorname{mcd}(m, n) = 1.$$

Por ejemplo,

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \ncong \mathbb{Z}/4\mathbb{Z}.$$

▲

De hecho, las consideraciones de arriba pueden ser resumidas de manera más precisa.

10.1.4. Proposición (Teorema chino del resto). *Sean m y n dos números naturales coprimos. Entonces existe un isomorfismo canónico*

$$\begin{aligned}\mathbb{Z}/mn\mathbb{Z} &\xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \\ [a]_{mn} &\mapsto ([a]_m, [a]_n).\end{aligned}$$

Demostración. Consideremos el homomorfismo canónico

$$\begin{aligned}f\colon \mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \\ a &\mapsto ([a]_m, [a]_n)\end{aligned}$$

inducido por las proyecciones canónicas $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$ y $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$. Tenemos

$$\ker f = m\mathbb{Z} \cap n\mathbb{Z} = \operatorname{mcm}(m, n)\mathbb{Z}.$$

Ya que m y n son coprimos, $\text{mcm}(m,n) = mn$. Luego, f induce un monomorfismo

$$\overline{f}\colon \mathbb{Z}/mn\mathbb{Z} \xrightarrow{\cong} \text{im}\, f \rightarrowtail \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Pero

$$|\mathbb{Z}/mn\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = mn,$$

así que $\overline{f}$ tiene que ser un isomorfismo. ■

10.1.5. Corolario. *La función ϕ de Euler es multiplicativa en el sentido de que*

$$\phi(mn) = \phi(m) \cdot \phi(n), \quad \textit{si } \text{mcd}(m,n) = 1.$$

Demostración. $\phi(mn)$, $\phi(m)$, $\phi(n)$ representan el número de generadores de $\mathbb{Z}/mn\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ respectivamente. Bajo el isomorfismo

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

se ve que $[a]_{mn}$ es un generador de $\mathbb{Z}/mn\mathbb{Z}$ si y solamente si $[a]_m$ es un generador de $\mathbb{Z}/m\mathbb{Z}$ y $[a]_n$ es un generador de $\mathbb{Z}/n\mathbb{Z}$. ■

10.1.6. Proposición. *Si n es un número natural cuya factorización en primos es*

$$n = p_1^{k_1} \cdots p_\ell^{k_\ell},$$

entonces

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\ell}\right).$$

Demostración. Gracias a la multiplicatividad, tenemos

$$\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_\ell^{k_\ell}).$$

Luego de esto, se puede calcular directamente

$$\phi(p_i^{k_i}) = p_i^{k_i} \left(1 - \frac{1}{p_i}\right)$$

(véase el capítulo 4). ■

10.1.7. Ejemplo. Tenemos

$$\phi(198) = \phi(2 \cdot 3^2 \cdot 11) = \phi(2) \cdot \phi(3^2) \cdot \phi(11) = 1 \cdot 6 \cdot 10 = 60.$$

Otro ejemplo: $2018 = 2 \cdot 1009$ donde 1009 es primo, y por lo tanto $\phi(2018) = 1008$. ▲

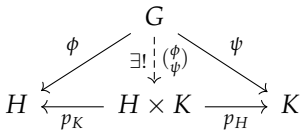
El producto directo está dotado de dos homomorfismos canónicos (proyecciones)

$$\begin{array}{ccccc} H & \xleftarrow{p_H} & H \times K & \xrightarrow{p_K} & K \\ h & \longleftarrow\!\shortmid & (h,k) & \longmapsto & k \end{array}$$

10.1.8. Observación (Propiedad universal del producto). *Sea G un grupo junto con dos homomorfismos $\phi\colon G \to H$ y $\psi\colon G \to K$. Entonces, existe una única aplicación $\binom{\phi}{\psi}\colon G \to H \times K$ tal que*

$$p_H \circ \binom{\phi}{\psi} = \phi, \quad p_K \circ \binom{\phi}{\psi} = \psi.$$

(10.1)



Demostración. A nivel de conjuntos, la única opción posible es

$$\begin{aligned}\binom{\phi}{\psi}\colon G &\to H \times K,\\ g &\mapsto (\phi(g), \psi(g)),\end{aligned}$$

y es un homomorfismo de grupos, puesto que ϕ y ψ lo son. ■

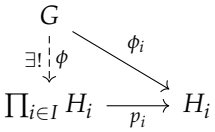
La propiedad universal del producto nos dice que los homomorfismos $G \to H \times K$ corresponden a pares de homomorfismos $G \to H$ y $G \to K$: existe una biyección *natural*

$$\begin{aligned}\mathrm{Hom}(G, H \times K) &\xrightarrow{\cong} \mathrm{Hom}(G, H) \times \mathrm{Hom}(G, K),\\ \phi &\mapsto (p_H \circ \phi, p_K \circ \phi).\end{aligned}$$

La misma propiedad universal se cumple para productos infinitos. A saber, tenemos homomorfismos canónicos de proyección

$$\begin{aligned}p_i\colon \prod_{i\in I} H_i &\to H_i,\\ (h_i)_{i\in I} &\mapsto h_i\end{aligned}$$

Si G es un grupo dotado de homomorfismos $\phi_i\colon G \to H_i$, entonces existe un homomorfismo único $\phi\colon G \to \prod_{i\in I} H_i$ tal que $p_i \circ \phi = \phi_i$:



En otras palabras, hay una biyección natural

$$\mathrm{Hom}(G, \prod_{i\in I} H_i) \cong \prod_{i\in I} \mathrm{Hom}(G, H_i).$$

10.1.9. Observación. *El producto de grupos es asociativo en el sentido de que para tres grupos H_1, H_2, H_3 hay isomorfismos naturales*

$$(H_1 \times H_2) \times H_3 \cong H_1 \times (H_2 \times H_3) \cong H_1 \times H_2 \times H_3.$$

Demostración. Sería instructivo probarlo usando únicamente las propiedades universales. Por ejemplo, el grupo

$$(H_1 \times H_2) \times H_3$$

está dotado de dos homomorfismos

$$H_1 \times H_2 \xleftarrow{p_{12}} (H_1 \times H_2) \times H_3 \xrightarrow{p_3} H_3$$

que satisfacen la propiedad universal correspondiente. Por otro lado, el grupo $H_1 \times H_2$ está dotado de dos homomorfismos

$$H_1 \xleftarrow{p_1} H_1 \times H_2 \xrightarrow{p_2} H_2$$

que satisfacen la propiedad universal correspondiente. Ahora dado un grupo G y tres homomorfismos $\phi_1 \colon G \to H_1$, $\phi_2 \colon G \to H_2$, $\phi_3 \colon G \to H_3$, existe un homomorfismo único $\phi_{12} = \binom{\phi_1}{\phi_2} \colon G \to H_1 \times H_2$ que satisface

$$p_1 \circ \phi_{12} = \phi_1, \quad p_2 \circ \phi_{12} = \phi_2$$

y luego un homomorfismo único $\phi = \binom{\phi_{12}}{\phi_3} \colon G \to (H_1 \times H_2) \times H_3$ que satisface

$$p_{12} \circ \phi = \phi_{12}, \quad p_3 \circ \phi = \phi_3.$$

En este caso

$$p_1 \circ p_{12} \circ \phi = \phi_1, \quad p_2 \circ p_{12} \circ \phi = \phi_2, \quad p_3 \circ \phi = \phi_3.$$

Entonces, $(H_1 \times H_2) \times H_3$ junto con los homomorfismos

$$p_1 \circ p_{12} \colon (H_1 \times H_2) \times H_3 \to H_1, \quad p_2 \circ p_{12} \colon (H_1 \times H_2) \times H_3 \to H_2, \quad p_3 \colon (H_1 \times H_2) \times H_3 \to H_3$$

satisface la propiedad universal de $H_1 \times H_2 \times H_3$. Por ende hay un isomorfismo

$$(H_1 \times H_2) \times H_3 \cong H_1 \times H_2 \times H_3.$$

■

10.1.10. Observación. *Existe un isomorfismo canónico $H \times K \cong K \times H$.*

Demostración. Este isomorfismo viene dado por $(h, k) \mapsto (k, h)$. También se puede notar que $H \times K$ y $K \times H$ satisfacen la misma propiedad universal (es simétrica en H y K). ■

10.1.11. Comentario. Cuando se trata de grupos *abelianos*, normalmente se habla de la **suma directa** que se denota por

$$A \oplus B = \{(a, b) \mid a \in A,\ b \in B\}.$$

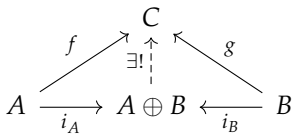
Esta viene con las inclusiones

$$\begin{aligned} i_A \colon A &\to A \oplus B, \\ a &\mapsto (a, 0) \end{aligned}$$

y

$$\begin{aligned} i_B \colon B &\to A \oplus B, \\ b &\mapsto (0, b) \end{aligned}$$

que satisfacen la propiedad universal



(donde C es también un grupo abeliano). Lo vamos a estudiar en el contexto más general para **módulos sobre anillos**.

