Lección nº 4 Junio, 2021

Capítulo 4

Grupos abelianos finitamente generados

Notación

(1) Los grupos a considerar en esta sección son abelianos y tiene notación aditiva. Es decir, $A, B, C, \ldots$ denotarán grupos abelianos; $+\colon A \times A \to A$ será la operación; 0 será el elemento neutro; y, dado $a \in A$, $-a$ denotará su inverso.

(2) Para la suma directa de dos grupos A y B usaremos $A \oplus B = \{(a, b) \,|\, a \in A,\, b \in B\}$ con la operación

$$(a, b) + (a', b') = (a + a', b + b').$$

El neutro será $0 = (0, 0)$ y el inverso $-(a, b) = (-a, -b)$. Además, sabemos que

$$A \hookrightarrow A \oplus B,\ a \longmapsto (a, 0),$$
$$B \hookrightarrow A \oplus B,\ b \longmapsto (0, b),$$

y que la aplicación

$$\begin{array}{rccc} \pi_A\colon & A \oplus B & \longrightarrow & A \\ & (a, b) & \longmapsto & a \end{array}$$

es un homeomorfismo tal que $\ker(\pi_A) = B$ (análogamente para la aplicación $\pi_B\colon A \oplus B \to B$).

Observación. Todo subgrupo de un grupo abeliano es normal. En efecto, si $A \leq B$, definimos $B/A = \{b + A \,|\, b \in B\}$ y

$$\begin{array}{rccc} \varphi\colon & B & \longrightarrow & B/A \\ & b & \longmapsto & b + A = \bar{b}. \end{array}$$

Se tiene que $\ker(\varphi) = A$. Así

$$\{0\} \longrightarrow A \hookrightarrow B \xrightarrow{\varphi} B/A \longrightarrow \{0\},$$

es una sucesión exacta corta. Esta se dice *escindida* si existe $s\colon B/A \to B$ tal que $\varphi \circ s = \mathrm{id}$; y s se llama una *sección*.

Ahora, con estas notaciones tenemos que una aplicación $f\colon A \to B$ es un homomorfismo si

$$f(x+y) = f(x) + f(y) \quad \forall\, x, y \in A,$$

lo que implica que $f(-x) = -f(x)$ y $f(0) = 0$.

Luego, sea A un grupo abeliano. Para todo entero $n \geq 1$,

$$\begin{aligned} nx &= x + \cdots + x \quad (n \text{ veces}), \\ (-n)x &= -(nx), \\ 0 \cdot x &= 0. \end{aligned}$$

Definición. Un elemento $x \in A$ se llama de *torsión* si existe $n \geq 1$ tal que $n \cdot x = 0$. Al menor de todos estos n se lo llama el *orden de* x.

Definición. Definimos el conjunto $A_t = \{x \in A \,|\, x \text{ es de torsión}\}$. Es claro que $A_t \leq A$, y se lo llama el *subgrupo de torsión de* A.

Definición. Un grupo A se dice *libre de torsión* si $A_t = \{0\}$. Por otro lado, si $A = A_t$, este se llama *grupo de torsión.*

Ejemplos 4.1.

(1) $A = \mathbb{Z}/n\mathbb{Z}$. Es fácil ver que $A = A_t$ y por tanto A es un grupo de torsión.

(2) $A = \mathbb{Z}^n = Z \oplus \cdots \oplus \mathbb{Z}$. En este caso se tiene que $A_t = \{0\}$. Equivalentemente $\left(\bigoplus_{i=1}^{n} \mathbb{Z}\right)_t = \{0\}$.

Proposición 4.2. *Sea Aun grupo abeliano y $A_t \leq A$. Entonces A/A_t es libre de torsión.*

Demostración. Denotemos $\bar{x} = x + A$. Sea $\bar{x} \in A/A_t$ de torsión, entonces existe $n \geq 1$ tal que

$$\begin{aligned} n\bar{x} = \bar{0} &\Longrightarrow \overline{nx} = \bar{0} \\ &\Longrightarrow nx \in A_t \\ &\Longrightarrow \exists\, m \geq 1,\ (mn)x = 0 \\ &\Longrightarrow x \in A_t \\ &\Longrightarrow \bar{x} = \bar{0}. \end{aligned}$$

Así $(A/A_t)_t = \{0\}$. □

En esta sección consideraremos grupos finitamente generados. Un conjunto $\{\alpha_1, \ldots, \alpha_n\} \subseteq A$ se llama un sistema de generadores de A si

$$A = \langle \alpha_1, \ldots, \alpha_n \rangle = \mathbb{Z}\alpha_1 + \ldots \mathbb{Z}\alpha_n,$$

es decir, si todo elemento $\alpha \in A$ es de la forma $\alpha = r_1\alpha_1 + \cdots + r_n\alpha_n$, con $r_i \in \mathbb{Z}$ para todo $i \in \{1, \ldots, n\}$.

Definición. Un conjunto $\{\alpha_1, \ldots, \alpha_n\} \subseteq A$ es una *base de* A si

(1) $\{\alpha_1, \ldots, \alpha_n\}$ es un sistema de generadores de A, es decir, si

$$A = \mathbb{Z}\alpha_1 + \ldots \mathbb{Z}\alpha_n$$

(2) Esta suma es directa; es decir, si

$$r_1\alpha_1 + \cdots + r_n\alpha_n = 0, \quad r_i \in \mathbb{Z},$$

implica que $r_i = \cdots = r_n = 0$.

Esta segunda condición es equivalente a la siguiente.

(2') Todo $\alpha \in A$ se escribe de forma única como combinación entera de elementos de $\{\alpha_1, \ldots, \alpha_n\}$, es decir que si

$$\alpha = r_1\alpha_1 + \ldots + r_n\alpha_n = s_1\alpha_1 + \cdots + s_n\alpha_n, \quad r_i, s_i \in \mathbb{Z}$$

entonces $r_i = s_i$ para todo $i \in \{1, \ldots, n\}$.

Es fácil probar que si A tiene una base $\{\alpha_1, \ldots, \alpha_n\}$, entonces $A \cong \mathbb{Z}^n$.

Notación: En esta caso, escribiremos $A = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$; y a A se lo llama un *grupo (abeliano) libre.*

Observación. Si $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$, con $\{\alpha_1, \ldots, \alpha_n\}$ un sistema de generadores. Entonces una *relación lineal* a $\alpha_1, \ldots, \alpha_n$ es una expresión de la forma

$$r_1\alpha_1 + \cdots + r_n\alpha_n = 0,$$

donde no todos los r_i son nulos.

Ejemplo 4.3. En $\mathbb{Z}/n\mathbb{Z}$, $n\bar{x} = 0$ para todo $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$. Por tanto, $\mathbb{Z}/n\mathbb{Z}$ no puede tener una base.

