9 Grupos abelianos libres

En Álgebra Lineal es clásica la estructura de espacio vectorial V sobre un cuerpo K. Esta sección trata de estudiar el caso análogo de un grupo abeliano sobre $\mathbf{Z}$.

La notación en grupos abelianos suele ser aditiva. Así, la operación se suele designar mediane $+$, el neutro mediante 0, el simétrico de x se denomina opuesto de x y se escribe $-x$; asimismo, dado $z \in \mathbf{Z}, x \in G$,

$$zx = \begin{cases} x + \cdots + x, \text{si } z > 0 \\ 0, \text{ si } z = 0 \\ -zx, \text{ si } z < 0, \end{cases}$$

Finalmente, en lugar de coproducto diremos suma directa y en vez de $G \times H$ escribiremos $G \oplus H$. Análogamente, $\coprod_{i \in I} G_i$ se escribirá $\oplus_{i \in I} G_i$. En principio, el producto directo arbitrario de grupos abelianos, como aplicaciones de soporte arbitrario, no será objeto de nuestro estudio; de hecho probaremos que todo grupo abeliano libre es isomorfo a un coproducto, es decir suma directa, de copias de $\mathbf{Z}$.

Definición 9.1 *Una parte finita X de un grupo abeliano se dice libre si es vacía o si*

$$z_1 x_1 + \cdots + z_n x_n = 0 \Longrightarrow z_i = 0$$

En caso contrario se dice ligada.

Ejemplos Los elementos no nulos de $\mathbf{Z}$ son libres; en cambio, los elementos de un grupo abeliano finito son ligados, pues si su orden es n, $nx = 0$.

Cualquier parte de $\mathbf{Z}$ con más de un elemento $\{n, m, \ldots\}$ es ligada. En efecto,

$$nm + (-m)n + 0 \ldots = 0$$

Definición 9.2 *Una parte X de un grupo abeliano se dice libre si lo es cualquier parte finita de X. En caso contrario, se dice ligada.*

Ejemplo En el grupo abeliano de los polinomios con coeficientes enteros, el subconjunto

$$\{1, x, x^2, \ldots, x^n, \ldots\}$$

es libre.

Observación 9.3 Pueden trasladarse algunas propiedades conocidas de la teoría de espacios vectoriales, pero no todas...

- Una parte que contenga el 0 es ligada.
- Toda familia con vectores repetidos es ligada.
- No todo elemento no nulo es libre. Elementos en estas condiciones se denominan de *torsión*. Por ejemplo en el grupo abeliano $\mathbf{Q}/\mathbf{Z}$ todo elemento es de torsión.

- No todo subgrupo S de un grupo abeliano poosee un T tal que $G = S \oplus T$. C_4 posee un subgrupo C_2

Definición 9.4 *Se dice base en un grupo abeliano a una parte libre que sea sistema generador.*

Ejemplos

- 1 es base de $\mathbf{Z}$.
- $(1, 0, \ldots, 0), (0, \ldots, 0, 1)$ es base de $\mathbf{Z}^n$. Se dice base canónica.

Definición 9.5 *Un grupo abeliano F se dice libre si posee una base.*

Ejemplos y contraejemplos

1. Cualquier suma directa de copias de $\mathbf{Z}$: $\mathbf{Z}, \mathbf{Z}^2, \ldots, \mathbf{Z}^n, \ldots$ es un grupo abeliano libre de base la canónica.
2. El grupo de polinomios con coeficientes enteros $\mathbf{Z}[x]$ es libre.
3. Ningún grupo abeliano finito puede ser libre, pues carece de partes libres.
4. $\mathbf{Q}$ tampoco puede ser un grupo abeliano libre[1], pues dos o más números racionales forman una familia ligada y un único racional no puede generar $\mathbf{Q}$.

Caractericemos todos los grupos abelianos libres.