10.1.12. Observación. *H y K se identifican con los subgrupos normales*

$$H \times \{1_K\} := \{(h, 1_K) \mid h \in H\} \quad y \quad \{1_H\} \times K := \{(1_H, k) \mid k \in K\}$$

de $H \times K$.

Demostración. Evidente de la definición del producto sobre $H \times K$. ■

10.1.13. Proposición. *Supongamos que G es un grupo y $H, K \subset G$ son dos subgrupos normales tales que $H \cap K = \{1\}$ y todo elemento de G puede ser escrito como $h\,k$ donde $h \in H$ y $k \in K$. Entonces,*

$$G \cong H \times K.$$

Demostración. Primero, notamos que $hk = kh$. En efecto, usando que H y K son normales,

$$hkh^{-1}k^{-1} = h\,(\underbrace{kh^{-1}k^{-1}}_{\in H}) = (\underbrace{hkh^{-1}}_{\in K})\,k^{-1} \in H \cap K = \{1\}.$$

Esto significa que

$$(h_1k_1) \cdot (h_2k_2) = (h_1h_2) \cdot (k_1k_2)$$

para cualesquiera $h_1, h_2 \in H$, $k_1, k_2 \in K$. También podemos comprobar que todo elemento de G se expresa *de modo único* como hk. Si tenemos $hk = h'k'$, entonces

$$h'^{-1}h = k'k^{-1} \in H \cap K = \{1\},$$

y luego $h = h'$ y $k = k'$. Todo esto significa que

$$\begin{aligned} H \times K &\to G, \\ (h, k) &\mapsto hk \end{aligned}$$

es un isomorfismo de grupos. ■

10.1.14. Comentario. Cuando G tiene dos subgrupos H y K que satisfacen las condiciones de 10.1.13, a veces se dice que G es el producto directo **interno**, mientras que la construcción de $H \times K$ de 10.1.1 se llama el producto directo **externo** de H y K.

10.1.15. Ejemplo. Todo número complejo no nulo puede ser escrito de modo único como $r\,e^{\phi\sqrt{-1}}$ donde $r > 0$ es un número real y $0 \leq \phi < 2\pi$. De aquí sigue que

$$\mathbb{C}^\times \cong \mathbb{R}_{>0} \times \mathbb{S}^1,$$

donde $\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\}$ es el grupo del círculo. ▲

10.1.16. Ejemplo. Consideremos el grupo $\mathrm{GL}_n^+(\mathbb{R})$ de matrices reales invertibles de determinante positivo. Este contiene como sus subgrupos normales el grupo $\mathrm{SL}_n(\mathbb{R})$ y el grupo de matrices escalares

$$\mathbb{R}_{>0} = \{\lambda I \mid \lambda > 0\}.$$

Toda matriz $A \in \mathrm{GL}_n^+(\mathbb{R})$ puede ser escrita como $\lambda A'$ donde $A' \in \mathrm{SL}_n(\mathbb{R})$ y $\lambda > 0$ (tomemos $\lambda = \sqrt[n]{\det A}$ y $A' = \lambda^{-1} A$). Notamos que $\mathbb{R}_{>0} \cap \mathrm{SL}_n(\mathbb{R}) = \{I\}$. Entonces,

$$\mathrm{GL}_n^+(\mathbb{R}) \cong \mathbb{R}_{>0} \times \mathrm{SL}_n(\mathbb{R}).$$

▲

10.2 Productos semidirectos

Hemos visto que un grupo G es un producto directo si y solamente si en G hay subgrupos normales H y K tales que $H \cap K = \{1\}$ y $G = HK$. Podemos considerar una colección más debil de condiciones:

1) sean N y H dos subgrupos de G donde N es normal,

2) supongamos que $N \cap H = \{1\}$,

3) supongamos que $G = NH$.

Entonces, usando el mismo argumento de 10.1.13, se deduce que todo elemento de G puede ser escrito de modo único como nh donde $n \in N$ y $h \in H$. Véamos cómo se multiplican estos elementos. Tenemos

$$(n_1h_1) \cdot (n_2h_2) = n_1\,(h_1n_2h_1^{-1}) \cdot (h_1h_2),$$

donde $h_1n_2h_1^{-1} \in N$, puesto que N es normal. Esta fórmula puede ser escrita como

$$(n_1h_1) \cdot (n_2h_2) = (n_1 \cdot I_{h_1}(n_2)) \cdot (h_1h_2), \tag{10.2}$$

donde I_{h_1} es el automorfismo de conjugación $x \mapsto h\,x\,h^{-1}$ que se restringe a N gracias a su normalidad. La fórmula (10.2) se generaliza a la siguiente construcción.

10.2.1. Definición. Sean N y H dos grupos y sea

$$\begin{aligned} \phi\colon H &\to \mathrm{Aut}(N), \\ \phi &\mapsto \phi_h \end{aligned}$$

un homomorfismo. Entonces, el **producto semidirecto** $N \rtimes_\phi H$ es el conjunto

$$N \times H = \{(n,h) \mid n \in N, h \in H\}$$

dotado de la operación

$$(n_1,h_1) \cdot (n_2,h_2) := (n_1\,\phi_{h_1}(n_2), h_1h_2). \tag{10.3}$$

10.2.2. Observación. *Respecto a la operación de arriba, $N \rtimes_\phi H$ es un grupo.*

Demostración. Primero, hay que ver que la operación es asociativa. Tenemos

$$\begin{aligned}\Big((n_1,h_1)\cdot(n_2,h_2)\Big)\cdot(n_3,h_3) &= (n_1\,\phi_{h_1}(n_2),h_1h_2)\cdot(n_3,h_3) = (n_1\,\phi_{h_1}(n_2)\,\phi_{h_1h_2}(n_3),h_1h_2h_3)\\ &= (n_1\,\phi_{h_1}(n_2)\,\phi_{h_1}\circ\phi_{h_2}(n_3),h_1h_2h_3) = (n_1\,\phi_{h_1}(n_2\,\phi_{h_2}(n_3)),h_1h_2h_3)\\ &= (n_1,h_1)\cdot(n_2\,\phi_{h_2}(n_3),h_2h_3) = (n_1,h_1)\cdot\Big((n_2,h_2)\cdot(n_3,h_3)\Big).\end{aligned}$$

Aquí hemos usado las identidades

$$\phi_{hk}=\phi_h\circ\phi_k \quad \text{y} \quad \phi_h(mn)=\phi_h(m)\,\phi_h(n)$$

para cualesquiera $h,k\in H$ y $m,n\in N$, que provienen del hecho de que $h\mapsto\phi_h$ es un homomorfismo y cada $\phi_h\colon N\to N$ es también un homomorfismo .

La identidad en $N\rtimes_\phi H$ es $(1_N,1_H)$:

$$(n,h)\cdot(1_N,1_H)=(n\,\phi_h(1_N),h\cdot 1_H)=(n,h),$$

y de la misma manera

$$(1_N,1_H)\cdot(n,h)=(1_N\cdot\phi_{1_H}(n),1_H\cdot h)=(1_N\cdot\mathrm{id}(n),h)=(n,h).$$

Los elementos inversos vienen dados por

$$(n,h)^{-1}=(\phi_{h^{-1}}(n^{-1}),h^{-1}).$$

En efecto,

$$\begin{aligned}(n,h)\cdot(\phi_{h^{-1}}(n^{-1}),h^{-1}) &= (n\,\phi_h(\phi_{h^{-1}}(n^{-1})),h\,h^{-1}) = (n\,\phi_{h\,h^{-1}}(n^{-1}),h\,h^{-1})\\ &= (n\,n^{-1},h\,h^{-1}) = (1_N,1_H)\end{aligned}$$

y también

$$\begin{aligned}(\phi_{h^{-1}}(n^{-1}),h^{-1})\cdot(n,h) &= (\phi_{h^{-1}}(n^{-1})\,\phi_{h^{-1}}(n),h\,h^{-1}) = (\phi_{h^{-1}}(n^{-1}\,n),1_H)\\ &= (\phi_{h^{-1}}(1_N),1_H) = (1_N,1_H).\end{aligned}$$

■

10.2.3. Comentario. Cuando el homomorfismo $\phi\colon H\to\mathrm{Aut}(N)$ es trivial (es decir, $\phi_h=\mathrm{id}_N$ para todo $h\in H$), entonces $N\rtimes_\phi H$ es el producto directo $N\times H$.