Proposición 4.4. *Sea A un grupo abeliano y sean $\{\alpha_1, \ldots, \alpha_n\}, \{\beta_1, \ldots \beta_m\}$ dos bases de A. Entonces $n = m$.*

Demostración. Tenemos que $A = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_m$. Sea p un primo cualquiera, entonces

$$pA = p\mathbb{Z}\alpha_1 \oplus \cdots \oplus p\mathbb{Z}\alpha_n = p\mathbb{Z}\beta_1 \oplus \cdots \oplus p\mathbb{Z}\beta_m.$$

Luego,

$$A/pA = \frac{\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n}{p\mathbb{Z}\alpha_1 \oplus \cdots \oplus p\mathbb{Z}\alpha_n} = \frac{\mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_m}{p\mathbb{Z}\beta_1 \oplus \cdots \oplus p\mathbb{Z}\beta_m}.$$

Ahora, sabemos que (¿por qué?)

$$\frac{B \oplus C}{pB \oplus pC} \cong \frac{B}{pB} \oplus \frac{C}{pC},$$

lo que implica que

$$A/pA \cong \frac{\mathbb{Z}\alpha_1}{p\mathbb{Z}\alpha_1} \oplus \cdots \oplus \frac{\mathbb{Z}\alpha_n}{p\mathbb{Z}\alpha_n} \cong \frac{\mathbb{Z}\beta_1}{p\mathbb{Z}\beta_1} \oplus \cdots \oplus \frac{\mathbb{Z}\beta_m}{p\mathbb{Z}\beta_m}.$$

Además, si α no es de torsión entonces

$$\frac{\mathbb{Z}\alpha}{p\mathbb{Z}\alpha} \cong \mathbb{Z}/p\mathbb{Z}.$$

Así,

$$A/pA \cong \underbrace{\mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}}_{n \text{ veces}} \cong \underbrace{\mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}}_{m \text{ veces}},$$

es decir $A/pA \cong (\mathbb{Z}/p\mathbb{Z})^n \cong (\mathbb{Z}/p\mathbb{Z})^m$, lo que implica que $n = m$, pues ambos son espacios vectoriales sobre el cuerpo finito en p-elementos. □

Corolario 4.5. *$\mathbb{Z}^n \cong \mathbb{Z}^m$ si y solo si $n = m$.*

Definición. Si A es un grupo abeliano y $\{\alpha_1, \ldots, \alpha_n\}$ es una base de A, decimos que $n = \text{rang}A$ es el *rango de A* (n es la dimensión de A respecto de $\mathbb{Z}$). También se escribe $n = \text{rg}A$.

Teorema 4.6 (Propiedad Universal de las Bases)**.** *Sea $A = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ es un grupo libre de rango n. Sea además, B un grupo abeliano arbitrario y $\beta_1, \ldots, \beta_n \in B$. Existe un único homomorfismo $\phi\colon A \to B$ tal que $\alpha_i \mapsto \beta_i$ para todo $1 \leq i \leq n$.*

Demostración. Si $\alpha \in A$, entonces $\alpha = r_1\alpha_1 + \cdots + r_n\alpha_n$ con $r_i \in \mathbb{Z}$ únicamente determinados. Se define $\phi(\alpha) = r_1\beta_1 + \cdots + r_n\beta_n$ y así se obtiene el resultado. □

Corolario 4.7. *Sea A un grupo finitamente generado y sea $\{\alpha_1, \ldots, \alpha_n\}$ un sistema de generadores. Entonces existe un epimorfismo $\pi\colon \mathbb{Z}^n \twoheadrightarrow A$ tal que $\pi(e_i) = \alpha_i$ para todo $i \in \{1, \ldots, n\}$, donde $e_i = (0, \ldots, 0, 1, 0 \ldots, 0)$ y $\{e_i \mid 1 \leq i \leq n\}$ es la base natural de $\mathbb{Z}^n$.*

Demostración. Por el teorema anterior, existe un único homorfismo $\pi\colon \mathbb{Z}^n \to A$ tal que $\pi(e_i) = \alpha_i$ para $1 \leq i \leq n$. Claramente, π es un epimorfismo. □

Recordemos que por el Primer Teorema de Isomorfia, $\mathbb{Z}^n/\ker(\pi) \cong A$. Así, todo grupo finitamente generado es un cociente de un grupo libre de rango finito.

Corolario 4.8. *Sea A un grupo finitamente generado. Entonces todo subgrupo de A es también finitamente generado.*

Demostración. Si A es finitamente generado, existe un epimorfismo $\mathbb{Z}^n \xrightarrow{\pi} A$.

Ahora, sea $A_1 \leq A$. Por ende, $B_1 = \pi^{-1}(A_1) \leq \mathbb{Z}^n$ que contiene al núcleo de π y

$$\bar{\pi}\colon B_1/\ker(\pi) \xrightarrow{\sim} A_1.$$

Como $B_1 \leq \mathbb{Z}^n$ y $\mathbb{Z}^n$ es libre, entonces B_1 es libre (¿por qué?) y $\text{rg}B \leq n$. Así $A_1 = \bar{\pi}(B_1/\ker(\pi))$ y A_1 es generado por las imágenes de una base de B_1. □

Sea A un grupo abeliano finitamente generado $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Por el corolario 4.7 existe un epimorfismo $f\colon \mathbb{Z}^n \twoheadrightarrow A$ tal que $f(e_i) = \alpha_i$ para todo $i \in \{1, \ldots, n\}$. Luego, por el primer teorema de isomorfía tenemos el isomorfismo $A \cong \mathbb{Z}^n/\ker(f)$, es decir que A es un cociente de un grupo libre de rango finito. Por otro lado, definimos $B_1 = f^{-1}(B) \leq \mathbb{Z}^n$, de modo que B_1 es un cociente de un grupo libre de rango finito de rango $m \leq n$. De esta manera existen $\beta_1, \ldots, \beta_n \in B_1$ tales que

$$B = \mathbb{Z}\beta_1 \oplus \cdots \oplus \beta_n.$$

Por tanto

$$B = f(B_1) = \mathbb{Z}f(\beta_1) + \cdots + \mathbb{Z}f(\beta_m),$$

de modo que B también es un grupo finitamente generado.

Ejercicio 4.9. Demostrar que todo grupo abeliano finitamente generado que es de torsión, es finito.

Lema 4.10. *Sean A un grupo abeliano, A' un grupo libre de rango finito, $f\colon A \to A'$ un epimorfismo y notemos $B = \ker(f) \leq A$. Entonces existe un subgrupo libre $C \leq A$ tal que $f\colon C \to A'$ es un isomorfismo de grupos y tal que $A = B \bigoplus C$.*

Observaciones. Como A' es libre, existen $\overline{\alpha}_i \in A'$, $i \in \{1, \ldots, n\}$, tales que $A' = \mathbb{Z}\overline{\alpha}_1 + \ldots \mathbb{Z}\overline{\alpha}_n$. Luego, como f es sobreyectivo, para todo $i \in \{1, \ldots, n\}$, existen α_i tales que $f(\alpha_i) = \overline{\alpha}_i$. Por otro lado, por el teorema ..., existe un único homomorfismo $\phi\colon A' \to A$ tal que $\phi(\overline{\alpha_i}) = \alpha_i$, para todo $i \in \{1, \ldots, n\}$. Luego, para $(r_1, \ldots, r_n) \in \mathbb{Z}^n$ arbitrario

$$s(r_1\overline{\alpha_1} + \cdots + r_n\overline{\alpha_n}) = r_1\lambda_1 + \cdots + r_n\alpha_n.$$

Por tanto

$$f \circ s(r_1\overline{\alpha}_1 + \cdots + r_n\overline{\alpha}_n) = r_1\overline{\lambda}_1 + \cdots + r_n\overline{\alpha}_n.$$

Es decir que $f \circ s = \mathrm{id}_{A'}$.

Ejercicio 4.11. Con los mismos grupos y el epimorfismo f del lema 4.10, consideremos la sucesión exacta corta

$$\{0\} \hookrightarrow B \hookrightarrow A \xrightarrow{f} A' \to \{0\}.$$

Pruebe que si $s\colon A' \to A$ es tal que $f \circ s = \mathrm{id}_{A'}$ entonces $s(A) \cong A'$ y $A = B \bigoplus s(A)$.

