Estructuras algebráicas

1 Generalidades y teorema de Lagrange

1.1 Grupos

Definición 1.1 Un grupo es un conjunto no vacío G en el que se define una operación binaria $G \times G \longrightarrow G$; $(a, b) \mapsto ab$ que cumple (1) **asociatividad** ($(ab)c = a(bc)$), (2) **existencia de elemento neutro** $u \in G$; $ua = a = au$ y (3) **existencia de elemento inverso** $a, x \in G$; $ax = u = xa$. Tanto u como a son únicos. Para la suma $u = 0, a = -x$ y para el producto $u = 1, a = x^{-1}$.

Otras propiedades inmediatas de los grupos son (1) **simplificación**: $ab = ac \iff b = c$; $ba = ca \iff b = c$; (2) **asociatividad generalizada**: $(a_1 \cdots a_k)(a_{k+1} \cdots a_n) = (a_1 \cdots a_l)(a_{l+1} \cdots a_n)$, (3) **inverso de un producto**: $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.

Definición 1.2 Un **grupo simétrico** S_n es el conjunto de biyecciones de un conjunto X con n elementos. Se cumple que $\text{card}(S_n) = n!$. Otros ejemplos de grupos son $GL_n(\mathbb{R})$, el grupo de matrices no singulares para la operación producto; o D_n es el conjunto de biyecciones que conserva la distancia en un polígono de n lados.

Definición 1.3 Un grupo es **abeliano** si $ab = ba \quad \forall a, b \in G$. Todo grupo con dos elementos es abeliano, pues $aa = aa; uu = uu; ua = a = au$; pero para $n \geq 3$, S_n no puede ser abeliano. $GL_n; n \geq 2$, ni $D_n; n \geq 3$ son abelianos.

Proposición 1.4 (1) Si $x^2 = 1 \ \forall x \in G$, entonces G es abeliano; (2) si $(ab)^2 = a^2b^2$ entonces G es abeliano.

Demostración. (1) Para cada x, $x \cdot x = 1 \iff x = x^{-1}$, luego si $a, b \in G$ entonces $a = a^{-1}; b = b^{-1}$x y si $c = ab$ entonces $ab = c = c^{-1} = (ab)^{-1} = b^{-1}a^{-1} = ba$. (2) Dados $a, b \in G$, se tiene que $a(ba)b = (ab)^2 = a^2b^2 = a(ab)b$ y, por simplificación, $ab = ba$.

Definición 1.5 Si G, G' son dos grupos con operaciones $G \times G \longrightarrow G : (a, b) \mapsto ab \quad ; \quad G' \times G' \longrightarrow G' : (a', b') \mapsto a'b'$ el **producto cartesiano** $G'' = G \times G''$ es un grupo con operación $G'' \times G'' \longrightarrow G''$: $((a, a'), (b, b')) = (ab, a'b')$. La asociatividad se mantiene, y se ve que $1_{G''} = (1_G, 1_{G'})$. Además, si G, G' son abelianos, G'' también lo es. Se dice que $G_1 \times \cdots \times G_r$ es el **producto directo**.

1.2 Subgrupos

Definición 1.6 Un subconjunto no vacío $H \subset G$ es un **subgrupo** de G si es un grupo con la misma operación que G. **EN ALGUNOS SITIOS** $H \subset G$ **INDICA QUE** H **ES SUBGRUPO DE** G. Se puede ver que el elemento neutro de H es 1_G, y que si $x \in H; x^{-1} \in H$. Para que (1) H sea subgrupo de G se tiene que cumplir que (2) si $x, y \in H$, entonces $xy^{-1} \in H$.

$\{1_G\}$ y G son subgrupos de G. El resto de subgrupos se llaman **subgrupos propios** de G. Por ejemplo, $m\mathbb{Z} = \{mx \mid x, m \in \mathbb{Z};\}$ es un subgrupo de $\mathbb{Z}$.

Definición 1.8.3 Se denomina a $\langle S \rangle$ al **subgrupo generado** por S.

$\langle S\rangle = \left\{s_1^{h_1}\cdots s_n^{h_n} \mid n\in\mathbb{N}, s_i\in S, h_i\in\mathbb{Z}, 1\le i\le n\right\}$. Esto se puede simplificar como

$\langle S\rangle = \left\{x_1\cdots x_m \mid m\in\mathbb{N}, x_i\in S, 1\le i\le m\right\}$. Es decir, es el conjunto de todos los elementos de S combinados con operación binaria. Si $\mathcal{F}_S$ es la familia de los subgrupos de G que contienen a S, entonces se cumple que $\langle S\rangle = \bigcap_{H\in\mathcal{F}_S} H$.