10.2.4. Observación. *N y H se identifican con subgrupos $N\times\{1_H\}$ y $\{1_N\}\times H$ de $N\rtimes_\phi H$. El subgrupo $N\times\{1_H\}$ es normal, y se tiene*

$$N\rtimes_\phi H/N\times\{1_H\}\cong H.$$

Demostración. Todo está claro de la fórmula del producto (10.3). Para calcular el grupo cociente $N\rtimes_\phi H/N\times\{1_H\}$, podemos considerar el homomorfismo

$$\begin{aligned}N\rtimes_\phi H &\to H,\\ (n,h) &\mapsto h\end{aligned}$$

que es sobreyectivo y tiene $N\times\{1_H\}$ como su núcleo. ■

10.2.5. Proposición. *Sea G un grupo y sean N, H sus subgrupos. Supongamos que N es normal, $N \cap H = \{1\}$ y $G = NH$. Entonces, $G \cong N \rtimes_I H$, donde $I\colon H \to \mathrm{Aut}(N)$ asocia a cada $h \in H$ el automorfismo $I_h\colon n \mapsto h\,n\,h^{-1}$.*

Demostración. De la discusión al inicio de esta sección sigue que

$$\begin{aligned} N \rtimes_I H &\to G, \\ (n,h) &\mapsto nh \end{aligned}$$

es un isomorfismo de grupos. ■

10.2.6. Ejemplo. En el grupo diédrico D_n todo elemento es de la forma r^i o bien $fr^i = r^{-i}f$. El subgrupo de rotaciones $\langle r\rangle$ es normal, siendo un subgrupo de índice 2. Además $\langle r\rangle \cap \langle f\rangle = \{\mathrm{id}\}$. En vista de lo anterior, se concluye que $D_n \cong \langle r\rangle \rtimes \langle f\rangle$, donde f actúa sobre $\langle r\rangle$ por la conjugación $r^i \mapsto frf^{-1} = r^{-i}$. ▲

10.2.7. Ejemplo. Sea V un espacio vectorial. El **grupo afín** $\mathrm{Aff}(V)$ es el grupo de aplicaciones

$$\begin{aligned} \phi_{A,u}\colon V &\to V, \\ x &\mapsto Ax + u, \end{aligned}$$

donde $A \in \mathrm{GL}(V)$ y $u \in V$. Es un subgrupo del grupo de biyecciones $V \to V$: tenemos

$$\phi_{B,v} \circ \phi_{A,v}(x) = B\,(A\,x + u) + v = BA\,x + B\,u + v = \phi_{BA,Bu+v}(x).$$

Luego, la identidad es la aplicación $\phi_{I,0}$ y los inversos vienen dados por

$$\phi_{A,u}^{-1} = \phi_{A^{-1},-A^{-1}\,u}.$$

Notamos que $\mathrm{GL}(V)$ se identifica con el subgrupo $H := \{\phi_{A,0} \mid A \in \mathrm{GL}(V)\}$ y el grupo aditivo V se identifica con el subgrupo $N := \{\phi_{I,u} \mid u \in V\}$. El último es normal. Tenemos $N \cap H = \{\phi_{I,0}\}$, y todo elemento de $\mathrm{Aff}(V)$ puede ser escrito como una composición de N y H. Se sigue que

$$\mathrm{Aff}(V) \cong V \rtimes \mathrm{GL}(V).$$

Aquí $\mathrm{GL}(V)$ actúa sobre V de la manera habitual:

$$\phi_{A,0} \circ \phi_{I,u} \circ \phi_{A,0}^{-1} = \phi_{A,0} \circ \phi_{I,u} \circ \phi_{A^{-1},0} = \phi_{I,Au}.$$

▲

10.2.8. Ejemplo. Toda matriz en el grupo $\mathrm{GL}_n(k)$ puede ser escrita como

$$A \cdot \begin{pmatrix} x & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} =: A \cdot \mathrm{diag}(x, 1, \ldots, 1)$$

donde $\det A = 1$ y $x \in k^\times$. Las matrices de determinante 1 forman un subgrupo normal $\mathrm{SL}_n(k)$, mientras que las matrices $\mathrm{diag}(x, 1, \ldots, 1)$ forman un subgrupo isomorfo a $k^\times$ (que no es normal). La intersección de estos dos subgrupos es trivial. Se sigue que

$$\mathrm{GL}_n(k) \cong \mathrm{SL}_n(k) \rtimes k^\times.$$

Aquí $x \in k^\times$ actúa sobre $\mathrm{SL}_n(k)$ mediante la conjugación por $\mathrm{diag}(x, 1, \ldots, 1)$. ▲

10.3 Sucesiones exactas cortas y extensiones

10.3.1. Definición. Una **sucesión exacta corta** de grupos es una sucesión de homomorfismos

$$1 \to H \xrightarrow{i} G \xrightarrow{p} K \to 1$$

donde

1) i es un monomorfismo,

2) p es un epimorfismo,

3) $\operatorname{im} i = \ker p$.

En este caso se dice que G es una **extensión** de K por H.

10.3.2. Comentario. En una sucesión exacta corta "1" denota el grupo trivial $\{1\}$. Los homomorfismos triviales $1 \to H$ y $K \to 1$ significan que $\ker(H \to G) = \operatorname{im}(1 \to H) = \{1\}$ e $\operatorname{im}(G \to K) = \ker(K \to 1) = K$. Cuando se trata de grupos abelianos aditivos, en lugar de "1" se escribe "0".

10.3.3. Ejemplo. Cuando hay un monomorfismo $i\colon H \rightarrowtail G$, el grupo H puede ser identificado con su imagen $i(H) \subseteq G$. Además, la condición $\operatorname{im} i = \ker p$ significa que $i(H)$ es un subgrupo normal, siendo un núcleo. El primer teorema de isomorfía implica que $G/\ker p = G/i(H) \cong K$. Entonces, esencialmente, toda sucesión exacta corta corresponde a la situación cuando H es un subgrupo normal en G, el homomorfismo $i\colon H \rightarrowtail G$ es la inclusión y el homomorfismo p es la proyección canónica sobre el grupo cociente:

$$1 \to H \xrightarrow{i} G \xrightarrow{p} G/H \to 1$$

(Note que en este caso $\operatorname{im} i = \ker p$.) ▲

10.3.4. Ejemplo. Para un producto semidirecto $N \rtimes_\phi H$ tenemos una sucesión exacta corta

$$1 \to N \xrightarrow{n \mapsto (n,h)} N \rtimes_\phi H \xrightarrow{(n,h) \mapsto h} H \to 1$$

Un caso particular es cuando ϕ es trivial y se trata del producto directo $N \times H$. ▲

10.3.5. Ejemplo. Tenemos la siguiente sucesión exacta corta:

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{[1]_2 \mapsto [2]_4} \mathbb{Z}/4\mathbb{Z} \xrightarrow{[1]_4 \mapsto [1]_2} \mathbb{Z}/2\mathbb{Z} \to 0$$

▲

10.3.6. Ejemplo. Tenemos una sucesión exacta corta

$$0 \to \mathbb{Z}/3\mathbb{Z} \xrightarrow{[1]_3 \mapsto [2]_6} \mathbb{Z}/6\mathbb{Z} \xrightarrow{[1]_6 \mapsto [1]_2} \mathbb{Z}/2\mathbb{Z} \to 0$$

y la sucesión exacta corta

$$1 \to A_3 \to S_3 \to \{\pm 1\} \to 1$$

Dado que $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ y $\{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$, ambas sucesiones exactas cortas representan extensiones de $\mathbb{Z}/2\mathbb{Z}$ por $\mathbb{Z}/3\mathbb{Z}$, pero son muy diferentes: la primera es abeliana y la segunda no lo es. ▲

10.3.7. Lema. *Consideremos un diagrama conmutativo de homomorfismos de grupos*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{i} & G & \xrightarrow{p} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & H & \xrightarrow{i'} & G' & \xrightarrow{p'} & K & \longrightarrow & 1 \end{array}$$

donde las filas son sucesiones exactas cortas. Luego, $f\colon G \to G'$ es un isomorfismo.