Observación. Vimos que si A es finitamente generado y $\{\alpha_1, \ldots, \alpha_n\}$ es un sistema de generadores, entonces existe un epimorfismo $f\colon \mathbb{Z}^n \to A$ tal que $f(e_i) = \lambda_i$ para todo $1 \leq i \leq n$ (corolario ...). Luego $\ker(f) \leq \mathbb{Z}^n$ es libre de rango $m \leq n$, $\ker(f) = \mathbb{Z}\beta_1 + \bigoplus \cdots \bigoplus \mathbb{Z}\beta_n$. Por otro lado, como $\mathbb{Z}^n$ es libre de rango n, tenemos en particular que los β_j se escriben de la forma $\beta_j = \sum_{i=1}^n a_{ij}e_i$, de donde podemos considerar la matriz $\Lambda = (a_{ij}) \in \mathbb{M}_{n\times m}(\mathbb{Z})$ que define define una aplicación

$$\mathbb{Z}^m \xrightarrow{\Lambda} \mathbb{Z}^n \xrightarrow{f} A$$

tal que $\mathrm{Img}(\Lambda) = \ker(f)$ y $\beta_j = \Lambda e_j$ para todo $1 \leq j \leq m$, por tanto $A \cong \mathbb{Z}^n/\mathrm{Img}(\Lambda)$.

Teorema 4.12. *Todo subgrupo de un grupo libre de rango n es libre de rango $m \leq n$.*

Demostración. Sea A un grupo abeliano libre de rango n y $B \leq A$ un subgrupo no trivial. Procedemos por inducción sobre n:

- Para $n = 1$. $B \leq A = \mathbb{Z}e_1$, podemos tomar $d > 0$ el entero más pequeño tal que $de_1 \in B$. Mostraremos que $B = \mathbb{Z}de_1$, en efecto, sea $h \in B$, entonces existe $g \in \mathbb{Z}$ tal que $h = ge_1$. Dividiendo g por d, existen $q \in \mathbb{N}$ y $0 \leq r < d$ tales que $g = qd + r$. Entonces $re_1 = ge_1 - qde_1 \in B$, de donde, por definición de d, necesariamente r tiene que ser 0. De esta manera $g = qd$ y $B = \mathbb{Z}de_1$.

- Suponemos que A es de la forma $A = \mathbb{Z}\alpha_1 \bigoplus \cdots \bigoplus \mathbb{Z}\alpha_n$ y tomamos $A_1 = \mathbb{Z}\alpha_2 \bigoplus \cdots \bigoplus \mathbb{Z}\alpha_n \leq A$, de manera que $A = \mathbb{Z}\alpha_1 \bigoplus A_1$. Si $B \leq A_1$, entonces por hipótesis de inducción B es libre de rango $m \leq n - 1$. Si $B \not\leq A_1$, la inclusiíon $i\colon B \hookrightarrow A$ induce un homomorfismo $\bar{i}\colon B \to A/A_1 = \mathbb{Z}\alpha_1$ tal que $\ker(\varphi) = B \cap A_1$. Entonces, por el primer teorema de isomorfia, existe un isomorfismo $B/B \cap A_1 \to \mathrm{Img}(\bar{i}) = a_1\mathbb{Z}\alpha_1$ ($a_1 \geq 1$). Tenemos entonces que $B/B \cap A_1$ es cíclico, $B/B \cap A_1 = \mathbb{Z}\overline{\beta}_1$, donde $\beta_1 = a_1\alpha_1 + \beta$, con $\beta \in B \cap A_1$. Finalmente como $B \cap A_1 \leq A_1$, por hipótesis de inducción $B \cap A_1$ es cíclico de orden menor o igual a $n-1$. Tomamos $\{\beta_2, \ldots, \beta_m\}$, $m \leq n - 1$, base de $B \cap A_1$, por ende $B \cap A_1 = \mathbb{Z}\beta_1 \bigoplus \cdots \bigoplus \mathbb{Z}\beta_m$.

  Probaremos que $\{\beta_1, \ldots, \beta_m\}$ es base de B:

i. Sea $\sigma \in B$, entonces para $\overline{\sigma} \in B/B \cap A_1$, existe $b_1 \in \mathbb{Z}$ tal que $\overline{\sigma} = b_1\overline{\beta}_1$. Esto implica que $\overline{\sigma - b_1\beta_1} = 0$, o lo que es lo mismo, que $n - b_1\beta_1 \in B \cap A_1$ y así existen $b_2, \ldots, b_m \in \mathbb{Z}$ tales que $\sigma - b_1\beta_1 = b_2\beta_2 + \cdots + b_m\beta_m$. Luego

$$\sigma = b_1\beta_1 + \cdots + b_m\beta_m \in \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_m,$$

que es lo que queríamos.

ii. Supongamos que $b_1\beta_1 + \cdots + b_m\beta_m = 0$. Luego $b_1\beta_1 = -(b_2\beta_2 + \cdots + b_m\beta_m) \in B \cap A_1$, y por tanto $b_1\overline{\beta}_1$. Pero como β_1 no tiene torsión, entonces $b_1 = 0$. Repitiendo el mismo procedimiento se concluye que $b_2 = \cdots = b_m = 0$.

□

Lema 4.13. *Sea*

$$\{0\} \to B \xrightarrow{i} A \xrightarrow{f} \!\!\!\!\rightarrow C \to \{0\}$$

una sucesión exacta de grupos abelianos, con $B = \ker(f) \leq A$. Supongamos que existe un homomorfismo $s\colon C \to A$ tal que $f \circ s = \mathrm{id}_C$. Entonces s es un isomorfismo $s\colon C \xrightarrow{\simeq} s(C) \leq A$ y se cumple que

$$A = B \bigoplus s(C) = \ker(f) \bigoplus \mathrm{Img}(s).$$

Demostración.

- s es monomorfismo: Si $s(c) = 0$, entonces $f(s(c)) = c = f(0) = 0$, así s es inyectiva y $s\colon C \xrightarrow{\simeq} s(C) \leq A$.
- $A = B \bigoplus s(C)$: Sea $a \in A$, entonces $f(a) \in C$ y $s(f(a)) \in s(C)$, además

  $$f(s(f(a))) = (f \circ s)(f(a)) = f(a).$$

  Por tanto tenemos $f(a - s(f(a))) = 0$, es decir que $a - s(f(a)) \in \ker(f) = B$. Así

  $$a = [a - s(f(a))] + s(f(a)) \in B + s(C).$$

  Recíprocamente, tomamos $a \in B \cap s(C)$. Existe $c \in C$ tal que $a = s(c)$ y $a \in B = \ker(f)$, por tanto

  $$0 = f(a) = f(s(c)) = c,$$

  lo cual implica que

  $$a = s(c) = s(0) = 0.$$

  Es decir que $B \cap s(C) = \{0\}$, y entonces $A = B \bigoplus s(C)$.

□

Observación. Caso particular: Sea

$$\{0\} \to B \to A \xrightarrow{f} C \to \{0\}$$

una sucesión exacta de grupos abelianos, con $B = \ker(f)$ y $C = \mathrm{Img}(f)$. Supongamos que C es libre

$$C = \mathbb{Z}\overline{\alpha}_1 \oplus \cdots \oplus \mathbb{Z}\overline{\alpha}_n,$$

donde $\{\overline{\alpha}_i \,|\, 1 \leq i \leq n\}$ es base de C. Para cada $1 \leq i \leq n$ tomamos $\alpha_i \in A$ tal que $f(\alpha_i) = \overline{\alpha}_i$, y tomamos el homomorfismo

$$\begin{aligned} s\colon C &\to A \\ \overline{\alpha}_i &\mapsto s(\alpha) = \alpha_i, \end{aligned}$$

dado por el teorema 4.6, entonces $f \circ s = \mathrm{id}_C$ y por el lema 4.13 se tiene que $A = B \bigoplus s(C)$.