Teorema 9.6 *Son equivalentes*

i) *F es libre.*
ii) *F es suma directa interna de subgrupos monógenos infinitos.*
iii) *F es isomorfo a una suma directa de (copias) de $\mathbf{Z}$.*
iv) *Existe un conjunto X y una aplicación $\iota: X \longrightarrow F$ tal que para cada grupo abeliano G y aplicación $f: X \longrightarrow G$ existe un único homomorfismo de grupos $\varphi: F \longrightarrow G$ tal que $\varphi \circ \iota = f$*

Demostración: Antes de nada digamos que el item iv), donde es clave la propiedad universal de la suma directa, será de utilidad a la hora de describir los grupos abelianos libres, salvo isomorfismo, por su rango. Asimismo, el item ii) permite considerar cada grupo abeliano como cociente de un grupo abeliano libre.

i) $\Longrightarrow$ ii): Sea X una base de F y para cada $x \in X$ sea F_x el subgrupo de F generado por x; entonces, al ser x libre su orden es infinito. Ahora $F =< X >$ da $F =< \cup_{x \in X} F_x >$. Por otro lado,

$$z \in F_x \cap < \cup_{y \neq x} F_y > \implies z = nx = n_1 y_1 + \cdots + n_r y_r \overset{X\text{libre}}{\Longrightarrow} z = 0$$

ii) $\Longrightarrow$ iii): Por la proposición 8.23, F es isomorfo a $\oplus_{x \in X} < x >$ y éste a $\oplus_{x \in X} \mathbf{Z}$, pues cada $< x >$ es monógeno infinito luego una copia de $\mathbf{Z}$.

[1] aunque es libre de torsión

iii) $\Longrightarrow$ i): Sea $\oplus_{x\in X}\mathbf{Z} \overset{\varphi}{\cong} F$ y para cada $x \in X$, sea α_x la inyección canónica de $\mathbf{Z}$ en la suma directa y $f_x = (\varphi \circ \alpha_x)(1)$. Veamos que $\{f_x \mid x \in X\}$ es una base de F.

$\{f_x \mid x \in X\}$ es libre

$$z_1 f_{x_1} + \cdots + z_r f_{x_r} = 0_F \Longrightarrow z_1(\varphi \circ \alpha_{x_1})(1) + \cdots + z_r(\varphi \circ \alpha_{x_r})(1) = 0_F$$

Puesto que φ es monomorfismo

$$z_1\alpha_{x_1}(1) + \cdots + z_r\alpha_{x_r}(1) = 0_{\oplus_{x\in X}\mathbf{Z}} \Longrightarrow (z_1\alpha_{x_1}(1) + \cdots + z_r\alpha_{x_r}(1))(x_k) = 0$$

Puesto que (ver proposición 8.17) $z\,\alpha_x(1)(y) = \delta_{x,y}\,z$, se tiene $z_k = 0\,\forall k$.

$\{f_x \mid x \in X\}$ es sistema generador

Al ser φ un epimorfismo es suficiente probar que $\{\alpha_x(1) \mid x \in X\}$ es sistema generador de la suma directa. Dado un g en dicha suma directa, si J es su soporte, sabemos (proposición 8.18 con notación aditiva) que $g = \sum_{j\in J} \alpha_j(g(j))$ y como $g(j) \in \mathbf{Z}$

$$g = \sum_{j\in J} \alpha_j(g(j).1) = \sum_{j\in J} g(j)\alpha_j(1)$$

iii) $\Longrightarrow$ iv): Sea $\oplus_{x\in X}\mathbf{Z} \overset{\lambda}{\cong} F$ y $\iota\colon X \longrightarrow F$ dada por $\iota(x) = \lambda \circ \alpha_x(1)$, donde α_x la inyección canónica de $\mathbf{Z}$ en la suma directa. Dada $f\colon X \longrightarrow G$, sea $(\beta_x\colon \mathbf{Z}_x \longrightarrow G)$ dada por $\beta_x(z) = zf(x)$; es claro que se trata de una familia de homomorfismos. Por la *propiedad universal*, existe un único homomorfismo $\phi\colon \oplus_{x\in X}\mathbf{Z} \longrightarrow G$ tal que $\phi \circ \alpha_x = \beta_x$. Ahora $\varphi = \phi \circ \lambda^{-1}$ es un homomorfismo de F en G y

$$\varphi \circ \iota(x) = \phi \circ \lambda^{-1} \circ \iota(x) = \phi \circ \lambda^{-1} \circ \lambda \circ \alpha_x(1) = \phi \circ \alpha_x(1) = \beta_x(1) = f(x)\,\forall x \in X$$

Por tanto, $\varphi \circ \iota = f$.

