Introducción a grupos abelianos y módulos
Día 1: Grupos abelianos

G. A. Chicas Reyes

14 de diciembre de 2020

Resumen

Estos son los apuntes para un minicurso de la pre-Escuela CIMPA El Salvador 2020. Agradecimientos a Marvin Alberto Ferman Bell por su ayuda en la preparación de este documento.

1. Grupos abelianos

1.1. Resumen de definiciones

Definición 1.1 *Un **grupo abeliano** es un conjunto A dotado de una operación $+$ que satisface los siguientes axiomas para cualesquiera $x, y, z \in A$:*

- Asociatividad*:* $x + (y + z) = (x + y) + z$.
- Elemento neutro*: existe* $0 \in A$ *tal que* $x + 0 = 0 + x = x$ *para todo* $x \in A$.
- Elementos inversos*: para todo* $x \in A$ *existe* $y \in A$ *tal que* $x + y = y + x = 0$.
- Conmutatividad*:* $x + y = y + x$.

Definición 1.2 *Sean A y B grupos abelianos. Un **homomorfismo de grupos (abelianos)** es una aplicación $f : A \to B$ tal que para cualesquiera $x, y \in A$*

$$f(x + y) = f(x) + f(y).$$

Resulta que la clase de grupos abelianos y todos los homomorfismos entre ellos forman una *categoría*, por lo cual todos nuestros cálculos están teniendo lugar en la **categoría de grupos abelianos**.*

Definición 1.3 *Un **subgrupo** de un grupo abeliano A es un subconjunto no vacío B tal que si $x, y \in B$, entonces $x - y \in B$.*

Definición 1.4 *Dado un subgrupo $B \subseteq A$, se define una clase de equivalencia $\sim$ como sigue: $x \sim y$ si y sólo si $x - y \in B$. El conjunto A/B de clases de equivalencia está dotado de una operación bien definida*

$$\bar{x} + \bar{y} = \overline{x + y}$$

*que le otorga la estructura de grupo abeliano (**grupo cociente**).*

---

*Para más detalles sobre categorías y su uso en álgebra homológica, véase [8], Cap. 1.

Ahora introducimos dos construcciones categóricas (productos y coproductos) que son indispensables en la clasificación de grupos abelianos, pues permiten expresar un grupo en términos de factores más simples.

Definición 1.5 *Sea $\{A_j\}_{j\in J}$ una colección de grupos. Su* ***producto directo*** *se define como el producto cartesiano*

$$\prod_{j\in J} A_j = \{(a_j)_{j\in J} : a_j \in A_j \text{ para todo } j \in J\}$$

dotado de la operación de suma coordenada por coordenada, es decir

$$(a_j)_{j\in J} + (b_j)_{j\in J} = (a_j + b_j)_{j\in J}.$$

Su ***suma directa*** *es el conjunto*

$$\bigoplus_{j\in J} A_j = \left\{ (a_j)_{j\in J} \in \prod_{j\in J} A_j : a_j = 0 \text{ salvo para un número finito de } j \right\}$$

dotado de la operación inducida por el producto directo.

Notamos que $\bigoplus_j A_j$ es un subgrupo de $\prod_j A_j$ y que estas dos construcciones coinciden si y sólo si la colección de grupos es finita.

Ahora repasamos brevemente algunos conceptos específicos al estudio de grupos abelianos.