Un caso particular es cuando $S=\{a\}$. En tal caso es el **subgrupo generado por a**, $\langle a\rangle = \{a^k \mid k\in\mathbb{Z}\}$. Un subconjunto $S\subset G$ se llama **generador de** G si $G=\langle S\rangle$. Es cierto que $\langle G\rangle = G$. Si S es finito, entonces se dice que G es **finitamente generado**.

Definición 1.8.4 Si H es subgrupo de G, se llama **centralizador de** H **en** G a $C_G(H)=\{x\in G \mid ax = xa\ \forall a\in H\}$. El centralizador de G en G, llamado **centro de** G es el caso $Z(G)=\{x\in G\mid xa=ax\ \forall a\in G\}$. Se ve que $C_G(H)$ es un subgrupo de G.

Definición 1.8.5 Si $S\subset G$ y $a\in G$, se llama **conjugado de** S **por** a al conjunto $S^a=\{a^{-1}xa \mid x\in S\}$

Definición 1.8.6 Si $S\subset G$, se llama **normalizador de** S **en** G al conjunto $N_G(S)=\{a\in G\mid S^a=S\}$. El normalizador de S es un subgrupo de G porque si $a,b\in N_G(S)$, entonces $S^{ab^{-1}}=(S^a)^{b^{-1}}=S^{b^{-1}}=(S^b)^{b^{-1}}=S^{bb^{-1}}=S$

Definición 1.8.8 Dados dos subgrupos K,H de G, se define $HK=\{hk\mid h\in H, k\in K\}$. Para que HK sea un subgrupo de G entonces $HK=KH$. Si $H\subset K, HK=K=KH$.

1.3 Orden de un grupo

Definición 1.9 El **orden** de un subgrupo finito $H\subset G$ es el número de elementos que tiene. Se denota por $o(H)$. Un elemento $a\in G$ es **de torsión** si $\langle a\rangle$ es finito. En tal caso el orden es $o(a)$.

Proposición 1.10 Sea G un grupo y $a\in G$ de torsión. Entonces se cumple que

- Existe $k\ge 1$ tal que $a^k=1$
- $o(a)$ es el menor número tal que $a^n=1$
- Si $n=o(a)$, $\langle a\rangle=\{1,a,\cdots,a^{n-1}\}$
- $a^k=1$ sii k es múltiplo de n
- $o(a^{-1})=o(a)$
- Si $x=a^k$ y $n=o(a)$, entonces $o(x)=\frac{n}{mcd(n,k)}$
- Si $b\in G$ es de torsion y $ab=ba$ entonces $o(ab)$ es divisor de $mcm(o(a),o(b))$. Si $o(a),o(b)$ son primos entre si, $o(ab)=o(a)o(b)$
- $o(ab)=o(ba)$

1.4 Índice de un subgrupo

Definición 1.2/**Observación 1.12.6/7** Sea G un grupo y $H\subset G$. Sean R^H, R_H las relaciones de equivalencia en G:

$$xR_Hy \iff xy^{-1}\in H$$
$$xR^Hy \iff x^{-1}y\in H$$

Además, se definen $Hx = \{hx \mid h \in H\}; xH = \{xh \mid h \in H\}$. Se cumple que si $x, y \in G$, y yR_Hx entonces $yx^{-1} = h \in H$ y, por tanto, $y = hx \in Hx$.

Además, las aplicaciones $H \to Hx : h \mapsto hx$ y su equivalente en xH son biyectivas. Es importante que pese a existir una biyeccíón entre Hx y xH, **no siempre Hx y xH son iguales**.

Proposición 1.12.3 La aplicación entre conjuntos cocientes $G/R_H \to G/R^H : Hx \to x^{-1}H$ es biyectiva.

Definición 1.12.4 $H \subset G$ es un subgrupo de **índice infinito** si G/R_H es un conjunto infinito. Por otra parte, el índice de H en G, $[G : H]$ es el número de elementos de G/R_H.

Proposición 1.12.8 (T de Lagrange) Sea $H \subset G$ un subgrupo. Se cumple que si G es finito, entonces $o(H)$ es finito, H tiene índice finito en G y $o(G) = o(H) \cdot [G : H]$.