Demostración ("caza de diagramas"). Primero comprobemos que f es inyectivo. Si para algún $g \in G$ se cumple $f(g) = 1$, entonces $p(g) = p'(f(g)) = 1$, y por lo tanto $g \in \ker p = \operatorname{im} i$. Tenemos entonces $g = i(h)$ para algún $h \in H$. Entonces, $i'(h) = f(i(h)) = 1$. La inyectividad de h' implica que $h = 1$. En fin, $g = i(h) = 1$.

Para ver que f es sobreyectiva, tomemos $g' \in G'$. Necesitamos encontrar un elemento $g \in G$ que $f(g) = g'$. Consideremos $p'(g') \in K$. Ya que p es sobreyectivo, existe $g_1 \in G$ tal que $p(g_1) = p'(g')$. Luego,

$$p'(g' \cdot f(g_1)^{-1}) = p'(g') \cdot p' \circ f(g_1)^{-1} = p'(g') \cdot p(g_1)^{-1} = p'(g') \cdot p'(g')^{-1} = 1.$$

Podemos concluir que $g' \cdot f(g_1)^{-1} \in \ker p' = \operatorname{im} i'$ y que existe $h \in H$ tal que $i'(h) = g' \cdot f(g_1)^{-1}$. Tomemos $g := i(h) \cdot g_1$. Luego,

$$f(g) = f \circ i(h) \cdot f(g_1) = i'(h) \cdot f(g_1) = g' \cdot f(g_1)^{-1} \cdot f(g_1) = g'.$$

■

10.3.8. Comentario. El resultado de arriba tiene la siguiente generalización: en el diagrama conmutativo

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{i} & G & \xrightarrow{p} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 1 & \longrightarrow & H' & \xrightarrow{i'} & G' & \xrightarrow{p'} & K' & \longrightarrow & 1 \end{array}$$

1) si f y h son monomorfismos, entonces g es también un monomorfismo;

2) si f y h son epimorfismos, entonces g es también un epimorfismo.

En particular, si f y h son isomorfismos, g es también un isomorfismo. Esto lo he probado solo para el caso de $H' = H$, $K' = K$, $f = \mathrm{id}_H$, $h = \mathrm{id}_K$ para simplificar la notación. La versión general no nos va a servir.

10.3.9. Proposición. *Consideremos una sucesión exacta corta de grupos*

$$1 \to H \xrightarrow{i} G \xrightarrow{p} K \to 1$$

Las siguientes condiciones son equivalentes.

1) Existe un homomorfismo de grupos $r\colon G \to H$ tal que $r \circ i = \mathrm{id}_H$.

2) Existe un isomorfismo $f\colon G \xrightarrow{\cong} H \times K$ que forma parte del diagrama conmutativo

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{i} & G & \xrightarrow{p} & K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \cong\downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & H & \xrightarrow[h\mapsto(h,1)]{} & H \times K & \xrightarrow[(h,k)\mapsto k]{} & K & \longrightarrow & 1 \end{array} \tag{10.4}$$

Demostración. En la implicación 1) ⇒ 2) el isomorfismo f viene dado por

$$\begin{aligned} f\colon G &\to H \times K, \\ g &\mapsto (r(g), p(g)). \end{aligned}$$

Es un homomorfismo, puesto que r y p son homomorfismos. Es fácil comprobar que $f\colon g \mapsto (r(g), p(g))$ hace conmutar el diagrama (10.4). En fin, el lema 10.3.7 implica que f es un isomorfismo.

Para probar 2) ⇒ 1), notamos primero que la conmutatividad del segundo cuadrado significa que $f(g) = (h, p(g))$ para algún $h \in H$. Pongamos $r(g) = h$. Dado que f es un homomorfismo, r es también un homomorfismo $G \to H$. Luego, la conmutatividad del primer cuadrado significa que $r(i(h)) = h$ para todo $h \in H$. ■

10.3.10. Ejemplo. La sucesión exacta corta

$$0 \to \mathbb{Z}/3\mathbb{Z} \xrightarrow{i\colon [1]_3 \mapsto [2]_6} \mathbb{Z}/6\mathbb{Z} \xrightarrow{[1]_6 \mapsto [1]_2} \mathbb{Z}/2\mathbb{Z} \to 0$$

admite un homomorfismo $r\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ tal que $r \circ i = \mathrm{id}_{\mathbb{Z}/3\mathbb{Z}}$. Esta viene dada por $[1]_6 \mapsto [2]_3$. Esto nos da un isomorfismo $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. ▲

10.3.11. Ejemplo. Se ve que la sucesión exacta corta

$$0 \to \mathbb{Z} \xrightarrow{i\colon 1 \mapsto n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

no admite un homomorfismo $r\colon \mathbb{Z} \to \mathbb{Z}$ tal que $r \circ i = \mathrm{id}_{\mathbb{Z}}$. Y de hecho, si tal aplicación existiera, tendríamos $\mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ lo que es falso (a diferencia de $\mathbb{Z}$, el grupo $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tiene elementos no triviales de orden finito). ▲

10.3.12. Proposición. *Consideremos una sucesión exacta corta de grupos*

$$1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$$

Las siguientes condiciones son equivalentes.

1) *Existe un homomorfismo de grupos $s\colon H \to G$ tal que $p \circ s = \mathrm{id}_H$.*

2) *Existe un homomorfismo $\phi\colon H \to \mathrm{Aut}(N)$ y un isomorfismo $f\colon N \rtimes_\phi N \xrightarrow{\cong} G$ que hace parte del diagrama conmutativo*

(10.5)
$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{n \mapsto (n,1)} & N \rtimes_\phi H & \xrightarrow{(n,h) \mapsto h} & H & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \cong \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & N & \xrightarrow{i} & G & \xrightarrow{p} & H & \longrightarrow & 1 \end{array}$$

Cuando se cumplen estas condiciones, se dice que la sucesión exacta corta es ***escindida***[*].

Demostración. Para ver la implicación 1) ⇒ 2) notamos que H actúa sobre N por la conjugación en el siguiente sentido. Se puede identificar N con el subgrupo $i(N) \subseteq G$, que es normal, siendo el núcleo de p. Luego, dado que $p \circ s = \mathrm{id}_H$, se ve que $s\colon H \to G$ es un monomorfismo, y gracias a esto H se identifica con el subgrupo $s(H) \subseteq G$. Ya que $i(N)$ es normal, conjugando sus elementos por los elementos de $s(H)$, se obtienen elementos de $i(N)$.

[*] "split" en inglés.

La acción de $s(h) \in s(H)$ sobre $i(N)$ viene dada por

$$i(n) \mapsto s(h) \cdot i(n) \cdot s(h)^{-1} =: i(\phi_h(n)), \tag{10.6}$$

donde $\phi_h(n) \in N$. Esto define un homomorfismo

$$\begin{aligned} \phi \colon H &\to \operatorname{Aut}(N), \\ h &\mapsto \phi_h \end{aligned}$$

—el lector puede verificar todos los detalles usando la fórmula (10.6), pero salvo la identificación de N con $i(N)$ y H con $s(H)$, se trata de la acción habitual por la conjugación, y hemos comprobado en el capítulo anterior que en este caso la acción es por automorfismos. Ahora usando ϕ, podemos construir la suma semidirecta $N \rtimes_\phi H$, y luego considerar la aplicación

$$\begin{aligned} f \colon N \rtimes_\phi H &\to G, \\ (n, h) &\mapsto i(n) \cdot s(h). \end{aligned}$$

Esto es un homomorfismo: en G se cumple

$$\begin{aligned} i(n_1) \cdot s(h_1) \cdot i(n_2) \cdot s(h_2) &= i(n_1) \cdot s(h_1) \cdot i(n_2) \cdot s(h_1)^{-1} \cdot s(h_1) \cdot s(h_2) \\ &= i(n_1) \cdot i(\phi_{h_1}(n_2)) \cdot s(h_1 h_2) = i(n_1 \, \phi_{h_1}(n_2)) \cdot s(h_1 h_2), \end{aligned}$$

lo que corresponde a la multiplicación en $N \rtimes_\phi H$. Se ve que el homomorfismo f que acabamos de definir hace conmutar el diagrama (10.5), y el lema 10.3.7 nos dice que f es necesariamente un isomorfismo.