Definición 1.6 *Un elemento $x \in A$ es de* ***torsión*** *si es de orden finito, es decir si existe $n \neq 0$ tal que $nx = 0$. El conjunto de todos los elementos de torsión de A forma un subgrupo, llamado* ***subgrupo de torsión*** *de A. Decimos que A es* ***libre de torsión*** *si su subgrupo de torsión es trivial.*

Definición 1.7 *Para p primo, decimos que A es un p-**grupo** si todo elemento posee orden igual a una potencia de p; es decir, para todo $x \in A$ existe m tal que $p^m x = 0$.*

Definición 1.8 *Decimos que A es* ***divisible*** *si para todo $x \in A$ y $n \neq 0$ existe $y \in A$ tal que $x = ny$.*

Definición 1.9 *Un grupo abeliano A es* ***libre*** *si posee un conjunto de generadores $\mathbb{Z}$-linealmente independiente; es decir una colección $\{x_j\}_{j\in J} \subseteq A$ tal que todo $x \in A$ puede escribirse de manera única como*

$$x = \sum_{\ell=1}^{n} a_{j_\ell} x_{j_\ell} \qquad (a_{j_1}, \ldots, a_{j_n} \in \mathbb{Z}).$$

Equivalentemente, existe un isomorfismo $A \cong \bigoplus_J \mathbb{Z}$.

Definición 1.10 *Un grupo abeliano A es* ***finitamente generado*** *si posee un conjunto finito de generadores; es decir, existen $x_1, \ldots, x_n \in A$ tales que todo $x \in A$ puede escribirse como*

$$x = \sum_{i=1}^{n} a_i x_i \qquad (a_i \in \mathbb{Z}).$$

Un grupo abeliano es ***cíclico*** *si es generado por un solo elemento.*

1.2. Ejemplos

- Los grupos $\mathbb{Z}/n\mathbb{Z}$, que son cíclicos y finitos (en particular de torsión).
- $\mathbb{Z}$, que es un grupo cíclico infinito y además un grupo abeliano libre.
- $\mathbb{Q}$, un grupo abeliano divisible y libre de torsión.
- El anillo de enteros p-ádicos $\mathbb{Z}_p$, que es un grupo libre de torsión, y además un anillo compacto junto a la topología p-ádica.
- El cuerpo de los números p-ádicos $\mathbb{Q}_p$, que es un grupo divisible y libre de torsión, y además un cuerpo localmente compacto junto a la topología p-ádica.†
- El grupo de Prüfer $\mathbb{Z}(p^\infty) = \mathbb{Z}[p^{-1}]/\mathbb{Z} = \mathbb{Q}_p/\mathbb{Z}_p$, que es un p-grupo divisible y de torsión.
- El grupo del círculo $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, que es un grupo de Lie abeliano compacto.
- El grupo de raíces de la unidad $\mathbb{Q}/\mathbb{Z}$, que es el subgrupo de torsión de $\mathbb{T}$ y además puede expresarse como una suma directa
$$\mathbb{Q}/\mathbb{Z} \cong \bigoplus_p \mathbb{Z}(p^\infty).$$

2. Teoría de divisores elementales

En el álgebra lineal, las teorías de formas canónicas (diagonalización, triangulación, forma de Jordan…) son sumamente útiles para el estudio y clasificación de matrices y aplicaciones lineales. A continuación describiremos la construcción de una forma canónica para matrices de coeficientes enteros.‡

Denotemos por $M(m,n;\mathbb{Z})$ el conjunto de matrices de $m \times n$ con coeficientes enteros.

Definición 2.1 *Una* ***operación elemental por filas*** *es una de los siguientes tipos.*

(I) *Intercambiar dos filas.*

(II) *Multiplicar por* -1 *todos los elementos de una fila.*

(III) *Sumar a una fila un múltiplo escalar de otra fila.*

Una ***operación elemental por columnas*** *es una de los siguientes tipos.*

(I) *Intercambiar dos columnas.*

(II) *Multiplicar por* -1 *todos los elementos de una columna.*

(III) *Sumar a una fila un múltiplo escalar de otra columna.*

Para expresar estas operaciones en el lenguaje del álgebra lineal, conviene introducir tres tipos de **matrices elementales** de $n \times n$.