Supongamos que $\psi\colon F \longrightarrow G$ satisface $\psi \circ \iota = f$. Entonces,

$$\psi \circ \lambda \circ \alpha_x(1) = \psi \circ \iota(x) = f(x) = \beta_x(1) \Longrightarrow \psi \circ \lambda \circ \alpha_x = \beta_x$$

Por tanto, la unicidad de la *propiedad universal* da $\psi \circ \lambda = \phi$; es decir,

$$\psi = \phi \circ \lambda^{-1} = \varphi$$

iv) $\Longrightarrow$ iii): Veremos que F es una suma directa de $(\mathbf{Z}_x \mid x \in X)$. Al efecto, definimos $\alpha_x\colon \mathbf{Z}_x \longrightarrow F$ mediante $\alpha_x(1) = \iota(x)$. Sea $(\beta_x\colon \mathbf{Z}_x \longrightarrow G)$ una familia de homomorfismos. Definimos $f\colon X \longrightarrow G$ mediante $f(x) = \beta_x(1)$. Entonces, la hipótesis iv) da un único $\varphi\colon F \longrightarrow G$ tal que $f = \varphi \circ \iota$. Por tanto,

$$(\varphi \circ \alpha_x)(1) = \varphi \circ \iota(x) = f(x) = \beta_x(1)$$

En definitiva, $\varphi \circ \alpha_x = \beta_x$.

Finalmente, si existe otro ϕ tal que $\phi \circ \alpha_x = \beta_x$ se tiene

$$\phi \circ \iota(x) = \phi \circ \alpha_x(1) = \beta_x(1) = f(x)$$

Luego la unicidad en iv) da $\phi = \varphi$. Hemos terminado.

Observación 9.7 Una vez descrita la caracterización de grupos abelianos libres la pregunta que se plantea es obvia ¿cada dos bases poseen la misma cantidad de elementos? La respuesta es afirmativa[2].

Teorema 9.8 *Sean X e Y dos bases de F. Entonces $|X| = |Y|$. Se dice rango*[3] *de F.*

Demostración: La técnica de la demostración será la siguiente. Supondremos X finito y probaremos que Y debe ser asimismo finito y que $|X| = |Y|$. A continuación supondremos que todas las bases de F son no finitas y estableceremos una aplicación inyectiva de X en Y.

$\underline{X = \{x_1, \ldots, x_n\}}$:

Entonces,

$$F =< x_1 > \oplus \cdots \oplus < x_n >$$

Sea

$$2F = \{2x \mid x \in F\} =< 2x_1 > \oplus \cdots \oplus < 2x_n >$$

Así,

$$F/2F \cong \oplus_{i=1}^n < x_i > / < 2x_i > \cong \oplus_{i=1}^n \mathbf{Z}/2\mathbf{Z}$$

Por tanto, $|F/2F| = 2^n$. En conclusión cualquier base finita debe poseer n elementos.

Si Y fuera una base infinita, escribiendo x_i como c.l. de los elementos de Y encontraríamos una parte finita Y_o de Y, por tanto libre, que es sistema generador de F. Ahora, $\exists\, y \in Y \setminus Y_o$ y la parte $\{y\} \cup Y_o \subseteq Y$ es ligada.

$\underline{X \text{ arbitrario}}$: Veremos que $|X| = |F|$, lo que indudablemente conlleva una buena ración de teoría de cardinales, que no es objeto de etse curso. Puesto que[4] $|X| \leq |F|$, será suficiente ver la otra desigualdad. Sea S la unión numerable de los productos cartesianos finitos de X:

$$S = X \cup X^2 \cup X^3 \cup \cdots \cup X^n \cup$$

Dado $s \in S$ existe $n \in N$ tal que $s = (x_1, \ldots, x_n) \in X^n$; consideremos el subgrupo $G_s =< x_1, \ldots, x_n >$ de F generado por estos n elementos. Entonces, $F = \cup_{s \in S} G_s$

Eliminando elementos repetidos, G_s es isomorfo a una suma directa finita de copias de $\mathbf{Z}$, por lo que $|G_s| = |Z|$. Basta ver que $|S| = |X|$ y $|F| \leq |S||\mathbf{Z}| = |S|$, pero éstos y otros detalles[5] es lo que se sale del alcance de este curso.