Corolario 1.12.9 Si H, K son subgrupos finitos de G, $o(H) = m$, $o(K) = n$, entonces $o(H \cap K) = 1 \iff H \cap K = \{1_G\}$

Proposición 1.12.10 (F de transitividad del índice) Sean H, K subgrupos de G. Si H es subgrupo de K, y los indices entre subgrupos, y con G, son finitos, entonces se cumple $[G : H] = [G : H][H : K]$

Proposición 1.12.11 Sean H, K subgrupos de G, finito. Entonces

$$card(HK) = \frac{o(H)o(K)}{o(H \cap K)}$$

Definición 1.15 / **Observación 1.15.4** Un grupo G se llama **cíclico** si existe $a \in G$ tal que $G = \langle a \rangle$. Si $o(a) = p$, primo, el grupo es cíclico.

Proposición 1.16 / 1.17 Sea G cíclico y $n = o(G)$, para cada divisor m de n existe un único subgrupo de G de orden m, y ese subgrupo es cíclico. Además, todo subgrupo de un grupo cíclico [finito o no] es cíclico.

Definición 1.18 Sea G finitamente generado. Un sistema generador S se llama **minimal** si cualquier subconjunto de G con menos elemenos que S no es generador de G.

Proposición 1.19 Sea G finito de orden n y $S = \{x_1, \cdots, x_p\}$ un sistema generador minimal de G. Entonces $2^p \leq n$.

Demostración. Llamamos $S_i = \{x_1, \cdots, x_i\}$, $1 \leq i \leq p$; y $H_i = \langle S_i \rangle$. Evidentemente, $H_i \subset H_{i+1}$. Por ele teorema de Lagrange y la fórmula de la transitividad del índice,

$$[G : H_1] = [H_P : H_1] = [H_P : H_{P-1}][H_{P-1} : H_{P-2}] \cdots [H_2 : H_1]$$

Además,

$$[H_{i+1} : H_i] = \frac{o(H_{i+1})}{o(H_i)} > 1 \iff [H_{i+1} : H_i] \geq 2$$

pues los índices son enteros. Por tanto, $[G : H_1] \geq 2^{p-1}$, y como $o(H_1) \geq 2$, entonces, $o(G) = o(H_1)[G : H_1] \geq 2^p$

Page intentionally left in blank

2 Subgrupos normales, homomorfismos, teorema de estructura de grupos abelianos finitos

Proposición 2.1 Sea G un grupo y H un subgrupo. H es un subgrupo **normal** (**LO DEFINO AQUÍ COMO** $\subset_N$) si se cumplen las condiciones equivalentes:

1. Para todo $a \in G$, $aH = Ha$
2. Para todo $a \in G$, $H = H^a$
3. Para todo $a, b \in G$, $ab \in H \iff ba \in H$, luego H es abeliano.

Demostración. $1 \implies 2$. Si $y \in H^a$ entonces $aya^{-1} = h \in H$. Como $ay = ha \in Ha = aH$ existe $h' \in H$ tal que $ay = ah'$. Así, $y \in H^a = h' \in H \iff H^a \subset H$. Si aplicamos lo mismo con xa^{-1} tenemos $H^{a^{-1}} \subset H$ y, con ello $H \subset H^a$, luego $H = H^a$. $2 \implies 3$. Como $ab \in H$, $ba = a^{-1}aba \in H^a$, y como $ba \in H$, $H = H^a$. $3 \implies 1$. Sea $x \in Ha$, luego $\exists h \in H, x = ha$, y $xa^{-1} = h \in H$. Por hipótesis $h' = a^{-1}x \in H$ y $x = ah' \in aH$, luego $Ha \subset aH$. Si empezamos con $x \in aH$ obtenemos que $aH \subset Ha$, luego $aH = Ha$.

Observación 2.2.1 Si H es normal, entonces $R^H = R_H$, y G/R_H se escribe G/H.

Observación 2.2.4/2.2.5 Si H es un subgrupo de G, y $[G : H] = 2$, H es subgrupo normal de G. Asimismo, los subgrupos $\{1_G\}, G$ son normales.

Definición 2.2.14 Un grupo G es **simple** si los únicos subgrupos son $\{1_G\}, G$. Si $o(G)$ es primo p, por el teorema de Lagrange, los únicos subgrupos son $\{1_G\}, G$, luego G es simple.