†Para mayor información sobre enteros y números p-ádicos, se recomienda un texto tal y como [7], Cap. 1.
‡En inglés, a veces se conoce como *Smith normal form.*

Definición 2.2

(I) *$P_n(i,j)$ es la matriz tal que todos los coeficientes sobre su diagonal a excepción de (i,i) y (j,j), y además los coeficientes en (i,j) y (j,i) son 1, mientras que el resto son 0.*

$$P_n(i,j) = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & \mathit{0} & \\ & & 1 & & & & & & \\ & & & 0 & \cdots & 1 & & & \\ & & & \vdots & \ddots & \vdots & & & \\ & & & 1 & \cdots & 0 & & & \\ & & & & & & 1 & & \\ & \mathit{0} & & & & & & \ddots & \\ & & & & & & & & 1 \end{pmatrix}$$

(II) *$Q_n(i,-1)$ es la matriz tal que todos los coeficientes sobre su diagonal a excepción de (i,i) son 1, el coeficiente en (i,i) es -1 y el resto son 0.*

$$Q_n(i;-1) = \begin{pmatrix} 1 & & & & & & \\ & 1 & & & & \mathit{0} & \\ & & \ddots & & & & \\ & & & -1 & & & \\ & & & & 1 & & \\ & \mathit{0} & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

(III) *$R_n(i,j;c)$ donde $i \neq j$ es la matriz con todos sus coeficientes sobre su diagonal igual a 1, el coeficiente en (i,j) igual a $c \in \mathbb{Z}$, y el resto son 0.*

$$R_n(i,j;c) = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & \mathit{0} & \\ & & \ddots & & & & & \\ & & & 1 & & c & & \\ & & & & \ddots & & & \\ & & & & & 1 & & \\ & \mathit{0} & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}$$

Es inmediato comprobar lo siguiente.

Proposición 2.3 *Sea $A \in M(m,n;\mathbb{Z})$.*

(I) *Las operaciones elementales por filas sobre A corresponden a multiplicar por la **izquierda** alguna matriz elemental P_m, Q_m o R_m.*

(II) *Las operaciones elementales por columnas sobre A corresponden a multiplicar por la **derecha** alguna matriz elemental P_n, Q_n o R_n.*

Las matrices elementales cumplen otra propiedad adicional de interés: son invertibles.

Definición 2.4 *Una **matriz unimodular** es una matriz cuadrada invertible (con coeficientes enteros).*

Es sencillo comprobar que el producto de dos matrices unimodulares es unimodular, y además la inversa de una matriz unimodular también lo es. Además, toda matriz unimodular tiene determinante ± 1.

Definición 2.5 *Decimos que dos matrices $A, B \in M(m,n;\mathbb{Z})$ son **equivalentes** si podemos obtener una a partir de la otra aplicando un número finito de transformaciones elementales.*

Teorema 2.6 *Toda matriz $A \in M(m,n;\mathbb{Z})$ es equivalente a una de la forma*

$$\left(\begin{array}{ccc|c} e_1 & & & \\ & \ddots & & 0 \\ & & e_r & \\ \hline & 0 & & 0 \end{array}\right)$$

donde $e_1, \ldots, e_r$ son números naturales tales que $e_i \mid e_{i+1}$ para todo $i = 1, \ldots, r-1$. Más aún, esta sucesión es únicamente determinada por A.

Demostración.

Existencia. Procedemos por inducción sobre m. Supongamos primero que $m = 1$, es decir $A = (a_1, \cdots, a_n)$. Si $A = 0$ el resultado es trivial, así que asumamos $A \neq 0$. Consideramos todas las matrices $(a'_1, a'_2, \ldots, a'_n)$ equivalentes a A. Por el principio del buen orden, podemos elegir $A_1 = (e_1, a'_2, \ldots, a'_n)$ con e_1 mínimo.