Teorema 4.14. *Todo subgrupo libre de un grupo libre de grado n, es libre de grado $m \leq n$.*

Demostración. Sea A un grupo abeliano libre de rango n, $A = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ y sea $B \leq A$. Procedemos por inducción sobre n :

Ya fue probado para el caso $n = 1$. Para $n \geq 1$ definimos el homomorfismo

$$\begin{aligned} f\colon A &\to \mathbb{Z}\alpha_n \\ \alpha_i &\mapsto 0, \qquad 1 \leq i \leq n-1 \\ \alpha_n &\mapsto \alpha_n. \end{aligned}$$

Si restringimios f a B, entonces $f(B) \leq \mathbb{Z}\alpha_n$, entonces $f(B) = \mathbb{Z}d\alpha_n$, con $d \leq 1$ entero. Tomando $B_1 = \ker(f|_B) \leq B$ obtenemos una sucesión exacta corta

$$\{0\} \to B_1 \to B \xrightarrow{f|_B} \mathbb{Z}d\alpha_n \to \{0\}.$$

Luego, por lo anterior visto, como $\mathbb{Z}d\alpha_n$ es un grupo libre de rango 1 entonces $B \cong B_1 \bigoplus \mathbb{Z}d\alpha_n$. Pero

$$B_1 = \ker(f|_B) \leq \ker(f) = \mathbb{Z}\alpha_1 \bigoplus \cdots \bigoplus \mathbb{Z}\alpha_{n-1},$$

y este último grupo es libre de rango $n-1$. Por ende B_1 es libre de rango menor o igual a $n-1$ y B es un grupo libre de rango $m \leq n$. □

Teorema 4.15. *Sea A un grupo abeliano finitamente generado y libre de torsión. Entonces A es un grupo abeliano libre de rango finito.*

Demostración. Suponemos que A es un grupo finitamente generado distinto de $\{0\}$, entonces existe un sistema de generadores $\{\alpha_1, \ldots, \alpha_n\}$ tal que $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Tomemos $\{\alpha_1, \ldots \alpha_m\}$, $m \leq n$, el subconjunto más grande de $\{\alpha_1, \ldots, \alpha_n\}$ que sea linealmente independiente, este conjunto existe pues conjunto unitario $\{\alpha_i\}$ es linealmente independiente para cualquier $\alpha_i \neq 0$ pues A es libre de torsión. Por la definición de $\{\alpha_1, \ldots \alpha_m\}$, todos los conjuntos $\{\alpha_1, \ldots \alpha_i\}$ con $i > m$ son linealmente dependientes.

Sea ahora $B = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_m \leq A$. Si $m = n$ entonces no hay nada que probar, supponemos entonces $m < n$. Luego, el conjunto $\{\alpha_1, \ldots, \alpha_m, \alpha_{m+1}\}$ es linealmente dependiente y por ende existen $a_1, \ldots, a_m, a_{m+1}$ no todos iguales a cero tales que

$$a_1\alpha_1 + \cdots + a_m\alpha_m + a_{m+1}\alpha_{m+1} = 0, \quad \text{con } a_{m+1} \neq 0,$$

así, $a_{m+1}\alpha_{m+1} \in B$. Bajo el mismo argumento existe $a_{m+2} \in \mathbb{Z} \setminus \{0\}$ tal que $a_{m+2}\alpha_{m+2} \in B$ y continuando de esta misma manera, para todo $i \geq 1$ tal que $m+1 \leq m+i \leq n$, existe $a_{m+1} \in \mathbb{Z} \setminus \{0\}$ tal que $a_{m+i}\alpha_{m+i} \in B$. Sea

$$a = \prod_{k=m+1}^{n} a_k \in \mathbb{Z} \setminus \{0\}.$$

Tenemos que $a\alpha_{m+1}, a\alpha_{m+2}, \ldots, a\alpha_m \in \mathbb{Z}$, y como

$$A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m + \mathbb{Z}\alpha_{m+1} + \cdots + \mathbb{Z}\alpha_n = B + \mathbb{Z}\alpha_{m+1} + \cdots + \mathbb{Z}\alpha_n,$$

entonces

$$aA = \mathbb{Z}a\alpha_1 + \cdots + \mathbb{Z}a\alpha_m + \mathbb{Z}a\alpha_{m+1} + \cdots + \mathbb{Z}a\alpha_n \leq B = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \alpha_n.$$

Pero como B es libre, aA es libre de rango menor o igual a m. Consideremos la aplicación

$$\begin{aligned} A &\to aA \\ \alpha &\mapsto a\alpha, \end{aligned}$$

la cual es claramente epiyectiva, y como A es libre de torsión, también es inyectiva, de donde $A \cong aA$, por lo tanto A es libre. □

Es obvio que cualquier grupo libre es libre de torsión. Sea A un grupo abeliano finitamente generado, como $A_t \leq A$, entonces A_t es finitamente generado. Como A_t es de torsión y finitamente generado, entonces A_t es finito. Además A/A_t es finitamente generado y sin torsión. Luego, por el teorema anterior A/A_t es libre y tenemos que la sucesión

$$0 \to A_t \hookrightarrow iA \xrightarrow{f} A/A_t \to 0$$

es exacta y como A/A_t es libre, por el lema 4.13, existe $s\colon A/A_t \to A$, con $f \circ s = \mathrm{id}_{A/A_t}$ y además

$$A \cong A_t \bigoplus A/A_t \quad \text{con } A/A_t \cong \mathbb{Z}^r, \quad r \geq 0.$$

Luego, tenemos el siguiente teorema.

Teorema 4.16. *Sea A un grupo abeliano finitamente generado, entonces*

$$A \cong A_t \bigoplus A/A_t \cong A_t \bigoplus \mathbb{Z}^r$$

para algún $r \geq 0$, donde r está únicamente determinado por A y es llamado rango de A *y se denota por* $\mathrm{rg}(A) \in \mathbb{Z}^+ \cup \{0\}$.

Demostración. En la discusión anterior se mostró el resultado exceptuando la unicidad de r. Supongamos que existe $s \in \mathbb{Z}^+ \cup \{0\}$ tal que

$$\mathbb{Z}^s \cong A/A_t \equiv \mathbb{Z}^r,$$

luego, por el corolario 4.5 se sigue que $s = r$. □

Corolario 4.17 (Primer paso hacia la clasificación)**.** *Sean A, B dos grupos abelianos finitamente generados. Se tiene*

$$A \cong B \iff \begin{cases} A_t \cong B_t \\ \mathrm{rg}(A) = \mathrm{rg}(B). \end{cases}$$

Demostración. Del teorema anterior, sabemos que $A \cong A_t \bigoplus \mathbb{Z}^{\mathrm{rg}(A)}$ y $B \cong \mathbb{Z}^{\mathrm{rg}(A)}$, por tanto, si $A_t \cong B_t$ y $\mathrm{rg}(A) = \mathrm{rg}(B)$ entonces $A \cong B$. Recíprocamente, suponemos que existe un isomorfismo $f\colon A \to B$. Sea $\alpha \in A_t$, entonces existe $a \in \mathbb{Z}$ distinto de 0 tal que $a\alpha = 0$, de donde $af(\alpha) = 0$, y así $f(\alpha) \in B_t$. Entonces

$$f|_{A_t}\colon A_t \to B_t$$

es un monomorfismo. Como $f\colon A \to B$ es un isomorfismo, existe $f^{-1}\colon B \to A$, y por el mismo razonamiento

$$f^{-1}|_{B_t}\colon B_t \to A_t$$

es un monomorfismo. Luego $f|_{A_t}$ es un isomorfismo. Además

$$A/A_t \xrightarrow{\overline{f}} B/B_t$$

es un isomorfismo y $\mathbb{Z}^{\mathrm{rg}(A)} \cong \mathbb{Z}^{\mathrm{rg}(B)}$, de donde $\mathrm{rg}(A) = \mathrm{rg}(B)$. □