[2] gracias a la conmutatividad de los números enteros

[3] o dimensión

[4] la inclusión de X en F es inyectiva

[5] como $|X| \leq |Y|, |Y| \leq |X| \Longrightarrow |X| = |Y|$ (teorema de Schroeder-Bernstein)

Como en el caso de espacios vectoriales, el rango describe los grupos abelianos libres salvo isomorfismos.

Proposición 9.9 *Dos grupos abelianos libres son isomorfos si y sólo si poseen el mismo rango.*

Demostración: El directo es consecuencia de que un isomorfismo transforma una base en una base.

Para el recíproco supongamos que F y G poseen el mismo rango; sea pues γ una biyección entre X e Y bases respectivas de F y G. Entonces, existen homomorfismos únicos $\varphi: F \longrightarrow G$ y $\phi: G \longrightarrow F$ tales que

$$\varphi \circ \iota_X = \iota_Y \circ \gamma$$

$$\phi \circ \iota_Y = \iota_X \circ \gamma^{-1}$$

Así,

$$(\phi \circ \varphi) \circ \iota_X = \iota_X \quad (\varphi \circ \phi) \circ \iota_Y = \iota_Y$$

Puesto que

$$id_F \circ \iota_X = \iota_X \quad id_G \circ \iota_Y = \iota_Y$$

la unicidad de la propiedad universal da:

$$\phi \circ \varphi = id_f \quad \varphi \circ \phi = 1_G$$

y se trata de isomorfismos entre F y G (uno inverso del otro).

Finalizamos asociando a cada grupo abeliano uno libre que se proyecta sobre él

Proposición 9.10 *Todo grupo abeliano G es cociente de un grupo abeliano libre de rango el tamaño de un conjunto de generadores de G.*

Demostración: Sea X un sistema generador de G y $F = \oplus_{x \in X} \mathbf{Z}$. Entonces, F es libre (véase la demostración del apartado iii) $\Longrightarrow$ i) en 9.6) de rango $|X|$ y existe $\varphi: F \longrightarrow G$ tal que $\varphi \circ \iota$ es la inclusión de X en G. Así, $X \subseteq \varphi(F)$ y φ es epimorfismo.

EJERCICIOS

1. Probar que los coeficintes de un elemento como c.l. de una base son únicos; se diecn coordenadas.
2. Encontrar elementos libres en $\mathbf{Z}$ que no son base de $\mathbf{Z}$.
3. Encontrar elementos libres en $\mathbf{Z}$ no prolongables a una base de $\mathbf{Z}$.
4. Probar que si $m \geq 1$, $m\mathbf{Z}$ es un subgrupo propio de $\mathbf{Z}$ del mismo rango.
5. Encontrar sistemas generadores en $\mathbf{Z}$ que no contienen ninguna base de $\mathbf{Z}$.
6. Sea f un homomorfismo del grupo abeliano libre G en el grupo abeliano H. Probar que son equivalentes:
   (a) f es mono
   (b) Toda familia libre se transforma en una familia libre
   (c) Toda base se transforma en una base
   (d) Existe una base que se transforma en una familia libre.
   (e) $\ker f = 0_G$
7. Sea f un homomorfismo del grupo abeliano libre G en el grupo abeliano H. Probar que son equivalentes:
   (a) f es iso
   (b) Toda base se transforma en una base
   (c) Existe una base que se transforma en una base
8. Probar que los racionales no tienen un sistema generador finito.
9. Probar que el grupo aditivo $\mathbf{Z}[x]$ es isomorfo al multiplicativo $(Q^+)^*$. Deducir que el conjunto de primos es una base de $(Q^+)^*$.
10. Pruébese que todo grupo abeliano libre es libre de torsión[6]

[6] sus elementos no nulos son libres