Afirmamos que $e_1 \mid a'_i$ para todo $i \geq 2$. En efecto, si tuviéramos $e_1 \nmid a'_i$, por el algoritmo de la división podemos escribir $a'_i = qe_1 + r$ donde $1 \leq r \leq e_1 - 1$. Multiplicando por q la columna 1 y restándosela a la columna i vemos que $A_1 \sim (e_1, a'_2, \ldots, r, \ldots)$. Intercambiando las columnas 1 e i resulta que $A_1 \sim (r, a_2, \ldots, e_1, \ldots)$, pero como $r < e_1$ esto contradice la minimalidad de e_1. Por tanto e_1 divide a a'_i para todo i, y razonando igual que arriba concluimos que $A_1 \sim (e_1, 0, \ldots, 0)$.

Veamos ahora el caso $m \geq 2$. Nuevamente asumimos que $A \neq 0$, pues de lo contrario no hay nada que probar. Gracias al principio del buen orden, de entre todas las matrices equivalentes a A, podemos seleccionar A'_1 de modo que su $(1,1)$-ésima entrada e_1 sea mínima. Escribamos

$$A \sim A' = \begin{pmatrix} e_1 & a'_{12} & \cdots \\ a'_{21} & & \\ \vdots & \ddots & \\ & & \end{pmatrix}$$

Usando un razonamiento análogo al caso anterior, puede comprobarse que $e_1 \mid a'_{i1}$ y $e_1 \mid a'_{1j}$ para cualesquiera $i, j \geq 2$, y mediante transformaciones elementales obtenemos

$$A \sim \left(\begin{array}{c|c} e_1 & 0 \\ \hline 0 & A_{m-1,n-1} \end{array}\right)$$

donde $A_{m-1,n-1} \in M(m-1, n-1, \mathbb{Z})$. Aplicando la hipótesis inductiva, podemos escribir

$$A_{m-1,n-1} \sim \left(\begin{array}{ccc|c} e_2 & & & \\ & \ddots & & 0 \\ & & e_r & \\ \hline & 0 & & 0 \end{array}\right)$$

donde $e_i \mid e_{i+1}$ para todo $i \geq 2$.

Nos queda establecer que $e_1 \mid e_2$. En caso contrario, tuviéramos que $e_2 = qe_1 + r$ donde $1 \leq r \leq e_1 - 1$. Usando operaciones elementales, podemos llevar a r hasta la $(1,1)$-ésima entrada, lo cual contradice la minimalidad de e_1. Concluimos que hemos encontrado una sucesión de elementos $e_1, \ldots, e_r$ que satisfacen las condiciones del enunciado.

Unicidad. Denotamos por d_k el máximo común divisor de todos los menores de tamaño $k \times k$ en A. Es un ejercicio interesante comprobar que *los d_k son invariantes bajo transformaciones elementales.* Al calcularlos a partir de la forma canónica obtenemos que $d_k = e_1 \ldots e_k$. Resolviendo para e_k concluimos que $e_1 = d_1$ y $e_k = d_k / d_{k-1}$ para $k \geq 2$, lo cual muestra que los e_k se calculan de manera única a partir de A. ■

Puesto que las operaciones elementales corresponden a multiplicar matrices elementales (por la izquierda o derecha), y estas son matrices unimodulares, tenemos otra manera de expresar la forma canónica.

Corolario 2.7 *Para toda $A \in M(m, n; \mathbb{Z})$ existen matrices unimodulares P y Q de tamaño $m \times m$ y $n \times n$ respectivamente, tales que*

$$PAQ = \left(\begin{array}{ccc|c} e_1 & & & \\ & \ddots & & 0 \\ & & e_r & \\ \hline & 0 & & 0 \end{array}\right)$$

donde $e_1, \ldots, e_r$ son números naturales tales que $e_i \mid e_{i+1}$ para todo $i = 1, \ldots, r-1$. Más aún, esta sucesión es únicamente determinada por A.

Conviene notar que la demostración del Teorema 2.6 también nos da una manera práctica de calcular la forma canónica de cualquier matriz (mediante operaciones elementales).