Proposición 2.2.8 Todo subgrupo $H \subset Z(G) = \{a \in G \mid ag = ga \ \forall g \in H\}$ es subgrupo normal de G.

Proposición 2.2.10 Sea H subgrupo de G.

1. H es subgrupo de $N_G(H) = \{a \in G \mid H = H^a\}$.
2. $H \subset_N N_G(H)$.
3. Si $H \subset K \subset G$ y $H \subset_N K$, entonces $K \subset N_G(H)$.

Definición 2.2.11 Si H, K son subgrupos de G, K es un **subgrupo conjugado** de H si existe $a \in G$ tal que $K = H^a$. Como la relación es recíproca, se dice que K y H son conjugados.

Proposición 2.2.11

- Si Σ es la familia de conjugados de H y $N = N_G(H)$, la aplicación $\phi : G/R_N \to \Sigma : Na \to H^a$ es biyectiva.
- Si N tiene índice finito en G, el número de conjugados con H es $[G : N]$.

Proposición 2.2.13 Si $A \subset_N G$, $H \subset K \subset G$, y $H \subset_N K$, entonces $AH \subset_N AK$.

La normalidad no es transitiva, es decir, si $H \subset_N K \subset_N G$, no siempre es cierto que $H \subset_N G$.

Definición 2.2.16/**Observación 2.2.16.1** Si $H \subset G$, se llama corazón de H a

$$\heartsuit(H) = K(H) = \bigcap_{a \in G} H^a$$

Si $N \subset_N H$ entonces $N \subset K(H)$, pues para cada $a \in G$: $N = N^a \subset H^a$, luego $N = N^a \subset \cap_{a \in G} H^a = K(H)$

Proposición 2.2.17 (T de Poincaré) Si G posee un subgrupo de índice finito, también posee un subgrupo normal de índice finito.

2.1 Grupos cocientes

Proposición 2.3 El grupo cociente G/H de $H \subset_N G$ tiene estructura de grupo con la operación:

$$\begin{aligned} G/H \times G/H &\longrightarrow G/H \\ (aH, bH) &\longmapsto abH \end{aligned}$$

El elemento neutro del grupo cociente es H, y el inverso de aH es $(aH)^{-1} = a^{-1}H$.

Observación 2.3.1 Si $H \subset_N K \subset G$ (entonces $H \subset_N G$), el grupo cociente $K/H \subset G/H$, ya que si $aH, bH \in K/H, a, b \in K$, entonces $(aH)(bH)^{-1} = (aH)(b^{-1}H) = ab^{-1}H \in K/H$, ya que como $K \subset G, ab^{-1} \in K$

Observación 2.3.1.1 $K \subset_N G \iff K/H \subset_N G/H$

Ejemplo 2.3.3 (Función ϕ de Euler) Si denotamos $\mathbb{Z}_m^* = \{a + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z} \mid mcd(a, m) = 1\}$ y consideramos la operación binaria

$$\mathbb{Z}_m^* \times \mathbb{Z}_m^* \to \mathbb{Z}_m^* : (a + m\mathbb{Z}, b + m\mathbb{Z}) \mapsto ab + m\mathbb{Z}$$

vemos que $\mathbb{Z}_m^*$ forma un grupo abeliano con elemento neutro $1 + m\mathbb{Z}$ y elemento inverso $u + m\mathbb{Z}$, con $au = 1$.

Entonces, la función $\phi : \mathbb{N}\{0\} \to \mathbb{N}\{0\}$ que a cada m positivo le corresponde el orden de $\mathbb{Z}_m^*$ es la función de Euler. Para p primo, $\phi(p) = p - 1$, y $\phi(p^k) = p^{k-1}(p-1)$. Si tenemos m, n tal que $mcd(m, n) = 1$, entonces $\phi(mn) = \phi(m)\phi(n)$. Con todo esto, si tenemos un numero $a = p_1^{k_1} \cdots p_i^{k_i}$, entonces $\phi(a) = p_1^{k_1-1} \cdots p_i^{k_i-1}(p_1 - 1) \cdots (p_i - 1)$

2.2 Homomorfismos

Definición 2.4 / 2.6 Una aplicación $f : G \to G'$ es un **homomorfismo de grupos** si $f(ab) = f(a)f(b) \forall a, b \in G$. Para todo homomorfismo se tiene que $f(1_G) = 1_{G'}$ y $f(a^{-1}) = (f(a))^{-1}$. Si un homomorfismo es biyectivo se llama **isomorfismo**. Se denota por $G \simeq G'$ cuando dos grupos son isomorfos.