Este corolario reduce el problema de clasificación de grupos abelianos finitamente generados a clasificar grupos abelianos finitos. Sea A un grupo abeliano finitamente generado y sea $\{\alpha_1, \ldots, \alpha_n\}$ un sistema de generadores de A. Por el corolario 4.7 existe un epimorfismo

$$f\colon \mathbb{Z}^n \to A$$

tal que $f(e_i) = \alpha_i$, para todo $1 \leq i \leq n$. Para cualquier $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ se tiene que

$$f((a_1, \ldots, a_n)) = a_1\alpha_1 + \cdots + a_n\alpha_n.$$

Por otro lado, $\ker(f) \leq \mathbb{Z}^n$ es libre y de rango $m \leq n$, es decir

$$\ker(f) = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_m,$$

con $\beta_j \in \mathbb{Z}^n$ para todo $1 \leq j \leq m$. Luego

$$\beta_j = \sum_{i=1}^{n} a_{ij}e_i, \qquad a_{ij} \in \mathbb{Z}.$$

Así, los β_j están determinados por la matriz $\Lambda \in \mathbb{M}_{n\times m}(\mathbb{Z}/)\mathbb{Z}$

$$\Lambda = (a_{ij}), \quad \Lambda e_j = \beta_j.$$

Y entonces, tenemos el isomorfismo

$$\mathbb{Z}^n/\mathrm{Img}(\Lambda) \xrightarrow{\sim} A.$$

Para determinar la matriz Λ acudiremos al método de diagonalización de Λ por operadores elementales de filas y columnas. Usamos el hecho de que $\mathbb{Z}$ es un anillo con el algoritmo de Euclides

$$\Lambda = (a_{ij}) \xrightarrow[\text{sobre filas y columnas}]{\text{operadores elementales}} \underbrace{\left.\begin{pmatrix} b_1 & & \\ & \ddots & \\ & & b_m \\ & & \end{pmatrix}\right\} n}_{m}$$

Observación. Las operaciones elementales son elementos de $\mathrm{GL}(n, \mathbb{Z})$ (para las filas) y $\mathrm{GL}(m, \mathbb{Z})$ (para las columnas).

Teorema 4.18. *Sea $\Lambda \in \mathbb{M}_{n\times m}(\mathbb{Z})$, entonces existen matrices $P \in \mathrm{GL}(n, \mathbb{Z})$ y $Q \in \mathrm{GL}(m, \mathbb{Z})$*

y enteros $d_1, \ldots, d_m$ *tales que* $d_i \mid d_{i+1}$ *para todo* $1 \leq i \leq m-1$ *y*

$$P\Lambda Q = \underbrace{\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_m \\ & & \end{pmatrix}}_{m} \Bigg\} n$$

Esta descomposición se conoce como forma normal de Smith *y los enteros* $d_1, \ldots, d_m$ *se llaman* divisores elementales de Λ.

Demostración. Se presenta el algoritmo que lleva una matriz a esta forma:

(1) Se busca Λ un término de valor absoluto distinto de 0 más pequeño, si es negativo se cambia de signo de la fila o columna respectiva de este valor.

(2) Intercambiando filas y columnas posicionamos a este término en lugar (1,1). Re-definiendo esta nueva matriz $\Lambda = (a_{ij})$, el término a_{11} es el valor positivo de módulo más pequeño.

(3) Dividimos a_{11} a todos los coeficientes de la primera fila, así

$$a_{1i} = q_i a_{11} + r_i, \quad 0 \leq r_i < a_{11}, \quad i \geq 2.$$

Luego seguimos de la siguiente manera:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1m} \\ \vdots & \vdots & \vdots & & \vdots \\ \cdot & \cdot & \cdot & \ldots & \cdot \end{pmatrix} = \begin{pmatrix} a_{11} & q_2 a_{11} + r_2 & q_3 a_{11} + r_3 & \ldots & q_m a_{11} + r_m \\ \vdots & \vdots & \vdots & & \vdots \\ \cdot & \cdot & \cdot & \ldots & \cdot \end{pmatrix}$$

$$\xrightarrow{c_2 \leftarrow q_2 c_1} \begin{pmatrix} a_{11} & r_2 & q_3 a_{11} + r_3 & \ldots & q_m a_{11} + r_m \\ \vdots & \vdots & \vdots & & \vdots \\ \cdot & \cdot & \cdot & \ldots & \cdot \end{pmatrix}$$

$$\vdots$$

$$\longrightarrow \begin{pmatrix} a_{11} & r_2 & r_3 & \ldots & r_m \\ \vdots & \vdots & \vdots & & \vdots \\ \cdot & \cdot & \cdot & \ldots & \cdot \end{pmatrix},$$

es decir:

A la columna j le restamos el producto de la columna 1 por q_j y así aparece solamente r_j como coeficiente.

Si hay algún $r_i > 0$ elejimos el más pequeño e intercambiamos filas y columnas posicionándolo en el lugar (1,1), así se obtiene

$$\Lambda \longrightarrow \begin{pmatrix} r_1 & r_2 & \ldots & r_m \\ \vdots & \vdots & & \vdots \\ \cdot & \cdot & \ldots & \cdot \end{pmatrix}$$

Se divide $r_2, \ldots, r_m$ por r_1 y repetimos el proceso anterior, así

$$\Lambda \longrightarrow \begin{pmatrix} r_1 & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ \cdot & \cdot & \ldots & \cdot \end{pmatrix}$$

Realizando el mismo procedimiento con la primera columna obtenemos

$$\Lambda \longrightarrow \begin{pmatrix} r_1 & 0 & \ldots & 0 \\ 0 & \cdot & \ldots & \cdot \\ \vdots & \vdots & & \vdots \\ 0 & \cdot & \ldots & \cdot \end{pmatrix}$$

Volvemos a aplicar el proceso a la submatriz inferior izquierda

$$\Lambda \longrightarrow \begin{pmatrix} r_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & r_m \\ \vdots & & \vdots \\ 0 & \ldots & 0 \end{pmatrix}$$

con $r_1 \mid r_2$, y continuando con el proceso vemos que

$$P\Lambda Q = \begin{pmatrix} d_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & d_m \\ \vdots & & \vdots \\ 0 & \ldots & 0 \end{pmatrix} \quad \text{con } d_1 | d_2 | \ldots | d_m.$$

□

Este proceso funciona si $\Lambda = (a_{ij})$ donde $a_{ij} \in R$ y R es un anillo tal que existe $\varphi \colon R \setminus \{0\} \to \mathbb{N}$ que verifica

$$\forall\, a, b \in R,\ b \neq 0,\ \exists\, r, q \in R \text{ tal que } a = bq + r \text{ y } r = 0 \text{ o } \varphi(r) < \varphi(b).$$

Por ejemplo, $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \colon a, b \in \mathbb{Z}\}$ cumple esta propiedad.

Ejemplo 4.19.

$$\Lambda = \begin{pmatrix} 0 & 2 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 7 & 10 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}.$$

Teorema 4.20. *En la reducción* $P\Lambda Q = \left(\begin{array}{ccc} d_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & d_m \\ \hline & 0 & \end{array}\right)$, *los divisores fundamentales no de-*

penden del proceso de diagonalización.