Corolario 2.8 *Toda matriz unimodular puede expresarse como producto finito de matrices elementales.*

Demostración. Sea A una matriz unimodular. Usando la notación del Teorema 2.6, tenemos que $d_n = |\det A| = e_1 \cdots e_n = 1$. Esto implica que $e_i = 1$ para todo i, por lo cual la forma canónica de A es la matriz identidad. Así, $PAQ = I$, es decir $A = P^{-1}Q^{-1}$. ■

3. Clasificación de grupos abelianos finitamente generados

Teorema 3.1 *Sean R un DIP, y M un R-módulo libre de rango m. Entonces todo R-submódulo N de M es libre, y además* $\operatorname{rank} N \leq \operatorname{rank} M$.

Demostración. Se procederá por inducción sobre m. La afirmación es evidente para $N = 0$, así que asumiremos que $N \neq 0$. Supongamos primero que $m = 1$, y sea $\{u\}$ una base para M. Consideramos el conjunto

$$I = \{c \in R : cu \in N\}.$$

Comprobamos que este es un ideal de R, y puesto que este es un DIP, podemos escribir $I = (a)$ para algún $a \in R$. Afirmamos que $a \neq 0$. En efecto, puesto que $N \neq 0$, existe $x \neq 0$ tal que $x \in N$; en particular $x \in M$ así que $x = ku$ donde $k \in R$, y como $x \neq 0$ resulta que k es un elemento no nulo de I.

Ahora bien, afirmamos que $\{au\}$ es una base para N. Por un lado, si $b(au) = (ba)u = 0$, entonces $ba = 0$ puesto que $\{u\}$ es una base para M. Ya que $a \neq 0$ y R es dominio, resulta que $b = 0$. Se sigue que $\{au\}$ es linealmente independiente. Por otro lado, consideramos un elemento cualquiera de N, que podemos escribir como cu para algún $c \in R$. Entonces $c \in I = (a)$, así que $c = ra$ para algún $r \in R$. Esto significa que $cu = r(au)$, por lo cual $\{au\}$ genera a N. En conclusión, N es un submódulo libre de rango 1.

A continuación abordamos el caso $m \geq 2$. Supongamos que M es un módulo libre de base $\{u_1, \dots, u_m\}$. Denotamos por M' el submódulo generado por $\{u_1, \dots, u_{m-1}\}$; notamos en particular que este es un módulo libre de rango $m-1$. Definiendo además $N' = N \cap M'$, este es un submódulo de M' al cual podemos aplicar la hipótesis inductiva; deducimos que N' es un submódulo libre de rango $s \leq m-1$. Fijamos una base $v_1, \dots, v_s$ para N'.

Consideramos la aplicación $f : M \to R$ que proyecta a un elemento $c_1 u_1 + \cdots + c_m u_m$ sobre su m-ésima coordenada c_m. Este es un homomorfismo de módulos que es evidentemente sobreyectivo, y además $\operatorname{Ker} f = M'$. Observamos que $f(N)$ es un submódulo de R, es decir un ideal; luego podemos escribir $f(N) = (a)$ para algún $a \in R$. Aquí tenemos dos posibilidades. Si $a = 0$, entonces $N = M'$ y así $N = N'$, por lo cual N es un submódulo libre de rango $s \leq m-1 < m$. Por otra parte, consideremos el caso $a \neq 0$. Podemos tomar $v \in N$ tal que $f(v) = a$. Afirmamos entonces que $v, v_1, \dots, v_s$ es una base para N.