Definición 2.4.3/**Proposición 2.4.4** El **núcleo** de un homomorfismo es $ker(f) = \{a \in G \mid f(a) = 1_{G'}\}$. f es inyectiva sii $ker(f) = \{1_G\}$.

Definición 2.4.5 Se llama **imagen** de f a $im(f) = \{f(x) \mid x \in G\}$.

Proposición 2.4.6 Si $f : G \to G'$ es homomorfismo y $H' \subset G'$, entonces $f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ es un subgrupo de G. Además, si $H' \subset_N G'$ entonces $f^{-1}(H') \subset_N G$.

Observación 2.4.7/2.4.8 Si $H \subset G$, la inclusión $j : H \to G : x \mapsto x$ es un homomorfismo inyectivo; y si $H \subset_N G$, la proyección $\pi : G \to G/H : x \mapsto xH$ es un homomorfismo sobreyectivo.

Proposición 2.4.9 Si $f : G \to G'$ y $g : G' \to G''$ son homomorfismos, $g \circ f : G \to G''$ también lo es, pues $(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$

Proposición 2.4.10 Si f es un homomorfismo y $x \in G$ tiene orden m, se cumple que (i) $o(f(x))$ divide a m (ii) Si f es inyectiva, $o(f(x)) = m$.

● **Proposición 2.5 (Factorización canónica de un homomorfismo)**

Sea $f : G \to G$ un homomorfismo. Entonces existe un homomorfismo biyectivo $b : G/ker(f) \to im(f)$ que hace conmutativo el diagrama

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & G' \\ G/ker(f) \arrow[r, "b"'] & im(f) \arrow[u, "j"'] \end{tikzcd}$$

Demostración. $f(x) = j((b \circ pi)(x)) = b(\pi(x)) = b(x\, ker(f))$. Comprobamos que se cumple el enunciado. (1) b está bien definida porque si $x\, ker(f) = y\, ker(f)$ entonces $x^{-1}y \in ker(f)$, $f(x)^{-1}f(y) = 1_{G'} \iff f(y) = f(x)$, luego $b(x\, ker(f)) = b(y\, ker(f))$. (2) b es homomorfismo, ya que $b((x\, ker(f))(y\, ker(f)) = b(xy\, ker(f) = f(xy) = f(x)f(y) = b(x\, ker(f))b(y\, ker(f))$. (3) b es inyectivo, ya que si $x\, ker(f) \in ker(b)$ entonces $f(x) = b(x\, ker(f)) = 1_{im(f)} = 1_{G'}$, y $xinker(f)$. (4) b es sobreyectiva ya que para cada elemento de $im(f)$ existe un elemento de la forma $b(x\, ker(f)$.

Proposición 2.6.X (Propiedades de isomorfismos) Si $G \simeq G'$, y G es abeliano o cíclico, entonces G' también lo es. Si X, Y son conjuntos con el mismo número de elementos, entonces $Biy(X) \simeq Biy(Y)$.

● **Corolario 2.7 (Primer teorema de la isomorfía)** Si $f : G \to G'$ es un homomorfismo, $G/ker(f) \simeq im(f)$.

Corolario 2.8 Todo grupo cíclico es isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}/m\mathbb{Z}$. Demostración. Sea $G = \langle a \rangle$ cíclico. Consideramos $f : \mathbb{Z} \to G : k \to f(k) = a^k$. Como $f(x + y) = a^{x+y} = a^x a^y = f(x)f(y)$, f es homomorfismo. Cada elemento $b \in G$ es de la forma a^k, luego f es sobreyectiva, es decir, $im(f) = G$. Por el primer tma de isomorfía tenemos que $\mathbb{Z}/ker(f) \simeq im(f)$, luego $\mathbb{Z}/ker(f) \simeq G$, y como $ker(f)$ es subgrupo de $\mathbb{Z}$, existe m tal que $ker(f) = m\mathbb{Z}$. Si $m = 0$, $ker(f) = 0\mathbb{Z} = \{0\}$, y $\mathbb{Z} \simeq G$. Si $m > 0$, $\mathbb{Z}/m\mathbb{Z} \simeq G$.