Antes de la demostración veamos una aplicación de este resultado. Sea $\Lambda \in \mathrm{GL}(n,\mathbb{Z})$, existen $P, Q \in \mathrm{GL}(n,\mathbb{Z})$ productos de matrices elementales tales que

$$P\Lambda Q = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & d_n \end{pmatrix}, \quad \text{con } d_1 \mid d_2 \mid \cdots \mid d_n.$$

Como Λ es invertible, entonces $\det(\Lambda) \in \{\pm 1\}$, luego $\det(P\Lambda Q) = d_1 \cdots d_n = 1$, de donde

$$d_1 = \cdots = d_n = 1,$$

así $P\Lambda Q = I_n$, es decir $\Lambda = P^{-1}Q^{-1}$. Lo que implica que Λ es un producto de matrices elementales. Luego, las matrices elementales son un sistema de generadores de $\mathrm{GL}(n,\mathbb{Z})$.

Demostración. Definamos para toda matriz $\Lambda \in \mathbb{M}(n,m,\mathbb{Z})$, $m \geq n$

$$\delta_k(\Lambda) = \text{ máximo común divisor de todos los } k \times k \text{ menores de } \Lambda.$$

Sea

$$P\Lambda Q = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & d_m \end{pmatrix}, \quad \text{con } d_1 \mid d_2 \mid \cdots \mid d_m.$$

Así,

$$\delta_k(\Lambda) = \delta_k(P\Lambda Q) = \delta_K \left(\begin{array}{ccc} d_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & d_m \\ \hline & 0 & \end{array}\right) = d_1 \cdots d_k, \quad 1 \leq k \leq m.$$

□

Ejercicio 4.21. Probar que para todo $P \in \mathrm{GL}(n,\mathbb{Z})$ y $Q \in \mathrm{GL}(n,\mathbb{Z})$ se tiene que

$$\delta_k(P\Lambda Q) = \delta_k(\Lambda)$$

Observación. Por el ejercicio anterior, tal que depende solamente de Λ, para todo k. Así, $d_k = \frac{\delta_k(\Lambda)}{\delta_{k-1}(\Lambda)}$. Luego, d_k depende solo de Λ.

Complemento del Teorema: Sea $\Lambda \in \mathbb{M}(n,m,\mathbb{Z})$, $m \geq n$, $m = \mathrm{rg}(\Lambda)$. Los $d_1, \ldots, d_m$ que se obtienen en

$$P\Lambda Q = \left(\begin{array}{ccc} d_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & d_m \\ \hline & 0 & \end{array}\right),$$

solo dependen de Λ, es decir, los divisores fundamentales de Λ son invariantes de Λ.

Teorema 4.22. *Sea A un grupo abeliano finitamente generado libre, y sea $B \leq A$. Existe una base $\{\alpha_1, \ldots, \alpha_n\}$ de A y enteros positivos $d_1, \ldots, d_m$, $m \leq n$, con $d_1 \mid d_2 \mid \cdots \mid d_m$ tal que*

$$\{d_1\alpha_1, \ldots, d_m\alpha_m\} \text{ es base de } B.$$

Demostración. Sean A libre, $\{\alpha_1, \ldots, \alpha_n\}$ una base de A y $B \leq A$. B es libre de rango $m \leq n$, entonces existen $\beta_1, \ldots, \beta_m \in A$ tales que

$$B = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_m.$$

Escribimos

$$\beta_j = \sum_{i=1}^{n} a_{ij}\alpha_i, \quad 1 \leq j \leq m,\ a_{ij} \in \mathbb{Z}, \tag{4.1}$$

y formamos la matriz

$$\Lambda = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix},$$

que es de dimensión $n \times m$ de rango m. Así, (4.1) se escribe

$$(\beta_1, \ldots, \beta_m) = (\alpha_1, \ldots, \alpha_n)\Lambda. \tag{4.2}$$

Por el teorema anterior, existe $P \in \mathrm{GL}(n, \mathbb{Z})$ y $Q \in \mathrm{GL}(m, \mathbb{Z})$, productos de matrices elementales, tales que

$$P\Lambda Q = \left(\begin{array}{ccc} d_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & d_m \\ \hline & 0 & \end{array}\right),$$

con $d_1, \ldots, d_m \in \mathbb{Z}_+$ y $d_1 \mid d_2 \mid \cdots \mid d_m$.

Ahora, de (4.2) tenemos que

$$(\alpha_1, \ldots, \alpha_n)P^{-1}P\Lambda = (\beta_1, \ldots, \beta_m)$$
$$(\alpha_1, \ldots, \alpha_n)P^{-1}P\Lambda Q = (\beta_1, \ldots, \beta_m)Q.$$

Sea $(p_1, \ldots, p_n) = (\alpha_1, \ldots, \alpha_n)P^{-1}$, la cual es una base de A y $(\lambda_1, \ldots, \lambda_m) = (\beta_1, \ldots, \beta_m)Q$ es una base de B. Pero

$$(p_1, \ldots, p_n)\left(\begin{array}{ccc} d_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & d_m \\ \hline & 0 & \end{array}\right) = (\lambda_1, \ldots, \lambda_m),$$

de donde $d_1p_1 = \lambda_1, \ldots d_mp_m = \lambda_m$. Por lo tanto, $(p_1, \ldots, p_n)$ es la base de A buscada. □

Ahora apliquemos este resultado. Sea A un grupo abeliano finitamente generado. Sea $\{\alpha_1, \ldots \alpha_n\}$ un sistema de generadores de A. Existe $f\colon \mathbb{Z}^n \twoheadrightarrow A$ un epimorfismo tal que $f(e_i) = \alpha_i,\ 1 \leq i \leq n$. Luego, $\ker(f) \leq \mathbb{Z}^n$ y $\mathbb{Z}^n/\ker(f) \xrightarrow{\sim} A$.

Apliquemos el teorema a $\ker(f) \leq \mathbb{Z}^n$. Existe una base $\{p_1, \ldots, p_n\}$ de $\mathbb{Z}^n$ y enteros positivos $d_1 \mid d_2 \mid \cdots \mid d_m$ con $m \geq n$ tales que $\{d_1 p_1, \ldots, d_m p_m\}$ es base de $\ker(f)$. Así

$$\mathbb{Z}^n = \mathbb{Z}p_1 \oplus \cdots \oplus \mathbb{Z}p_m \oplus \mathbb{Z}p_{m+1} \oplus \cdots \oplus \mathbb{Z}p_n,$$

y

$$\ker(f) = \mathbb{Z}d_1 p_1 \oplus \cdots \oplus \mathbb{Z}d_m p_m.$$

Por tanto

$$A \cong \frac{\mathbb{Z}p_1 \oplus \cdots \oplus \mathbb{Z}p_m \oplus \cdots \oplus \mathbb{Z}p_n}{\mathbb{Z}d_1 p_1 \oplus \cdots \oplus \mathbb{Z}},$$

de donde

$$\begin{aligned} A &\cong \frac{\mathbb{Z}p_1}{\mathbb{Z}d_1 p_1} \oplus \cdots \oplus \frac{\mathbb{Z}p_m}{\mathbb{Z}d_m p_m} \oplus \mathbb{Z}p_{m+1} \oplus \cdots \oplus \mathbb{Z}p_n \\ &\cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \oplus \mathbb{Z}^{n-m}. \end{aligned}$$

Teorema 4.23 (Clasificación de grupos abelianos finitamente generados)**.** *Sea A un grupo abeliano finitamente generado, entonces existen enteros $d_1 \mid d_2 \mid \cdots \mid d_m$, con $m, r \geq 0$, tales que*

$$A \cong \mathbb{Z}d_1 \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \oplus \overbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}^{r},$$

donde $d_1, \ldots, d_m$, m y r están únicamente determinados por A; es decir, si

$$A \cong \mathbb{Z}d_1 \oplus \cdots \oplus \mathbb{Z}d_m \oplus \mathbb{Z}^r \quad y \quad A \cong \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n \oplus \mathbb{Z}^s,$$

entonces $m = n$, $r = s$ y $d_1 = e_1, \ldots d_m = e_m$.