Comprobemos esta afirmación. Primero, sea $y \in N$ arbitrario. Podemos escribir $f(y) = ra$ para algún $r \in R$. Entonces $y - rv \in \operatorname{Ker} f$, pero además $y - rv \in N$, así que $y - rv \in \operatorname{Ker} f \cap N = N'$. Luego existen $r_1, \dots, r_s \in R$ tales que

$$y - rv = r_1 v_1 + \cdots + r_s v_s$$

de donde $y = rv + r_1 v_1 + \cdots + r_s v_s$, y por tanto $v, v_1, \dots, v_s$ generan a N. Ahora bien, supongamos que existe una relación

$$\alpha v + \alpha_1 v_1 + \cdots + \alpha_s v_s = 0.$$

Entonces

$$\alpha a = \alpha f(v) = f(\alpha v + \alpha_1 v_1 + \cdots + \alpha_s v_s) = f(0) = 0.$$

De lo anterior se desprende que $\alpha a = 0$, y la hipótesis $a \neq 0$ nos da $\alpha = 0$. Luego $\alpha_1 v_1 + \cdots + \alpha_s v_s = 0$, y como $v_1, \dots, v_s$ son linealmente independientes, deducimos que $\alpha_1 = \cdots = \alpha_s = 0$. Por tanto $v, v_1, \dots, v_s$ son linealmente independientes. De esta manera, hemos demostrado que N es un módulo libre de rango $s + 1 \leq m$, y hemos terminado. ∎

Teorema 3.2 *Sea M un grupo abeliano libre de rango finito. Entonces todo subgrupo N es libre y además* $\operatorname{rank} N \leq \operatorname{rank} M$. *Más aún, si $u_1, \ldots, u_r$ es una base para M, entonces existen números naturales $e_1, \ldots, e_s$ tales que $e_1 \mid e_2 \mid \cdots \mid e_s$ y $\{e_1 u_1, \ldots, e_s u_s\}$ es una base para N.*

Demostración. La primera parte ya fue establecida, gracias al hecho de que $\mathbb{Z}$ es un DIP. Para la segunda usaremos la teoría de divisores elementales.

Sean $x_1, \ldots, x_r$ una base para M y $y_1, \ldots, y_s$ una base para N. Podemos escribir

$$y_i = \sum_{j=1}^{r} a_{ij} x_j; \qquad a_{ij} \in \mathbb{Z}, 1 \leq i \leq s.$$

En otras palabras, usando notación matricial

$$\begin{pmatrix} y_1 \\ \vdots \\ y_s \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}.$$

De la teoría de divisores elementales, existe una matriz unimodular P de $s \times s$ y una matrix unimodular Q de $r \times r$ tal que

$$PAQ \sim \left(\begin{array}{ccc|c} e_1 & & & \\ & \ddots & & \mathbf{0} \\ & & e_s & \end{array} \right)$$

donde $e_1, \ldots, e_s \in R$ satisfacen $e_1 \mid e_2 \mid \cdots \mid e_s$.

Efectuando los cambios de base

$$\begin{pmatrix} v_1 \\ \vdots \\ v_s \end{pmatrix} = P \begin{pmatrix} y_1 \\ \vdots \\ y_s \end{pmatrix}; \qquad \begin{pmatrix} u_1 \\ \vdots \\ u_r \end{pmatrix} = Q^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}$$

resulta que $u_1, \ldots, u_r$ y $v_1, \ldots, v_s$ son bases para M y N, respectivamente, tales que

$$\begin{pmatrix} v_1 \\ \vdots \\ v_s \end{pmatrix} = \left(\begin{array}{ccc|c} e_1 & & & \\ & \ddots & & \mathbf{0} \\ & & e_s & \end{array} \right) \begin{pmatrix} u_1 \\ \vdots \\ u_r \end{pmatrix}.$$

A partir de la expresión anterior, obtenemos de inmediato que $v_i = e_i u_i$ para todo $i = 1, \ldots, s$. En particular notamos que ■

Corolario 3.3 *Todo grupo abeliano finitamente generado M es isomorfo a un grupo de la forma*

$$\mathbb{Z}^r \oplus \mathbb{Z}/e_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/e_s\mathbb{Z}$$

donde $r \geq 0$, $e_i \geq 2$ y además $e_1 \mid e_2 \mid \cdots \mid e_s$ están determinados de manera única por M (salvo isomorfismo).

