Sobre grupos divisibles e isomorfismos relacionados

Trabajo de Grado

Autor:

Andrés Sebastián Cañas Pérez

Director:

Dr. Héctor Edonis Pinedo Tapia

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Matemáticas
Bucaramanga, Agosto de 2015

Objetivos

Nuestro objetivo principal es demostrar que los grupos

$$\mathbb{C}^*, \quad \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}, \quad \mathbb{R}/\mathbb{Z}, \quad \prod_q \mathbb{Z}(q^\infty) \;\; \text{y} \;\; S^1,$$

donde q recorre todos los números primos, son isomorfos dos a dos. Además, queremos:

- Profundizar definiciones y resultados de álgebra lineal y teoría de conjuntos que se han estudiado previamente en los cursos de pregrado.
- Adquirir conceptos y propiedades sobre teoría de módulos y grupos abelianos divisibles.
- Hacer un estudio detallado en teoría elemental de grupos y la teoría de anillos para crear bases teóricas fuertes y alcanzar el objetivo general.

Grupos divisibles

Los grupos de torsión son base en nuestro trabajo. Por esto debemos recordar definiciones y proposiciones:

Definición

Sea G un grupo abeliano. Definimos el **subgrupo de tosión** *tG de G como*

$$tG = \{a \in G : a \text{ tiene orden finito } \}.$$

Diremos que G es un **grupo de torsión** *si $G = tG$ y que G es* **libre de torsión** *si $tG = \{0\}$.*

Ejemplo

Todo grupo abeliano fínito es de torsión. En efecto, sean G un grupo finito y $a \in G$. Por definición sabemos que $tG \subseteq G$, ahora queremos ver la otra contenencia. Por el Teorema de Lagrange obtenemos que $ord(a)||G|$ y podemos concluir que $ord(a)$ es finito. Por lo tanto $tG = G$. Es decir, todo grupo finito es de torsión.

Ejemplo

Consideremos el grupo aditivo $\mathbb{Z}$. Sea $a \in \mathbb{Z}$ tal que $a \neq 0$. Sabemos que para todo $n \in \mathbb{N}, n \geq 1$, $na \neq 0$, así a es de orden infinito y por lo tanto $t\mathbb{Z} = \{0\}$, es decir $\mathbb{Z}$ es libre de torsión.

Ejemplo

Veamos que el grupo multiplicativo $\mathbb{C}^*$ no es de torsión ni es libre de torsión. Sabemos que $2^n > 0$ para todo $n \in \mathbb{N}$, luego $2 \notin t\mathbb{C}^*$, entonces $\mathbb{C}^*$ no es de torsión. Para ver que no es libre de torsión, sea $n \in \mathbb{N}, n > 1$ y consideremos cualquier raíz n-ésima de la unidad diferente de 1, estos números estarán en $t\mathbb{C}^*$ y por lo tanto $t\mathbb{C}^* \neq \{1\}$.

Teorema

Sean G y H grupos. Tenemos que

- *i.* *G/tG es libre de torsión.*
- *ii.* *Si $G \cong H$, entonces $tG \cong tH$ y $G/tG \cong H/tH$.*

Definición

Sea G un grupo abeliano y p un primo.

i. *Decimos que G es un* **grupo p-primario** *si todos sus elementos tienen como orden una potencia de p.*
ii. *Definimos el* **componente p-primario** *G_p de G como el subgrupo de todos los elementos cuyo orden es potencia de p.*

Teorema

Todo grupo abeliano de torsión G es suma directa de sus componentes p-primarios:

$$G = \bigoplus_{p \in \mathbb{P}} G_p.$$

donde $\mathbb{P}$ es el conjunto de números primos.

Lema

Sean G y H grupos abelianos. Si $G \cong H$ entonces $G_p \cong H_p$ para todo p primo.