Para probar 2) $\Rightarrow$ 1), definamos $s(h) := f(1, h)$. Esto es un homomorfismo $s \colon H \to G$, dado que f lo es. Luego, de la conmutatividad del segundo cuadrado se sigue que $p \circ s(h) = p \circ f(1, h) = h$ para todo $h \in H$. ■

10.3.13. Ejemplo. Tenemos una sucesión exacta corta

$$1 \to \langle r \rangle \to D_n \xrightarrow{p} \langle f \rangle \to 1$$

Donde el subgrupo $\langle f \rangle = \{\mathrm{id}, f\}$ se identifica con el grupo cociente $D_n / \langle r \rangle$. La inclusión de subgrupo $s \colon \langle f \rangle \rightarrowtail D_n$ satisface $p \circ s = \mathrm{id}$. ▲

10.3.14. Ejemplo. Tenemos una sucesión exacta corta

$$1 \to \mathrm{SL}_n(k) \to \mathrm{GL}_n(k) \xrightarrow{\det} k^\times \to 1$$

Luego, hay un homomorfismo

$$\begin{aligned} k^\times &\to \mathrm{GL}_n(k), \\ x &\mapsto \begin{pmatrix} x & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \end{aligned}$$

y el determiante de la última matriz es igual a x. ▲

Notamos que cuando el grupo G que está en el medio es abeliano (y por ende N y H, siendo su subgrupo y grupo cociente), la fórmula (10.6) que define a ϕ_h implica que $\phi_h(n) = n$ para cualesquiera $h \in H$ y $n \in N$. Esto nos lleva al siguiente resultado.

10.3.15. Corolario. *Consideremos una sucesión exacta corta de grupos abelianos*

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

Las siguientes condiciones son equivalentes.

1) *Existe un homomorfismo de grupos* $r\colon B \to A$ *tal que* $r \circ i = \mathrm{id}_A$.

2) *Existe un homomorfismo de grupos* $s\colon C \to B$ *tal que* $p \circ s = \mathrm{id}_C$.

3) *Existe un isomorfismo* $f\colon B \xrightarrow{\cong} A \times C$ *que forma parte del diagrama conmutativo*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \cong\downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & A & \xrightarrow[a\mapsto(a,0)]{} & A\times C & \xrightarrow[(a,c)\mapsto c]{} & C & \longrightarrow & 0 \end{array}$$

10.3.16. Digresión. Se puede definir una equivalencia de extensiones de grupos

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0 \quad \text{y} \quad 0 \to A \xrightarrow{i'} B' \xrightarrow{p'} C \to 0$$

como un homomorfismo $B \to B'$ que hace conmutar el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & A & \xrightarrow{i'} & B' & \xrightarrow{p'} & C & \longrightarrow & 0 \end{array}$$

Como sabemos, en este caso $B \to B'$ es automáticamente un isomorfismo, y en particular se ve que se trata de una relación de equivalencia sobre las extensiones de C por A.

Cuando se trata de grupos abelianos, las extensiones módulo esta equivalencia también forman un grupo abeliano que se denota por $\mathrm{Ext}(C, A)$ y se denomina el **grupo de extensiones** de C por A. El elemento nulo de este grupo corresponde a la clase de equivalencia de la sucesión exacta escindida

$$0 \to A \xrightarrow{a\mapsto(a,0)} A \times C \xrightarrow{(a,c)\mapsto c} C \to 0$$

El cálculo de los grupos $\mathrm{Ext}(C, A)$ pertenece a la rama de las matemáticas conocida como **álgebra homológica**.

10.4 Grupos abelianos finitamente generados

Recordemos que un grupo abeliano (aditivo) A es **finitamente generado** si existe una colección finita $x_1, \ldots, x_k \in A$ de generadores:

$$A = \langle x_1, \ldots, x_k \rangle = \Big\{ \sum_{1 \le i \le k} n_i x_i \;\Big|\; n_i \in \mathbb{Z} \Big\}.$$

10.4.1. Definición. Digamos que $x_1, \ldots, x_k$ es una **base** de A si $A = \langle x_1, \ldots, x_k \rangle$ y

$$n_1 x_1 + \cdots + n_k x_k = 0,$$

para algunos $n_i \in \mathbb{Z}$, entonces $n_i x_i = 0$ para todo i.

10.4.2. Comentario. Esta condición es más débil que tener $n_i = 0$ para todo i. La última sería la definición correcta de una base, pero para esta sección vamos a usar la definición provisional de arriba.

10.4.3. Observación. *Si $x_1, \ldots, x_k$ es una base de A, entonces*

$$A \cong \langle x_1 \rangle \times \cdots \times \langle x_k \rangle.$$

Demostración. Consideremos el homomorfismo

$$\begin{aligned} \langle x_1 \rangle \times \cdots \times \langle x_k \rangle &\to A, \\ (n_1 x_1, \ldots, n_k x_k) &\mapsto \sum_{1 \leq i \leq k} n_i x_i. \end{aligned}$$

Es sobreyectivo, dado que $x_1, \ldots, x_k$ son generadores de A. Luego, es inyectivo por la definición de la base:

$$\sum_{1 \leq i \leq k} n_i x_i - \sum_{1 \leq i \leq k} n_i' x_i \iff \sum_{1 \leq i \leq k} (n_i - n_i')\, x_i = 0 \iff n_i x_i = n_i' x_i \text{ para todo } i.$$

■

10.4.4. Proposición. *Todo grupo abeliano finitamente generado posee una base y por lo tanto es isomorfso a un producto directo de grupos cíclicos.*

Para la prueba, vamos a usar el siguiente resultado auxiliar.

10.4.5. Lema. *Supongamos que $x_1, \ldots, x_k$ son generadores de A. Entonces para cualesquiera $c_1, \ldots, c_k \in \mathbb{N}$ tales que $\operatorname{mcd}(c_1, \ldots, c_k) = 1$ existen generadores $y_1, \ldots, y_k$ de A tales que*

$$y_1 = c_1 x_1 + \cdots + c_k x_k.$$

Demostración. Usemos inducción sobre $c := c_1 + \cdots + c_k$. La base de inducción es $c = 1$. En este caso, sin pérdida de generalidad, $c_1 = 1$ y $c_2 = \cdots = c_k = 0$, así que podemos tomar $y_i = x_i$.

Ahora si $c > 1$, entonces existen dos c_i que no son nulos. Sin pérdida de generalidad, $c_1 \geq c_2 > 0$. Notamos que

1) $A = \langle x_1, x_1 + x_2, x_3, \ldots, x_k \rangle$,

2) $\operatorname{mcd}(c_1 - c_2, c_2, c_3, \ldots, c_k) = 1$,

3) $(c_1 - c_2) + c_2 + c_3 + \cdots + c_k < c$.

Luego, por la hipótesis de inducción, existen generadores $y_1, \ldots, y_k$ tales que

$$y_1 = (c_1 - c_2)\, x_1 + c_2\, (x_1 + x_2) + c_3 x_3 + \cdots + c_k x_k = c_1 x_1 + \cdots + c_k x_k.$$

■

Demostración de 10.4.4. Usemos inducción sobre el número de generadores de A. La base es el caso cuando A puede ser generado por un elemento y es cíclico.

Supongamos que A puede ser generado por $k > 1$ elementos. Escojamos generadores $x_1, \ldots, x_k$ donde $\operatorname{ord} x_1$ es el mínimo posible. Vamos a probar que $A \cong \langle x_1 \rangle \times \langle x_2, \ldots, x_k \rangle$. Supongamos que

$$A \ncong \langle x_1 \rangle \times \langle x_2, \ldots, x_k \rangle.$$

Esto significa que $\langle x_1 \rangle \cap \langle x_2, \ldots, x_k \rangle \neq \{0\}$ y que existe una relación

$$n_1 x_1 + n_2 x_2 + \cdots + n_k x_k = 0$$

donde $n_1 x_1 \neq 0$. Reemplazando x_i por $-x_i$ si necesario, podemos suponer que $n_i \geq 0$. Además, sin pérdida de generalidad, $n_1 < \operatorname{ord} x_1$. Consideremos

$$d := \operatorname{mcd}(n_1, \ldots, n_k) > 0, \quad c_i := n_i/d.$$

Luego, $\operatorname{mcd}(c_1, \ldots, c_k) = 1$ y por el lema de arriba existen generadores $y_1, \ldots, y_k$ tales que $y_1 = c_1 x_1 + \cdots + c_k x_k$; es decir,

$$dy_1 = n_1 x_1 + \cdots + n_k x_k = 0.$$

Esto significa que

$$\operatorname{ord} y_1 \leq d \leq n_1 < \operatorname{ord} x_1.$$

Esto contradice nuestra elección de $x_1, \ldots, x_k$.