Demostración. Supongamos que M es generado por los elementos $x_1, \ldots, x_t$. Consideramos el homomorfismo de grupos

$$\phi : \mathbb{Z}^t \to M$$
$$(n_1, \ldots, n_t) \mapsto \sum_{i=1}^{t} n_i x_i$$

Escribiendo $N = \operatorname{Ker} \phi$, por el Teorema 3.2 existen una base $u_1, \ldots, u_t$ para $\mathbb{Z}^t$ y números naturales $e_1, \ldots, e_{s'}$ tales que $e_1 \mid \cdots \mid e_{s'}$ y $e_1 u_1, \ldots, e_{s'} u_{s'}$ es una base para N. Pongamos $t - s' = r$, y sea ℓ el índice tal que $e_1 = \cdots = e_\ell = 1$, $e_{\ell+1} > 1$. Por último, intercambiando $e_{\ell+1}, \ldots$ con $e_1, \ldots$ y escribiendo $s = s' - \ell$, una aplicación del teorema de isomorfía nos permite concluir que

$$M \cong \mathbb{Z}^t / N \cong \mathbb{Z}/e_1\mathbb{Z} \oplus \cdots \mathbb{Z}/e_s\mathbb{Z} \oplus \mathbb{Z}^r. \qquad \blacksquare$$

Finalizamos mencionando un teorema de clasificación alternativo, que se suele conocer como la **descomposición primaria** de un grupo.

Proposición 3.4 *Todo grupo abeliano finitamente generado A es isomorfo a uno de la forma*

$$\mathbb{Z}^r \oplus \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \mathbb{Z}/q_k\mathbb{Z}$$

donde r es un número natural y los q_i son potencias de primos.

Tanto los divisores elementales como la descomposición primara contienen la misma información. Para más detalles, véase [2], §5.2.

Ejercicios

1. Sea p un número primo. Determine el número de grupos abelianos distintos (salvo isomorfismo) cuyo orden es: (a) p^2. (b) p^3. (c) p^4.

2. Considere el siguiente homomorfismo de grupos abelianos.

$$\phi : \mathbb{Z}^3 \to \mathbb{Z}$$
$$(x, y, z) \mapsto 2x + 3y + 4z$$

   Encuentre una base para $\operatorname{Ker} \phi$.

3. Sea A un grupo abeliano generado por elementos x_1, x_2, x_3 sujetos a las relaciones

$$2x_1 - x_2 = 0$$
$$x_1 - 3x_2 = 0$$
$$x_1 + x_2 + x_3 = 0$$

   Determine el tipo de isomorfía de A.

4. Demuestre que los $d_1, \ldots, d_k$ definidos en el Teorema 2.6 son invariantes bajo transformaciones elementales.

Referencias

[1] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton University Press, 1956.

[2] D. S. Dummit and R. M. Foote, *Abstract algebra*, Wiley, 2003.

[3] L. Fuchs, *Infinite abelian groups*, vol. I, Pure and Applied Mathematics, no. 36, Academic Press, 1970.

[4] A. Grothendieck, *Sur quelques points de l'algèbre homologique*, Tohoku Math. J. **9** (1957), no. 2, 119–221.

[5] S. Lang, *Algebra*, Graduate Texts in Mathematics, no. 212, Springer, 2002.

[6] S. Mac Lane, *Homology*, Academic Press, New York, 1963.

[7] A.M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, no. 198, Springer-Verlag, 2000.

[8] J.J. Rotman, *An introduction to homological algebra*, Universitext, Springer New York, 2008.

ESCUELA DE MATEMÁTICA, FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA, UNIVERSIDAD DE EL SALVADOR, FINAL AV. "MÁRTIRES ESTUDIANTES DEL 30 DE JULIO", CIUDAD UNIVERSITARIA, SAN SALVADOR, EL SALVADOR.

Correo electrónico: `gabriel.chicas@ues.edu.sv`