Definición. Los enteros $d_1, \ldots, d_m$ se llaman divisores elementales de A y r es el rango de A.

Observación. De $A \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \oplus \mathbb{Z}^r$, entonces $A_t = \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$, y $\mathbb{Z}^r = A/A_t$. Así, r está únicamente determinado.

Este teorema permite escribir todos los grupos abelianos finitos con orden $|A|$ dado.

Ejemplo 4.24. Sea $A = \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$. Notemos que

$$10 = 2 \times 5, \quad 15 = 3 \times 5, \quad 20 = 4 \times 5,$$

y $5 \mid 2 \cdot 5 \mid 3 \cdot 4 \cdot 5$. Así,

$$\begin{aligned} A &\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \\ &\cong \mathbb{Z}/5\mathbb{Z}\,(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}) \\ &\cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/60\mathbb{Z}. \end{aligned}$$

Ejemplo 4.25. Sea $A = \mathbb{Z}/28\mathbb{Z} \oplus \mathbb{Z}/42\mathbb{Z}$ y observemos que

$$28 = 4 \times 7, \quad 42 = 2 \times 3 \times 7,$$

con $2 \cdot 7 \mid 3 \cdot 4 \cdot 7$. Así

$$A \cong \mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}/84\mathbb{Z}$$

Aplicación: Sea $G = \langle x_1, \ldots, x_n \rangle = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$, es decir $\{x_1, \ldots, x_n\}$ son generadores de G. Así, las relaciones

$$\Lambda = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}.$$

Las relaciones

$$\Lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0 \quad \text{o} \quad (x_1, \ldots, x_n)^\top \Lambda = 0.$$

Usamos la forma normal de Smith

$$P\Lambda Q = \left(\begin{array}{ccc|c} d_1 & 0 & 0 & \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & d_k & \\ \hline & 0 & & 0 \end{array}\right)$$

donde $k = \operatorname{rg}(\Lambda)$.

Vamos a demostrar la unicidad de los $d_1, \ldots, d_m$, para lo cual necesitamos hacer ciertos preparativos.

Primero, sea A un grupo abeliano finitamente generado y p un primo, entonces A/pA es un $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$-espacio vectorial de dimensión finita, pues si $a + p\mathbb{Z} \in \mathbb{F}_p$ y $x + pA \in A/pA$ se tiene que

$$(a + p\mathbb{Z})(x + pA) = ax + pA.$$

Ejemplo 4.26. Si consideramos $A = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$, entonces $A/3A \cong \mathbb{F}_3 \oplus \mathbb{F}_2$ y $\dim_{\mathbb{F}_3}(A/3A) = 2$. En efecto, $3A = 3\mathbb{Z}/9\mathbb{Z}$, lo que implica que

$$A/3A \cong \mathbb{Z}/3\mathbb{Z} \oplus \frac{\mathbb{Z}/9\mathbb{Z}}{3\mathbb{Z}/9\mathbb{Z}} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3 \oplus \mathbb{F}_3.$$

Si p es un primo arbitrario, para todo $j \geq 1$, $p^jA/p^{j+1}A$ es un $\mathbb{F}_p$-espacio vectorial.

Lema 4.27. *Sea $A = \mathbb{Z}/d\mathbb{Z}, d > 1$, entonces para todo primo p y para todo $j \geq 1$ se tiene que*

$$\dim_{\mathbb{F}_p}\left(p^jA/p^{j+1}A\right) = \begin{cases} 0 & \text{si } p^{j+1} \nmid d \\ 1 & \text{si } p^{j+1} \mid d. \end{cases}$$

Demostración. Supongamos que $p^{j+1} \nmid d$, entonces $(p^{j+1}, d) = (p^j, d) = p^k$ para cierto $k \in \mathbb{Z}$. Entonces

$$|p^{-j}| = \frac{d}{(p^j, d)} = \frac{d}{(p^{j+1}, d)} = |p^{-jk}|.$$

Luego, p^{-j}, p^{-jk} son generadores de p^jA y $p^{j+1}A$, de donde $p^jA = p^{j+1}A$, y así $\dim_{\mathbb{F}_p}(p^jA/p^{j+1}A) = 0$.

Si $p^{j+1} \mid d$, entonces $(p^{j+1}, d) = p^{j+1}$ y $(p^j, d) = p^j$, de donde

$$|p^j| = \frac{d}{p^j} \quad \text{y} \quad |p^{-jk}| = \frac{d}{p^{j+1}}.$$

Así, $p^jA/p^{j+1}A \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, de donde $\dim_{\mathbb{F}_p}(p^jA/p^{j+1}A) = 1$. □

Ejercicio 4.28. Sea $A = \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Muestre que

$$\dim_{\mathbb{F}_2}(A/2A) = 1, \quad \dim_{\mathbb{F}_2}(2A/4A) = 1, \quad \dim_{\mathbb{F}_2}(4A/8A) = 0, \quad \dim_{\mathbb{F}_3}(A/3A) = 1, \quad \dim_{\mathbb{F}_3}(3A/9A) = 0.$$

Demostración del Teorema 4.23. Se tiene que

$$\begin{aligned} A &\cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \oplus \mathbb{Z}^r, \quad d_1 \mid d_2 \mid \cdots \mid d_m \\ &\cong \mathbb{Z}/e_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/e_n\mathbb{Z} \oplus \mathbb{Z}^r, \quad e_1 \mid e_2 \mid \cdots \mid e_n. \end{aligned}$$

Así,

$$A_t = \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \cong \mathbb{Z}/e_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/e_n\mathbb{Z},$$

y por el lema anterior sabemos que $\dim_{\mathbb{F}_p}(A_t/pA_t) \leq m$ y $\dim_{\mathbb{F}_p}(A_t/pA_t) \leq n$. Por las hipótesis que tenemos sabemos que, si $p \mid d_1$ entonces $p \mid d_k$ para cada $1 \leq k \leq m$. De donde

$$\dim_{\mathbb{F}_p}(A/A_t) = m,$$

y así $m = \max_p \dim_{\mathbb{F}_p}(A_t/pA_t)$. Y de igual manera, si $p \mid e_1$ entonces $n = \max_p \dim_{\mathbb{F}_p}(A_t/pA_t)$. Por tanto, $m = n$.

Sea p primo arbitrario, $j \geq 0$. Definamos $l = \dim_{\mathbb{F}_p}(p^j A_t/p^{j+1}A_t)$, entonces

$$p^j A_t/p^{j+1}A_t = \bigoplus_{k=1}^{m} \frac{p^j\mathbb{Z}/d_k\mathbb{Z}}{p^{j+1}\mathbb{Z}/d_k\mathbb{Z}} = \bigoplus_{k=1}^{m} \frac{p^j\mathbb{Z}/e_k\mathbb{Z}}{p^{j+1}\mathbb{Z}/e_k\mathbb{Z}}.$$

□

Ejercicio 4.29. Concluir que

$$l = \#\{d_k \,|\, p^{j+1} \mid d_k\} = \#\{e_k \,|\, p^{j+1} \mid e_k\}.$$

Así, l es el número de d_k's tales que $p^{j+1} \mid d_k$ y l es el número de e_k's tales que $p^{j+1} \mid e_k$.
Observemos que si $p^{j+1} \mid d_k$ entonces $p^{j+1} \mid d_{k+1}, d_{k+2}, \ldots, d_m$.