Entonces,

$$A \cong \langle x_1 \rangle \times \langle x_2, \ldots, x_k \rangle.$$

Procediendo por inducción de esta manera, podemos descomponer $\langle x_2, \ldots, x_k \rangle$ en un producto directo de grupos cíclicos. ■

10.4.6. Comentario. Hay muchas pruebas diferentes de 10.4.4. El argumento de arriba tiene ventaja de ser muy breve, pero no es constructivo. La fuente que seguí son los apuntes de J.S. Milne sobre la teoría de grupos: http://jmilne.org/math/CourseNotes/gt.html

Podemos formular un resultado más preciso.

10.4.7. Teorema. *Todo grupo abeliano finitamente generado no nulo A es isomorfo a un producto directo de grupos cíclicos*

$$\mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r}.$$

*El número r está bien definido y se llama el **rango** de A. Los números $p_i^{k_i}$ son potencias de números primos (no necesariamente distintos) y también están definidos de modo único para A.*

Demostración. Según 10.4.4, todo grupo abeliano finitamente generado es un producto directo de grupos cíclicos. Cada uno de los factores cíclicos finitos es isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Tomando la factorización en números primos $n = p_1^{k_1} \cdots p_s^{k_s}$ y aplicando el teorema chino del resto, se obtiene

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z}.$$

Esto establece la existencia de isomorfismo

$$A \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r} \tag{10.7}$$

para todo grupo abeliano finitamente generado A. Nos falta ver que los números r y $p_i^{k_i}$ están bien definidos.

Sería útil separar la parte finita $\mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z}$ de la parte infinita $\underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r}$. Para esto podemos considerar el **subgrupo de torsión**

$$A_{tors} := \{a \in A \mid n \cdot a = 0 \text{ para algún } n = 1, 2, 3, \ldots\}.$$

Tenemos

$$A_{tors} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z}, \quad A_{tf} := A/A_{tors} \cong \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r}$$

("tf" significa "torsion free", "libre de torsión"). Ahora sea p cualquier número primo. Consideremos el grupo

$$pA_{tf} := \{p \cdot a \mid a \in A_{tf}\} \subset A_{tf}.$$

El grupo cociente

$$A_{tf}/pA_{tf} \cong \underbrace{\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}}_{r} = \underbrace{\mathbb{F}_p \times \cdots \times \mathbb{F}_p}_{r}$$

es un espacio vectorial sobre $\mathbb{F}_p$ y

$$\dim_{\mathbb{F}_q}(A_{tf}/pA_{tf}) = r.$$

Entonces, r no depende de un isomorfismo particular (10.7), sino es un invariante de A.

Para ver la unicidad de los números $p_i^{k_i}$, podemos analizar por separado cada primo. A saber, para cada primo p consideremos el **subgrupo de p-torsión**

$$A[p^\infty] := \{a \in A \mid p^n \cdot a = 0 \text{ para algún } n = 0, 1, 2, 3, \ldots\}.$$

Será suficiente ver que en

$$A[p^\infty] \cong \mathbb{Z}/p^{\ell_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\ell_t}\mathbb{Z}$$

los números p^{ℓ_i} están bien definidos. Procedamos por inducción sobre $\ell = \ell_1 + \cdots + \ell_t$. Si $\ell = 1$, entonces $A[p^\infty] \cong \mathbb{Z}/p\mathbb{Z}$. Para el paso inductivo, podemos considerar el subgrupo $pA[p^\infty] \subset A[p^\infty]$. Luego,

$$A[p^\infty]/pA[p^\infty] \cong \mathbb{Z}/p^{\ell_1-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\ell_t-1}\mathbb{Z}.$$

Por la hipótesis de inducción, los números $\ell_i - 1$ están bien definidos. La única excepción son los factores $\mathbb{Z}/p\mathbb{Z}$ que corresponden a $\ell_i = 1$ que van a desaparecer. El número de estos factores puede ser recuperado de la relación $\sum_i \ell_i = \ell$. ■

10.4.8. Corolario. *Todo subgrupo de un grupo abeliano finitamente generado es finitamente generado.*

Para grupos no abelianos, el último resultado no se cumple. Un grupo no abeliano finitamente generado puede tener subgrupos que no son finitamente generados.

10.4.9. Ejemplo. Hay tres grupos abelianos no isomorfos de orden 8:

$$\mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Para encontrar los grupos abelianos de orden 100, podemos factorizar $100 = 2^2 \cdot 5^2$. Entonces, tenemos

$$\mathbb{Z}/100\mathbb{Z} \cong \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

▲

10.4.10. Comentario. En la expresión

$$A \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r}$$

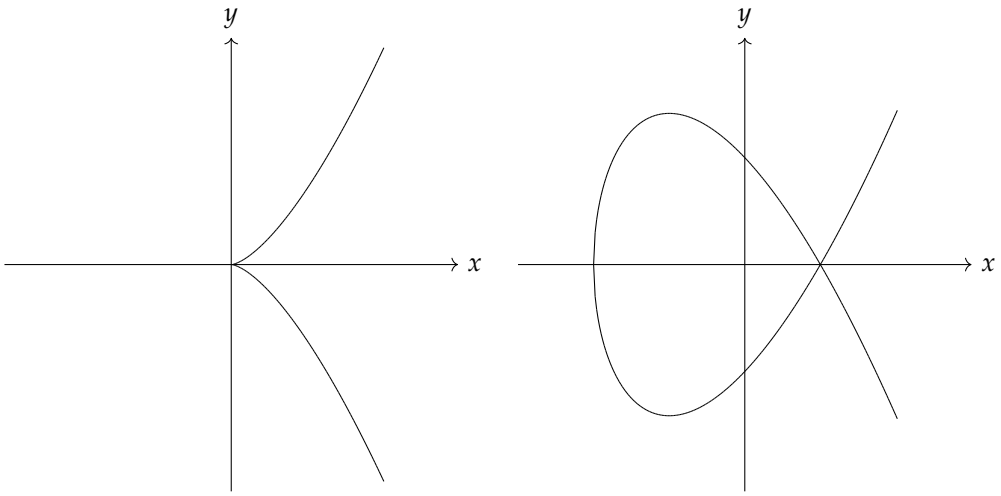
los números $p_i^{k_i}$ y r están bien definidos, pero el mismo isomorfismo depende de una base particular y por lo tanto no es canónico en ningún sentido.

10.5 Perspectiva: el grupo de Mordell–Weil

Finalizamos nuestra discusión de grupos abelianos finitamente generados con un ejemplo muy importante y no trivial. Sea E la curva plana definida por una ecuación cúbica

$$y^2 = x^3 + A\,x + B,$$

donde A y B son algunos coeficientes racionales. Esta curva puede tener una **cúspide** o un **nodo** como las curvas en el dibujo de abajo; en este caso se dice que E es **singular**.