Grupos divisibles

Definición

Sea D un grupo abeliano. Entonces, D es llamado **divisible** *si para todo $d \in D$ y para todo entero positivo n existe $d' \in D$ tal que $d = nd'$.*

Ejemplo

i. $\mathbb{Q}$ es un grupo divisible bajo la adición.
En efecto, sean $d \in \mathbb{Q}$ y sea n un entero positivo cualquiera. Si $d' = d/n$, tenemos que $d' \in \mathbb{Q}$. De aquí se sigue $d = nd'$ y $\mathbb{Q}$ es un grupo divisible.

ii. Veamos que cualquier grupo abeliano $G \neq \{e\}$ finito, no es divisible. Supongamos que G es divisible, por lo tanto para $x \in G \setminus \{e\}$ y $|G|$ existe $y \in D$ tal que $x = |G|y$. Como G es finito, $|G|y = e$, entonces $x = e$, lo cual nos genera una contradicción.

iii. Sea K un cuerpo algebraicamente cerrado. Sean $a \in K^*$ y $n \in \mathbb{N}$, consideremos el polinomio $f(X) = X^n - a$ en $K[X]$, como K un cuerpo algebraicamente cerrado, este polinomio tiene raíces en K. Es decir, existe $y \in K^*$ tal que $y^n = a$ y por lo tanto el grupo multiplicativo K^* es divisible.

Grupos divisibles

El siguiente teorema nos da propiedades de los grupos divisibles que serán de suma importancia.

Teorema

Sean H y G grupos abelianos.

- *i.* *Si G es divisible y $H \leq G$, entonces G/H es divisible.*
- *ii.* *Si G es divisible y $\phi : G \to H$ un homomorfismo entonces $\phi(G)$ es un subgrupo divisible de H. Es decir, la imagen de un divisible bajo un homomorfismo es divisible.*
- *iii.* *La suma directa de grupos es divisible si y sólo si cada sumando es divisible.*
- *iv.* *Un grupo abeliano D libre de torsión es divisible si y sólo si es un espacio vectorial sobre $\mathbb{Q}$.*
- *v.* *Todo subgrupo divisible de un grupo abeliano es un sumando directo.*
- *vi.* *Sea G un grupo, $H \leq G$ y D un grupo divisible. Sea $f : H \to D$ un homomorfismo. Entonces f puede ser extendido a un homomorfismo G en D.*

Observación: Cuando D es un grupo divisible libre de torsión, dado $d \in D$ y $n \in \mathbb{N}$, existe un único $d' \in D$ tal que $d = nd'$. Para el ítem *iv.*, dados $d \in D$ y $m/n \in \mathbb{Q}$, la acción de $\mathbb{Q}$ en D está definida por

$$(m/n)d = md',$$

donde $d' \in D$ es el único elemento tal que $d = nd'$.

Grupos divisibles

Definición

Si G es un grupo abeliano y n es un entero positivo, entonces

$$G[n] = \{g \in G : ng = 0\}.$$

Ejemplo

Consideremos $\mathbb{Z}_4$. tenemos que $\mathbb{Z}_4[3] = \{g \in G : 3g = 0\} = \{0\}$. En general, si m y n son primos relativos, entonces $\mathbb{Z}_m[n] = \{0\}$.

Teorema

Sean G y H grupos abelianos divisibles p-primarios, entonces $G \cong H$ si y sólo si $G[p] \cong H[p]$.

Un grupo importante para nosotros es el grupo de Prüfer, llamado así en honor al matemático alemán Heinz Prüfer reconocido por sus contribuciones a la teoría de grupos abelianos y números algebraicos, entre otros.

Definición

Sea $p \in \mathbb{Z}$ primo. El **grupo de Prüfer** *de tipo p^∞ es el subgrupo del grupo multiplicativo $\mathbb{C}^*$ dado por:*

$$\mathbb{Z}(p^\infty) = \langle e^{2\pi i/p^n} : n \geq 1 \rangle = \{ e^{2\pi im/p^n} : m \in \mathbb{Z}, n \in \mathbb{N} \}$$

Teorema

Sea p un número primo. Entonces $\mathbb{Z}(p^\infty)$ es un grupo abeliano divisible p-primario.

Gracias a este grupo se obtiene el siguiente teorema que clasifica todos los grupos abelianos divisibles.

Teorema

Todo grupo abeliano divisible es isomorfo a la suma directa de copias de $\mathbb{Q}$ y copias de $\mathbb{Z}(p^\infty)$ para varios primos p.