Ejemplo 2.9.4.4 Si n es múltiplo de m, existen homomorfismos inyectivos y el número de homomorfismos es $\phi(m)$. Si $mcd(m, n) = n$, existen isomorfismos sobreyectivos y el número es $\phi(n)$.

Ejemplo 2.9.6 Sea $n \geq 2$ y $X = \{1, 2, \cdots, n\}$ y $f_n \in S_n = Biy(X)$. Se llama **signatura de f**, $s(f)$ al número de pares $(i, j) \in X \times X$ tales que $i < j \quad f(i) > (j)$. La aplicación $\epsilon : S_n \to U_2 = \{-1, 1\} \quad f \mapsto \epsilon(f) = (-1)^{s(f)}$ es homomorfismo. Esta fórmula puede ser calculada también así: $\epsilon(f) = \prod_{i<j} \frac{f(i)-f(j)}{i-j}$ Se denomina **grupo alternado**, A_n al núcleo de ϵ: $A_n = \{f \in S_n \mid \epsilon(f) = 1\}$

Proposición 2.10 Si G es un grupo con $o(G) < 12$, para cada dividor d de n existe un subgrupo $G, o(G) = d$. Sin embargo, si $o(G) \geq 12$, no siempre se cumple esto (A_4 tiene $o(A_4) = 12$, pero no tiene subgrupos de orden 6. Esto verifica que el **recíproco del teorema de Lagrange no es cierto siempre**.

2.3 Teoremas de isomorfía

Proposición 2.15 (Segundo teorema de isomorfía) Sean $N, H \subset_N G$, y $N \subset H$. Entonces $H/N \subset_N G/N$ y $(G/N)/(H/N) \simeq G/H$

Proposición 2.16 (Tercer teorema de isomorfía Si $H, N \subset G$, y $N \subset_N G$,

1. $H \cap N \subset_N H$
2. $HN \subset G$
3. $N \subset_N HN$
4. $HN/N \simeq H/(H \cap N)$

Lema 2.17 Sean $A, B, C \subset G$, y $B \subset A$. Entonces $A \cap BC = B(A \cap C)$

Proposición 2.18 (Cuarto teorema de isomorfía). Sea $H_1, H_2 \subset G$, $N_i \subset_N H_i$. Entonces

- $N_1(H_1 \cap H_2) \subset H_1$ y $N_2(H_1 \cap H_2) \subset H_2$
- $N_1(H_1 \cap N_2) \subset_N N_1(H_1 \cap H_2)$ y $N_2(N_1 \cap H_2) \subset_N N_2(H_1 \cap H_2)$
- $(H_1 \cap N_2)(N_1 \cap H_2) \subset_N H_1 \cap H_2$
- $(N_1(H_1 \cap H_2))/(N_1(H_1 \cap N_2)) \simeq (H_1 \cap H_2)/(H_1 \cap N_2)\ (N_1 \cap H_2) \simeq (N_2(H_1 \cap H_2))/(N_2(N_1 \cap H_2)$

2.4 Estructura de grupos abelianos finitos

Lema 2.20 Sea G grupo abeliano finito y $x \in G$ un elemento de orden máximo. Entonces, para cada $y \in G$, el orden de y divide al de x.

Lema 2.20.2 Sea G abeliano finito y $x \in G$ de orden máximo. Sean $H = \langle x \rangle$ e $y \in G$, entonces existe $z \in Hy$ tal que $o(z) = o(Hy)$

Lema 2.20.3 Sean $H, K \subset_N G$ tales que $H \cap K = \{1\}$. Entonces $HK \simeq H \times K$.

Proposición 2.2.1 (Teorema de estructura de grupos abelianos finitos) Si G es abeliano finito, existen $m_1, \cdots, m_r$, denominados **coeficientes de torsión de G**, tales que

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$$

y cada m_i divide a m_{i-1}. Además, los coeficientes son únicos.

Proposición 2.22 Sean G_1, G_2 grupos cíclicos de órdenes m y n, y $G = G_1 \times G_2$, entonces las afirmaciones (1) G es cíclico, (2) $mcd(m, n) = 1$ son equivalentes.

Observación 2.22.3 Si $p_1 < \cdots < p_s$ son primos, todo grupo abeliano de orden $n = p_1 \cdots p_s$ es cíclico.