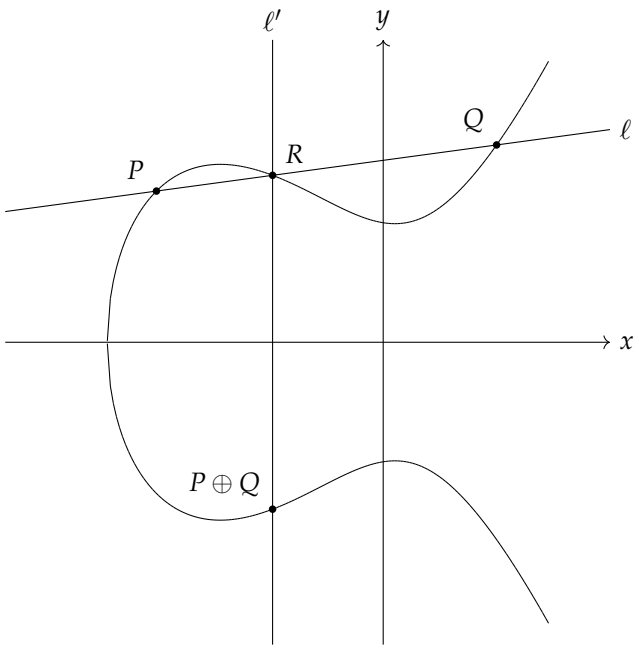


cúbica singular $y^2 = x^3$ cúbica singular $y^2 = x^3 - 3x + 2$

La curva no será singular precisamente cuando

$$4\,A^3 + 27\,B^2 \neq 0.$$

En este caso se dice que E es una **curva elíptica**. Sobre los puntos de E se puede definir la siguiente operación. Para dos puntos $P, Q \in E$, sea ℓ la recta que pasa por P y Q (si $P = Q$, se considera la tangente que pasa por P) y sea R el tercer punto de intersección de ℓ con E. Sea ℓ' la recta vertical que pasa por R. Entonces, el punto $P \oplus Q$ es el otro punto de intersección de E con ℓ'.



Un caso excepcional es cuando $P = (x, y)$ y $Q = (x, -y)$. En este caso se dice que el tercer punto de intersección "está al infinito" y se escribe $P \oplus Q = O$. Aquí O es un punto que se añade al plano afín; para este punto se define

$$P \oplus O = O \oplus P = P$$

para todo P. En el resto de casos, las coordenadas del tercer punto de intersección R pueden ser calculadas directamente.

1. Si $P = (x_P, y_P)$ y $Q = (x_Q, y_Q)$ donde $x_P \neq x_Q$, entonces se puede calcular que el tercer punto de intersección $R = (x_R, y_R)$ tiene coordenadas

$$x_R = \left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 - x_P - x_Q, \quad y_R = \frac{y_P - y_Q}{x_P - x_Q}\,(x_R - x_Q) + y_Q.$$

2. Si $P = Q = (x_P, y_P)$, entonces

$$x_R = \frac{(3\,x_P^2 + A)^2}{4\,y_P^2} - 2\,x_P, \quad y_R = \frac{3\,x_P^2 + A}{2\,y_P}\,(x_R - x_P) + y_P.$$

10.5.1. Teorema. *Sea E una curva elíptica definida por la ecuación*

$$y^2 = x^3 + A\,x + B,$$

donde $4\,A^3 + 27\,B^2 \neq 0$. Denotemos por $E(\mathbb{Q})$ los puntos con coordenadas racionales que están en la curva, junto con el punto O:

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + A\,x + B\} \cup \{O\}.$$

*Este se llama el **grupo de Mordell–Weil** de la curva elíptica E.*

Entonces, $E(\mathbb{Q})$ es un grupo abeliano respecto a la operación $\oplus$.

Bosquejo de demostración. De las fórmulas de arriba se ve que si P y Q tienen coordenadas racionales, entonces $P \oplus Q$ también tiene coordenadas racionales.

Por la definición, O es el elemento neutro. El elemento opuesto a $P = (x_P, y_P)$ es $-P = (x_P, -y_P)$. La operación es simétrica en P y Q, así que $P \oplus Q = Q \oplus P$ para cualesquiera $P, Q \in E(\mathbb{Q})$.

La única cosa que no está clara es la asociatividad: $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$. La única prueba comprensible y convincente usa geometría algebraica y la omitiré. ■

Un teorema clásico de Siegel dice que una curva elíptica tiene un número finito de puntos enteros. El número de puntos racionales puede ser infinito. Sin embargo, tenemos el siguiente resultado, conocido como el **teorema de Mordell–Weil**[*].

10.5.2. Teorema. *El grupo $E(\mathbb{Q})$ es finitamente generado.*

Esto significa que

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{tors},$$

donde r es un número natural, llamado el **rango** de la curva elíptica, y $E(\mathbb{Q})_{tors}$ es algún grupo finito. En otras palabras, existen algunos puntos

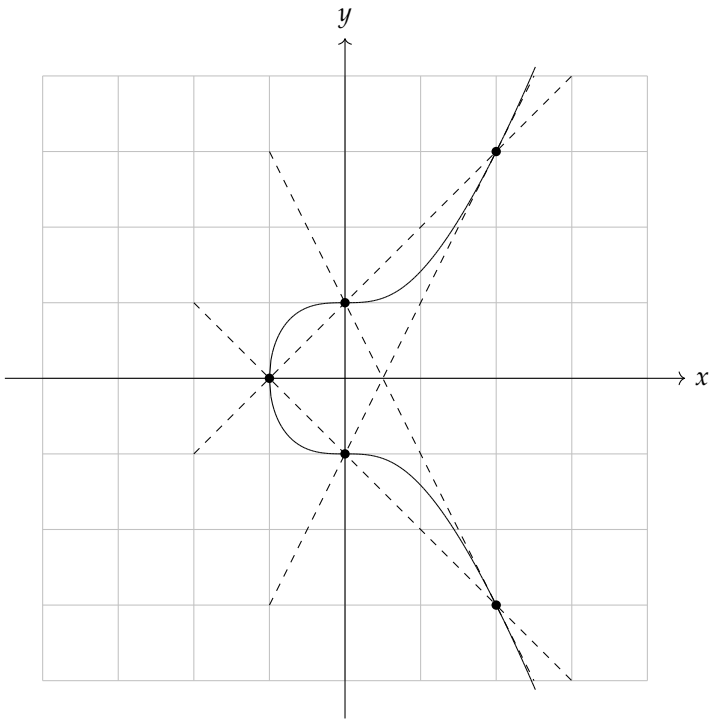
$$P_1, \ldots, P_r, Q_1, \ldots, Q_s$$

tales que todos los puntos racionales de la curva pueden ser obtenidas a partir de estas usando la operación $\oplus$.

10.5.3. Ejemplo. Para la curva $y^2 = x^3 + 1$ podemos calcular que el punto $(2, 3)$ es de orden 6:

$$2 \cdot (2,3) = (0,1),\ 3 \cdot (2,3) = (-1,0),\ 4 \cdot (2,3) = (0,-1),\ 5 \cdot (2,3) = (2,-3),\ 6 \cdot (2,3) = O.$$

Todo esto se ve del dibujo de abajo. Note que $(0, \pm 1)$ son puntos de inflexión.



curva elíptica $y^2 = x^3 + 1$

[*] Louis J. Mordell (1888–1972) probó el resultado en 1922 y André Weil (1906–1998) obtuvo una generalización en 1928.

De hecho, no hay otros puntos racionales y el grupo $E(\mathbb{Q})$ es cíclico de orden 6. ▲

10.5.4. Ejemplo. Resulta que para la curva $y^2 = x^3 - 4x + 4$ el grupo $E(\mathbb{Q})$ es isomorfo a $\mathbb{Z}$. Su generador es $P = (2, -2)$. Tenemos, por ejemplo

$$2 \cdot P = (0, -2), \quad 3 \cdot P = (-2, 2), \quad 4 \cdot P = (1, 1), \quad 5 \cdot P = (6, 14), \quad 6 \cdot P = (8, -22).$$

▲

En 1978 el matemático estadounidense Barry Mazur demostró que el subgrupo $E(\mathbb{Q})_{tors}$ es isomorfo a uno de los siguientes grupos:

$$\mathbb{Z}/n\mathbb{Z}, \text{ donde } n = 1, 2, 3, \ldots, 9, 10, 12,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \text{ donde } m = 2, 4, 6, 8,$$

y además, cada uno de los grupos mencionados surge como el subgrupo de torsión de alguna curva elíptica.

El número r es más misterioso. Una curva elíptica aleatoria suele tener rango 0 o 1. Una conjetura dice que r puede ser arbitrariamente grande, pero es muy difícil construir ejemplos particulares. El último récord pertenece al matemático estadounidense Noam Elkies: es una curva de rango ≥ 28.

Aparte del interés teórico, el grupo abeliano $E(\mathbb{Q})$ tiene aplicaciones en criptografía.

10.6 Ejercicios

Ejercicio 10.1. *Enumere todos los grupos abelianos de orden* 666 *salvo isomorfismo.*

Ejercicio 10.2. *Sea $n \geq 3$ un número natural impar. Consideremos el grupo diédrico*

$$D_{2n} = \{\mathrm{id}, r, r^2, \ldots, r^{2n-1}, f, fr, fr^2, \ldots, fr^{2n-1}\}$$

(las simetrías del $2n$-ágono regular) y sus subgrupos $H := \langle r^2, f\rangle$ y $K := \{1, r^n\}$.