Isomorfismos entre grupos divisibles

La siguiente definición nos dará la base para demostrar que dos grupos divisibles son isomorfos:

Definición

Si D es un grupo abeliano divisible se define

$$\delta_\infty = dim_{\mathbb{Q}}(D/tD)$$

y para todo $p \in \mathbb{Z}$ primo, se define

$$\delta_p = dim_{\mathbb{Z}_p}(D[p])$$

La definición anterior tiene sentido pues ya vimos todo grupo libre de torsión es espacio vectorial sobre $\mathbb{Q}$.
Además, dado cualquier grupo divisible D y p primo, $D[p]$ es un espacio vectorial sobre $\mathbb{Z}_p$.
Sean $d \in D[p]$ y $\bar{x} \in \mathbb{Z}_p$, entonces existe $n \in \mathbb{N}$ tal que $0 \leq n \leq p-1$ y $x \equiv n \pmod{p}$, definamos

$$\bar{x}d = nd.$$

Esta multiplicación está bien definida y da a $D[p]$ estructura de $\mathbb{Z}_p$ espacio vectorial.

Junto la definición anterior, el siguiente teorema es la herramienta más importante para cumplir con nuestro objetivo:

Isomorfismos entre grupos divisibles

Teorema

Sean D y D' grupos abelianos divisibles. Entonces $D \cong D'$ si y sólo si $\delta_\infty(D) = \delta_\infty(D')$ y $\delta_p(D) = \delta_p(D')$ para todo p primo.

Demostración.

($\Rightarrow$) Como $D \cong D'$, tenemos que $tD \cong tD'$ y $D/tD \cong D'/tD'$ como grupos. Ahora, D/tD y D'/tD' son espacios sobre $\mathbb{Q}$. Queremos ver que ellos son isomorfos como espacios vectoriales. Existe $f : D/tD \to D'/tD'$ un isomorfismo de grupos, veamos que f puede ser vista como una transformación lineal biyectiva entre espacios vectoriales sobre $\mathbb{Q}$.

Sea $d \in D/tD$ y $m/n \in \mathbb{Q}$, como D/tD es divisible y libre de torsión, $\exists!\, d' \in D/tD$ tal que $d = nd'$, luego $f(d) = f(nd')$ y concluimos que $f(d')$ es el único elemento en D'/tD' tal que $f(d) = nf(d')$. Ahora, sabemos que

$$(m/n)d = md' \text{ y } (m/n)f(d) = mf(d') = f(md').$$

A partir de esto obtenemos que $(m/n)f(d) = f((m/n)d)$, y por lo tanto D/tD y D'/tD' son isomorfos como espacios vectoriales sobre $\mathbb{Q}$.

Isomorfismos entre grupos divisibles

Demostración (Cont.)

Sabemos que las componentes p-primarias $(tD)_p \cong (tD')_p$ para todo p. Además, $(tD)_p[p] \cong (tD')_p[p]$ y como $D[p] = (tD)_p[p]$ obtenemos que $D[p] \cong D'[p]$ como grupos abelianos. De forma análoga al caso anterior se demuestra que $D[p] \cong D'[p]$ como espacios vectoriales sobre $\mathbb{Z}_p$, es decir, $\delta_p(D) = \delta_p(D')$.

($\Leftarrow$) Escribimos

$$D = V \oplus \bigoplus_p T_p, \quad D' = V' \oplus \bigoplus_p T'_p,$$

donde V y V' son los subgrupos divisibles libres de torsión, T_p y T'_p son los componentes p-primarios correspondientes. Luego $\delta_p(D) = \delta_p(D')$ implica que $T_p \cong T'_p$, es decir, existe $f_p : T_p \to T'_p$ isomorfismo para todo p. Mientras que $\delta_\infty(D) = \delta_\infty(D')$ implica que $V \cong V'$, es decir, existe $f_V : V \to V'$ isomorfismo. Dado $d \in D$, $d = d_v + \sum_p d_p$ donde, $d_v \in V$ y $d_p \in T_p$. Definimos $f : D \to D'$ por $f(d) = f_v(d_v) + \sum_p f_p(d_p)$. Luego, f es isomorfismo y por lo tanto $D \cong D'$. $\square$

En el inicio del trabajo nos propusimos encontrar una herramienta nueva para demostrar isomorfismos entre grupos divisibles. Para esto consideremos los grupos

$$\mathbb{C}^*, \quad \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}, \quad \mathbb{R}/\mathbb{Z}, \quad \prod_q \mathbb{Z}(q^\infty) \ \text{ y } \ S^1.$$

Donde $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. Primero queremos ver que estos grupos son divisibles para poder aplicar el teorema anterior.