Proposición 2.23 Si p es primo, $\mathbb{Z}_p^*$ es cíclico.

3 Grupos abelianos finitamente generados. Generadores relacionales

3.1 Teorema de la Estructura

Definición 7.1 Si G es un grupo, denotamos $T(G) = \{x \in G \mid o(x) \text{ es finito}\}$. G tiene **torsión** si $T(G) \neq \{1\}$.

1. Si G es abeliano, $T(G) \subset G$ ya que $o(1) = 1$, y si $x, y \in T(G)$, $o(xy^{-1}) | mcm(o(x), o(y))$, luego $o(xy) = o(xy^{-1})$ es finito y $xy^{-1} \in T(G)$.
2. El cociente $G/T(G)$ no tiene torsión.
3. Si G no es abeliano, $T(G)$ no tiene por qué ser subgrupo de G.
4. El grupo $G = \mathbb{Z} \times \cdots \times \mathbb{Z}$ no tiene torsión
5. Si G es finito, $G = T(G)$ ya que $\forall x \in G, x^{O(G)} = 1$.
6. Si G es infinito, puede ser que $G = T(G)$.
7. Si G es abeliano y $K \subset G$, $T(K) = K \cap T(G)$. Si K no tiene torsión, $K \cap T(G) = \{1\}$, y si G no tiene torsión, K tampoco la tiene.
8. Si $K = T(G)$, $T(T(G)) = T(K) = K \cap T(G) = T(G)$

Ejemplo 7.2 / 7.3 Si $G = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$, entonces $T(G) = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \times \{0\} \times \cdots \times \{0\}$ y $G/T(G) = \mathbb{Z} \times \cdots \times \mathbb{Z}$

Lema 7.5/7.6 Sea $\{x_1, \cdots, x_k\}$ un sistema generador minimal de G. Si existen enteros no nulos $m_1, \cdots, m_k$, tales que $\prod x_i^{m_i} = 1$, entonces G tiene torsión. Sea G abeliano, sin torsión y finitamente generado. Si n es el mínimo número de generadores de G, existen subgrupos de G cíclicos $H_1, \cdots, H_n \simeq \mathbb{Z}$ tales que $G = H_1 \cdots H_n \simeq H_1 \times \cdots \times H_n$

Proposición 7.7 (Teorema de estructura de grupos abelianos finitamente generados) Sea G abeliano finitamente generado. Existen enteros no negativos n, r, y si $n \neq 0$, enteros positivos $m_1, \cdots, m_n$, todos únicos, tales que

1. $G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \times \mathbb{Z} \times \cdots_r \times \mathbb{Z}$
2. m_i divide a m_{i-1} para cada $2 \leq i \leq n$.
3. $T(G) \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n$ y $r = \beta(G) =$ número de Betti de G.
4. $G \simeq T(G) \times G/T(G)$.

Ejemplo 7.8 Si G no es finítamente generado, puede ser que $G \not\simeq T(G) \times G/T(G)$. P. ej. en el grupo $G = \prod_{n \in \mathbb{N}} \mathbb{Z}/p_n\mathbb{Z}$, si $T(G) = \{a \in G \mid \text{sop}(a) \text{ es finito}\}$, $\text{sop}(a) = \{n \in \mathbb{N} \mid a_n + p_n\mathbb{Z} \neq 0 + p_n\mathbb{Z}\}$ falla en cumplir la isomorfía.

3.2 Generadores y relaciones

Proposición 7.10 Sea G abeliano y finitamente generado, con $S = \{x_1, \cdots, x_n\}$ un sistema de generadores. Sea f_S el homomorfismo $f_S : \mathbb{Z} \times \cdots_n \times \mathbb{Z} = \mathbb{Z}^n \to G : (m_1, \cdots, m_n) \mapsto m_1x_1 + \cdots + m_nx_n$ y sea $R(S) = ker(f_s)$. Vemos que $ker(f_S)$ es el conjunto que hace que $m_1x_1 + \cdots + m_nx_n = 0$. $R(S)$ se denomina el **subgrupo de relaciones de** G. Definimos $R = \{r_1, \cdots, r_l\}$ como el sistema generador de $R(S)$. El par (R, S) se denomina **presentación de** G **mediante generadores y relaciones**.

Se demuestra que $R(S) \simeq \mathbb{Z}^k, k \leq n$, y $\beta(G) = n - k$.