Ejercicio 4.30. Concluir, de la definición de l, que

$$p^{j+1} \nmid d_1, \ldots, d_{m-l} \quad \text{y} \quad p^{j+1} \mid d_{m-l+1}, \ldots, d_m.$$

Entonces las dimensiones l determinan completamente la factorización en primos $d_1, \ldots, d_m$. Por la misma razón, determinan la factorización en primos de $e_1, \ldots, e_m$. Así $d_1 = e_1, \ldots, d_m = e_m$.

Observación. Sea $A = \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \oplus \mathbb{Z}^r$. Los d_i admiten descomposición en primos

$$d_1 = p_1^{a_1} \cdots p_r^{a_r}, \ldots, d_m = p_1^{\sim} \cdots .$$

Así, $\mathbb{Z}/d_1\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_r^{a_r}\mathbb{Z}$. Juntando estas factorizaciones (consecuencia del teorema clásico del resto) se obtiene

Teorema 4.31 (De Clasificación II)**.** *Para todo grupo abeliano finitamente generado A, existen primos $p_1, \ldots, p_m$, enteros $k_1, \ldots, k_m, l_1, \ldots, l_m > 0$ tales que*

$$A = (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^{l_1} \oplus \cdots \oplus (\mathbb{Z}/p_m^{k_m}\mathbb{Z})^{l_m} \oplus \mathbb{Z}^r,$$

y $p_1, \ldots, p_m, k_1, \ldots, k_m, l_1, \ldots, l_m$ están únicamente determinados.

Problema: Sea A un grupo finitamente generado con generadores $x_1, \dots, x_n$ que satisfacen las relaciones

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0, \\ a_{21}x_1 + \cdots + a_{2n}x_n &= 0, \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0. \end{aligned}$$

¿Qué grupo es A? Sea

$$\Lambda = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & & \vdots & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},$$

por lo que las relaciones se escriben como

$$\Lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0 \quad \text{o} \quad (x_1, \dots, x_n)^\top \Lambda = 0.$$

Apliquemos la forma normal de Smith a $\top\Lambda$. Existen $P \in \mathrm{GL}(n, \mathbb{Z}), Q \in \mathrm{GL}(m, \mathbb{Z})$ tales que

$$P^\top \Lambda Q = \left(\begin{array}{ccc|c} d_1 & 0 & 0 & \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & d_k & \\ \hline & 0 & & 0 \end{array}\right) \quad \text{con } d_1 \mid d_2 \mid \cdots \mid d_k.$$

Como $A = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_n$, existe un epimorfismo $f\colon \mathbb{Z}^n \to A$ y $\mathbb{Z}^n/\ker(f) \xrightarrow{\simeq} A$, $\ker(f) = \langle Y_1, \dots, Y_m \rangle$,

$$Y_i = \sum_{j=1}^{n} a_{ij}x_i.$$

Entonces

$$\begin{aligned} (x_1, \dots, x_n)^\top \Lambda &= (Y_1, \dots, Y_m) \\ (x_1, \dots, x_n) P^{-1} P^\top \Lambda Q &= (Y_1, \dots, Y_m) Q \\ (x_1, \dots, x_n) P^{-1} \left(\begin{array}{ccc|c} d_1 & 0 & 0 & \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & d_k & \\ \hline & 0 & & 0 \end{array}\right) &= (Y_1, \dots, Y_m) Q. \end{aligned}$$

Definamos

$$(T_1, \dots, T_n) = (x_1, \dots, x_n) P^{-1}, \quad (Z_1, \dots, Z_m) = (Y_1, \dots, Y_m) Q,$$

bases de ... yker(f) respectivamente. Así

$$(T_1, \dots, T_n) \left(\begin{array}{ccc|c} d_1 & 0 & 0 & \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & d_k & \\ \hline & 0 & & 0 \end{array}\right) = (Z_1, \dots, Z_m),$$

lo que implica que

$$(d_1T_1, \ldots, d_kT_k, 0, \ldots, 0) = (Z_1, \ldots, Z_m).$$

Luego, $Z_i = 0$ para todo $i \geq k+1$ y $d_iT_i = Z_i$ para todo $i \in \{1, \ldots, k\}$. Así

$$\ker(f) = \mathbb{Z}/d_1T_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_kT_k\mathbb{Z},$$

y en consecuencia

$$\begin{aligned} A &\cong \left(\bigoplus_{i=1}^{n} \mathbb{Z}/x_i\mathbb{Z}\right) / \bigoplus_{i=1}^{m} (\mathbb{Z}/Y_i\mathbb{Z}) \\ &\cong \left(\bigoplus_{i=1}^{k} \mathbb{Z}/T_i\mathbb{Z}\right) / \bigoplus_{i=1}^{k} \mathbb{Z}/d_iT_i\mathbb{Z} \\ &\cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \bigoplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z}^{n-k}. \end{aligned}$$

Ejemplo 4.32. Consideremos $A = \mathbb{Z}x_1 + \mathbb{Z}x_2$, con las relaciones

$$\begin{aligned} 2x_1 &= 0, \\ 3x_2 &= 0. \end{aligned}$$

Aplicamos el proceso de diagonalización de Smith

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \to \begin{pmatrix} 2 & 3 \\ 0 & 3 \end{pmatrix} \to \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 3 & -6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}.$$

Entonces $d_1 = 1$ y $d_2 = 6$, es decir $A = \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}$.

Ejemplo 4.33. Consideremos $A = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \mathbb{Z}x_3$ con las relaciones

$$\begin{aligned} 3x_1 + 5x_2 - 3x_3 &= 0 \\ 4x_1 + 2x_2 &= 0. \end{aligned}$$

En este caso

$$\Lambda = \begin{pmatrix} 3 & 5 & -3 \\ 4 & 2 & 0 \end{pmatrix}$$

, de donde

$$\begin{aligned} {}^{\top}\Lambda = \begin{pmatrix} 3 & 4 \\ 5 & 2 \\ -3 & 0 \end{pmatrix} \to \begin{pmatrix} 5 & 2 \\ 3 & 4 \\ -3 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & 5 \\ 4 & 3 \\ 0 & -3 \end{pmatrix} \to \begin{pmatrix} 2 & 1 \\ 4 & -5 \\ 0 & -3 \end{pmatrix} \to \begin{pmatrix} 1 & 2 \\ -5 & 4 \\ -3 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ -5 & 14 \\ -3 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 14 \\ 0 & 6 \end{pmatrix} \\ \to \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 0 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

De donde $d_1 = 1$ y $d_2 = 2$, y así $A = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$

Ejemplo 4.34. Consideremos $A = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_5$, con las relaciones

$$\begin{aligned} x_1 - 5x_2 + 10x_4 - 15x_5 &= 0, \\ 4x_2 - 8x_4 + 12x_5 &= 0, \\ 3x_1 - 3x_2 - 2x_3 + 6x_4 - 9x_5 &= 0, \\ x_1 - x_2 + 2x_4 - 3x_5 &= 0, \end{aligned}$$

por lo que

$$\Lambda = \begin{pmatrix} 1 & -5 & 0 & 10 & -15 \\ 0 & 4 & 0 & -8 & 12 \\ 3 & -3 & -2 & 6 & -9 \\ 1 & -1 & 0 & 2 & -3 \end{pmatrix}.$$

Aplicamos la forma norma lde Smith

$$\Lambda \to \begin{pmatrix} 1 & -1 & 0 & 2 & -3 \\ 0 & 4 & 0 & -8 & 12 \\ 0 & 0 & -2 & 0 & 0 \\ 1 & -1 & 0 & 2 & -3 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 0 & 2 & -3 \\ 0 & 4 & 0 & -8 & 12 \\ 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & -8 & 12 \\ 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$
$$\to \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Por lo que $A \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$.