Veamos que $\mathbb{R}$ es divisible. Sea $x \in \mathbb{R}$ y $n \in \mathbb{N}$, entonces $y = x/n \in \mathbb{R}$ y $y = nx$. Ahora, $\mathbb{Q}$ es divisible, entonces $\mathbb{Q}/\mathbb{Z}$ es divisible y como $\mathbb{R}$ es divisible $\mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}$ también lo será.

Para $\mathbb{C}^*$ ya sabemos que dados $x \in \mathbb{C}^*$ y $n \in \mathbb{N}$ existe $y \in \mathbb{C}^*$ tal que $x = y^n$. De manera análoga S^1 es divisible. Por otro lado ya vimos que el grupo de Prüfer es divisible, luego $\prod_q \mathbb{Z}(q^\infty)$ es divisible.

Isomorfismos entre grupos divisibles

Teorema

Los siguientes grupos abelianos son isomorfos:

$$\mathbb{C}^*, \quad \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}, \quad \mathbb{R}/\mathbb{Z}, \quad \prod_q \mathbb{Z}(q^\infty) \ \text{ y } \ S^1,$$

donde q recorre el conjunto de los números primos.

Demostración.

Ya sabemos que todos los grupos listados anteriormente son divisibles así que por el teorema anterior debemos mirar que para cualesquiera dos grupos de estos, D y D' se tiene $\delta_\infty(D) = \delta_\infty(D')$ y $\delta_p(D) = \delta_p(D')$ para todo p primo.
Veamos que $\delta_p(D) = 1$, donde p es un primo cualquiera.

i. Para $\mathbb{C}^*$ los elementos en $\mathbb{C}^*[p]$ serán las raíces p-ésimas de la unidad, es decir

$$\mathbb{C}^*[p] = \{e^{2\pi i \frac{k}{p}} : k \in \mathbb{N}, 0 \leq k < p\}.$$

Ya sabemos que este conjunto tiene p elementos y como espacio vectorial sobre $\mathbb{Z}_p$ su dimensión es 1. Por lo tanto $\delta_p(\mathbb{C}^*) = 1$.

ii. El caso S^1 es igual al anterior, pues las raíces de la unidad tienen norma 1, así $\mathbb{C}^*[p] = S^1[p]$.

Demostración (Cont.)

iii. Para $\prod_q \mathbb{Z}(q^\infty)[p]$ notemos primero que para un $q \neq p$ primo, ningún elemento en $\mathbb{Z}(q^\infty)$ va a tener orden p. Así que los elementos $(x_q)_q \in \prod_q \mathbb{Z}(q^\infty)[p]$ son tales que $x_q = 1$ para todo primo $q \neq p$. Entonces sólo debemos mirar qué sucede en el término x_p. Si $x_p^p = 1$, tenemos que x_p es raíz de la unidad y el está en $\mathbb{C}^*[p]$, luego $\delta_p\left(\prod_q \mathbb{Z}(q^\infty)\right) = 1$

iv. Sea $(a/b + \mathbb{Z}, c) \in \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}$ tal que $mcd(a,b) = 1$ y $p(a/b + \mathbb{Z}, r) = (\mathbb{Z}, 0)$. Es decir, $pr = 0$ y $pa/b \in \mathbb{Z}$, lo que implica $r = 0$ y tenemos que $b = p$, luego $(1/p + \mathbb{Z}, 0)$ genera

$$(\mathbb{Q}/\mathbb{Z} \oplus \mathbb{R})[p] = \{(1/p + \mathbb{Z}, 0), (2/p + \mathbb{Z}, 0), \cdots ((p-1)/p + \mathbb{Z}, 0), (0 + \mathbb{Z}, 0)\},$$

que tiene p elementos, de donde $\delta_p(\mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}) = 1$.

v. De forma análoga sucede en $\mathbb{R}/\mathbb{Z}[p]$, sea $r + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}[p]$, luego $pr = 1$, es decir $r = 1/p$ y de nuevo, $\mathbb{R}/\mathbb{Z}[p]$ es un espacio generado por un elemento sobre $\mathbb{Z}_p$. Es decir $\delta_p(\mathbb{R}/\mathbb{Z}) = 1$.