1) *Demuestre que $H \cong D_n$ y $K \cong \mathbb{Z}/2\mathbb{Z}$.*

2) *Demuestre que $D_{2n} \cong H \times K$.*

3) *Si n es par, demuestre que $D_{2n} \ncong D_n \times \mathbb{Z}/2\mathbb{Z}$.*

Ejercicio 10.3. *Demuestre que la sucesión*

$$0 \to \mathbb{Z} \xrightarrow{n\mapsto(n,-n)} \mathbb{Z}[1/p] \times \mathbb{Z}_{(p)} \xrightarrow{(x,y)\mapsto x+y} \mathbb{Q} \to 0$$

es exacta. Aquí $\mathbb{Z}[1/p]$ es el subgrupo de $\mathbb{Q}$ formado por las fracciones con potencias de p en el denominador y $\mathbb{Z}_{(p)}$ es el subgrupo de fracciones con el denominador no divisible por p.

Ejercicio 10.4. *Demuestre que si $\mathbb{Q} \cong A \times B$ para algunos grupos abelianos A y B, entonces $A = 0$ o $B = 0$.*
Sugerencia: supongamos que A y B son subgrupos no triviales de $\mathbb{Q}$. Demuestre que $A \cap B \neq \{0\}$.

Ejercicio 10.5. *Demuestre que $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Z}[1/p]/\mathbb{Z} \times \mathbb{Z}_{(p)}/\mathbb{Z}$.*

Ejercicio 10.6. *Consideremos el grupo alternante A_4 y sus subgrupos*

$$V := \{\mathrm{id}, (1\,2)\,(3\,4), (1\,3)\,(2\,4), (1\,4)\,(2\,3)\}$$

y $H := \langle(1\,2\,3)\rangle$. Demuestre que A_4 es el producto semidirecto de V y H.

Ejercicio 10.7. *Demuestre que para $n \geq 5$ el grupo alternante A_n no puede ser isomorfo a un producto semidirecto $N \rtimes_\phi H$ donde N y H no son triviales.*

Ejercicio 10.8. *Sea $\mathrm{Isom}(\mathbb{R}^2)$ el grupo de isometrías del plano euclidiano. Demuestre que*

$$\mathrm{Isom}(\mathbb{R}^2) \cong \mathbb{R}^2 \rtimes_\phi O_2(\mathbb{R}),$$

donde $\mathbb{R}^2$ es el grupo aditivo $\mathbb{R} \times \mathbb{R}$ y el homomorfismo

$$\phi\colon O_2(\mathbb{R}) \to \mathrm{Aut}(\mathbb{R}^2)$$

viene dado por la multiplicación de vectores $\binom{x}{y} \in \mathbb{R}^2$ por matrices $A \in O_2(\mathbb{R})$:

$$\phi_A \binom{x}{y} := A \cdot \binom{x}{y}.$$

Ejercicio 10.9. *Demuestre que $O_n(\mathbb{R}) \cong SO_n(\mathbb{R}) \rtimes_\phi \{\pm 1\}$ para algún homomorfismo $\phi\colon \{\pm 1\} \to \mathrm{Aut}(SO_n(\mathbb{R}))$. Indicación: demuestre que la sucesión exacta corta*

$$1 \to SO_n(\mathbb{R}) \xrightarrow{i} O_n(\mathbb{R}) \xrightarrow{p} \{\pm 1\} \to 1$$

(donde i es la inclusión de subgrupo y p es la proyección sobre el grupo cociente) admite un homomorfismo $s\colon \{\pm 1\} \to O_n(\mathbb{R})$ tal que $i \circ s = \mathrm{id}$.

Ejercicio 10.10. *Encuentre todas las posibles extensiones de $\mathbb{Z}/2\mathbb{Z}$ por $\mathbb{Z}/2\mathbb{Z}$*

$$0 \to \mathbb{Z}/2\mathbb{Z} \to A \to \mathbb{Z}/2\mathbb{Z} \to 0$$

salvo isomorfismo.

Ejercicio 10.11. *Demuestre que toda sucesión exacta corta de grupos abelianos*

$$0 \to A \to B \to \mathbb{Z} \to 0$$

es equivalente a la extensión

$$0 \to A \xrightarrow{a \mapsto (a,0)} A \times \mathbb{Z} \xrightarrow{(a,n) \mapsto n} \mathbb{Z} \to 0$$

Indicación: demuestre que todo epimorsifmo $p\colon B \twoheadrightarrow \mathbb{Z}$ admite un homomorfismo $s\colon \mathbb{Z} \to B$ tal que $p \circ s = \mathrm{id}_{\mathbb{Z}}$.

Ejercicio 10.12. *Sea A un grupo abeliano que satisface la siguiente propiedad: todo monomorfismo de grupos abelianos $i\colon A \rightarrowtail B$ admite un homomorfismo $r\colon B \to A$ tal que $r \circ i = \mathrm{id}_A$. En este ejercicio vamos a demostrar que A es divisible.*

Sea $n = 1, 2, 3, \ldots$ y $a \in A$.

1) *Demuestre que $C := \{m \cdot a, -mn) \mid m \in \mathbb{Z}\}$ es un subgrupo de $A \times \mathbb{Z}$.*

2) *Consideremos el grupo cociente $(A \times \mathbb{Z})/C$ y el homomorfismo*

$$\begin{aligned} i\colon A &\to (A \times \mathbb{Z})/C, \\ x &\mapsto (x, 0) + C \end{aligned}$$

(esto es la composición de la inclusión de A como un subgrupo $A \times 0 \subset A \times \mathbb{Z}$ con la proyección sobre el grupo cociente). Demuestre que i es un monomorfismo.

3) *Demuestre que*

$$i(a) = (0, n) + C = n \cdot ((0, 1) + C) \quad \text{en } (A \times \mathbb{Z})/C.$$

4) *Por la hipótesis sobre A, existe un homomorfismo $r\colon (A \times \mathbb{Z})/C \to A$ tal que $r \circ i = \mathrm{id}_A$. Usando esto, encuentre un elemento $b \in A$ tal que $a = n \cdot b$. Concluya que A es divisible.*

Ejercicio 10.13. *Recordemos que dos sucesiones exactas cortas (extensiones de grupos)*

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0 \quad y \quad 0 \to A \xrightarrow{i'} B' \xrightarrow{p'} C \to 0$$

*son **equivalentes** si existe un homomorfismo $f\colon B \to B'$ tal que el diagrama*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & A & \xrightarrow{i'} & B' & \xrightarrow{p'} & C & \longrightarrow & 1 \end{array}$$

es conmutativo (hemos probado que en este caso f es un isomorfismo).

Sea p un número primo. Consideremos una sucesión de homomorfismos

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{[1]_p \mapsto [p]_{p^2}} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{[1]_{p^2} \mapsto [n]_p} \mathbb{Z}/p\mathbb{Z} \to 0$$

1) *Demuestre que para todo* $n = 1, 2, \ldots, p-1$ *es una sucesión exacta corta.*

2) *Demuestre que estas sucesiones no son equivalentes para diferentes* $n = 1, 2, \ldots, p-1$.

Ejercicio 10.14. *Sea*

$$1 \to H \to G \to K \to 1$$

una sucesión exacta corta de grupos finitos. Demuestre que $|G| = |H| \cdot |K|$.

Ejercicio 10.15. *Se dice que una sucesión de homomorfismos*

$$1 \xrightarrow{f_n} G_{n-1} \xrightarrow{f_{n-1}} G_{n-2} \xrightarrow{f_{n-2}} G_{n-3} \to \cdots \to G_1 \xrightarrow{f_1} G_0 \xrightarrow{f_0} 1$$

es ***exacta*** *si* $\operatorname{im} f_i = \ker f_{i-1}$ *para todo* $i = 1, \ldots, n$. *Es una generalización de la noción de sucesión exacta corta*

$$1 \xrightarrow{f_3} G_2 \xrightarrow{f_2} G_1 \xrightarrow{f_1} G_0 \xrightarrow{f_0} 1$$

Demuestre que para una sucesión exacta de grupos finitos se cumple

$$\prod_{0 \le i \le n-1} |G_i|^{(-1)^i} = 1.$$

Esto generaliza la fórmula del ejercicio precedente.