Demostración (Cont.)

Ahora, miremos qué sucede con $\delta_\infty(D)$.

i. Sea $D = \mathbb{Q}/\mathbb{Z} \oplus \mathbb{R}$. Luego $tD = \mathbb{Q}/\mathbb{Z}$ y $D/tD \cong \mathbb{R}$ como espacios sobre $\mathbb{Q}$, es decir

$$\delta_\infty(D) = dim_{\mathbb{Q}}(\mathbb{R}).$$

Veamos que esta dimensión es igual al cardinal del continuo. Sea $\mathcal{B}$ una base de $\mathbb{R}$ sobre $\mathbb{Q}$. Tenemos que $\mathcal{B}$ no es finita pues como π no es algebraico sobre $\mathbb{Q}$ el conjunto $\{\pi^n\}_{n\geq 1}$ es linealmente independiente sobre $\mathbb{Q}$, por lo tanto $|\mathcal{B}| \geq \aleph_0$.
Veamos que $|\mathcal{B}| > \aleph_0$. Si $|\mathcal{B}| = \aleph_0$, existe una enumeración para $\mathcal{B}$, sea esta $\mathcal{B} = \{x_i\}_{j=1}^{\infty}$. Si $A = \bigcup\limits_{r\geq 1} \mathbb{Q}^n$, entonces A es enumerable y para $x \in \mathbb{R}$, existen $m \in \mathbb{N}$, $r_1, \cdots, r_m \in \mathbb{Q}$ y $x_{i_1}, \cdots, x_{i_m} \in \mathcal{B}$ tales que $x = \sum\limits_{j=1}^{m} r_j x_{i_j}$ y así la función $\varphi : A \to \mathbb{R}$ definida por $\varphi(r_1, \cdots, r_n) = \sum\limits_{i=1}^{n} r_i x_i$ es sobreyectiva. Se sigue que $\mathfrak{c} = |\mathbb{R}| \leq |A| = \aleph_0$ lo cual es una contradicción y concluimos que $|\mathcal{B}| > \aleph_0$.
Ahora veamos que $|\mathcal{B}| = \mathfrak{c}$. Tenemos que $\aleph_0 < |\mathcal{B}| \leq |\mathbb{R}| = \mathfrak{c}$ y la hipótesis del continuo implica que $|\mathcal{B}| = \mathfrak{c}$.

Demostración (Cont.)

ii. Sean $D = \mathbb{R}/\mathbb{Z}$, primero calculemos tD. Si $r + \mathbb{Z} \in tD$ existe $n \in \mathbb{N}$ tal que $n(r + \mathbb{Z}) = \mathbb{Z}$ pero esto es lo mismo a decir que $nr \in \mathbb{Z}$, luego $r \in \mathbb{Q}$. Podemos concluir que $tD = \mathbb{Q}/\mathbb{Z}$. Por lo tanto $D/tD \cong \mathbb{R}/\mathbb{Q}$ como espacios vectoriales sobre $\mathbb{Q}$. Es decir $\delta_\infty(D) = dim_{\mathbb{Q}}(\mathbb{R}/\mathbb{Q})$. Como $dim_{\mathbb{Q}}(\mathbb{R}) = \mathfrak{c}$, entonces $\mathbb{R} \cong \bigoplus_{i \in I} \mathbb{Q}$, donde $|I| = \mathfrak{c}$. Luego

$$\mathbb{R} \cong \mathbb{Q} \oplus \bigoplus_{i \in I'} \mathbb{Q},$$

donde $|I'| = \mathfrak{c}$ y $\mathbb{R}/\mathbb{Q} \cong \bigoplus_{i \in I'} \mathbb{Q}$, y se sigue que $\delta_\infty(D) = \mathfrak{c}$.

iii. Sea $D = \mathbb{C}^*$. Definimos una función $f : \mathbb{R} \times \mathbb{R} \to \mathbb{C}$ por $f(a, b) = a + bi$. Luego

$$|\mathbb{C}| = |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}||\mathbb{R}| = \mathfrak{c}\mathfrak{c} = \mathfrak{c}$$

y como $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, entonces $|\mathbb{C}^*| = \mathfrak{c}$. Ahora escribimos $\mathbb{C}^* = V \oplus t\mathbb{C}^*$ donde V es libre de torsión, además $t\mathbb{C}^* = \bigoplus_{p \in \mathbb{P}'} T_p$, con $\mathbb{P}' \subset \mathbb{P}$ y $|T_p| = p$, de donde concluimos que $t\mathbb{C}^*$ es enumerable. Pero como $\mathbb{C}^*$ no es enumerable, el conjunto V no es enumerable. Ahora, $V \cong \bigoplus_{i \in I} \mathbb{Q}$, donde $dim_{\mathbb{Q}}(V) = |I|$. Si I es enumerable V también lo sería, por lo tanto I no es enumerable y como $V \subset \mathbb{C}^*$, entonces $|I| = \mathfrak{c}$, luego $dim_{\mathbb{Q}}(V) = \mathfrak{c}$. Pero como $D/tD \cong V$ como espacios sobre $\mathbb{Q}$, obtenemos que $\delta_\infty(D) = \mathfrak{c}$.

Demostración (Cont.)

iv. Sea $D = S^1$. Sea $f : [0, 2\pi) \to S^1$ definida por $f(\theta) = e^{i\theta}$. Ya sabemos que esta función es biyectiva, por lo tanto $|S^1| = |f[0, 2\pi)| = \mathfrak{c}$. Haciendo el proceso análogo del caso anterior obtenemos que $\delta_\infty(D) = \mathfrak{c}$.

v. Para $D = \prod_q \mathbb{Z}(q^\infty)$ sabemos que $|\mathbb{P}| = \aleph_0$. Veamos que $|\mathbb{Z}(q^\infty)| = \aleph_0$ para todo $q \in \mathbb{P}$.

Recordemos que ${\aleph_0}^{\aleph_0} = \mathfrak{c}$, entonces

$$|\prod_q \mathbb{Z}(q^\infty)| = \prod_q |\mathbb{Z}(q^\infty)| = \prod_q \aleph_0 = {\aleph_0}^{\aleph_0} = \mathfrak{c}.$$

De forma análoga a los casos anteriores, $\delta_\infty(D) = \mathfrak{c}$.

Para cada uno de los grupos obtenemos que $\delta_\infty(D) = \mathfrak{c}$ y $\delta_p(D) = 1$ para todo p primo. Por el teorema anterior se verifica que los grupos son isomorfos dos a dos. $\square$

Referencias

- Fusch, Lasló. *Infinite abelian groups*. Volume 36-1, Academic Press. 1970.
- Guba, V. S. *A finitely generated complete group*. Mathematics of the USSR-Izvestiya. 1986.
- Lam, T.Y. *Lectures on Modules and Rings*. Springer-Verlag. 1999.
- Chapman, E. y Hall, E. *Abstract Algebra with Applications*. Volume I, Springer-Verlag. 1993.
- Lezama, Oswaldo. *Anillos, módulos y categorías*. Universidad Nacional de Colombia, Santafé de Bogotá, 1994.
- Pinter, Charles C. *A book of Set Theory*. Dover Publications Inc., 2014.
- Robinson, Derrick. *A Course in the Theory of Groups*. Second Edition, Springer-Verlag. 1995.
- Roman, Steven. *Advanced Linear Algebra*. Fourth Edition, Springer-Verlag. 2005.
- Rotman, Joseph J. *Advanced Modern Algebra*. Segunda Edición, American Mathematical Society. 2003.
- Rotman, Joseph J. *An Introduction to the Theory of Groups*. Fourth Edition,Springer-Verlag. 1995.