Proposición 7.13 Sea G un grupo abeliano finitamente generado por $S = \{x_1, \cdots, x_n\}$. Entonces se cumple que $S = \{x_1, \cdots, -x_i, \cdots, x_n\}$ también es sistema generador, y si $\lambda_2, \cdots, \lambda_n$ son enteros, y $y_1 = x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$, entonces $S = \{y_1, x_2, \cdots, x_n\}$ también es un sistema generador.

Proposición 7.14 Sea (S, R) una presentación de G, entonces se pueden obtener los coeficientes de torsión y el coeficiente de Betti mediante el siguiente algoritmo.

PASO 1 Dados $S = \{x_1, \cdots, x_n\}$ y $R = \{r_1, \cdots, r_k\}$, escribimos la matriz M(S,R)

$$M(S,R) = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kn} \end{bmatrix}$$

Permutamos filas y columnas para que a_{11} sea el elemento con menor valor absoluto ($a_{11} \neq 0$. Ahora dividimos $a_{1j} = \lambda_1 a_{11} + b_{1j}$, con $0 \leq b_{ij} < a_{11}$.

Entonces, $a_{11}x_1 + \cdots + a_{1n}x_n = a_{11}x_1 + (\lambda_2 a_{11} + b_{12})x_2 + \cdots + (\lambda_n a_{11} + b_{1n})x_n = a_{11}[x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n] + b_{12}x_2 + \cdots + b_{1n}x_n = a_{11}[y_1] + b_{12}x_2 + \cdots + b_{1n}x_n = 0$, y $S = [y_1, x_2, \cdots, x_n]$ es un sistema generador, con $r_1^* = (a_{11}, b_{12}, \cdots, b_{1n}$. Repetir con todas las filas (r_i), aplicando los λ obtenidos en la fila 1; y ordenar la primera fila posicionando b_{1l}, el elemento más pequeño de la fila, en primer lugar.

Si b_{1l} no divide a todos los $a_{11}, b_{12}, \cdots, b_{1n}$, repetimos el paso hasta que pase. Entonces, renombramos la matriz

$$\begin{bmatrix} b_{1l} & b_{12} & \cdots & a_{11} & \cdots & b_{1n} \\ \vdots & \vdots & & \vdots & & \vdots \\ b_{kl} & b_{k2} & \cdots & a_{k1} & \cdots & b_{kn} \end{bmatrix} \to \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kn} \end{bmatrix}$$

PASO 2 Dividimos $a_{i1} = a_{11}q_i + c_{i1}$. Si $c_{i1} = 0$ para todas las filas, ya hemos terminado. En caso contrario, el sistema $R^* = \{r_1, r_2 - q_2 r_1, \cdots, r_k - q_k r_1\}$ es generador de $R(S)$. Se repite el paso, poniendo a c_{l1} como primer elemento de la matriz, hasta converger (lo mismo que el PASO 1, pero en filas). Así, obtenemos la matriz

$$M = \begin{bmatrix} a_{11} & 0 & & 0 \\ 0 & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & & \cdots \\ 0 & b_{k2} & \cdots & b_{kn} \end{bmatrix}$$

PASO 3 Si a_{11} no divide a algún b_{ij}, hacemos $r_1 = r_1 + r_i$ y repetimos el paso 1 hasta que todos los elementos b sean divisibles por a_{11}.

PASO 4/5 Sometemos a la submatriz de elementos b el mismo procedimiento que a la inicial, y llegamos a una presentación. Repitiendo, obtenemos la matrix de la derecha

$$M(S_1,R_1) = \begin{bmatrix} a_{22} & 0 & & 0 \\ 0 & c_{33} & \cdots & c_{3n} \\ \cdots & \cdots & & \cdots \\ 0 & c_{k3} & \cdots & c_{kn} \end{bmatrix} \to M(S,R) = \begin{bmatrix} a_{11} & 0 & & 0 \\ 0 & b_{22} & \cdots & 0 \\ \cdots & \cdots & & \\ 0 & 0 & & C \end{bmatrix} \to M(\hat{S},\hat{R}) = \begin{bmatrix} a_{11} & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & a_k k & 0 & \cdots & 0 \end{bmatrix}$$

Si tomamos $m_1 = a_{kk}, \cdots, m_{k-1} = a_{22}, m_k = a_{11}$, los coeficientes de torsión de G, entonces tenemos que $G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^{n-k}$, y $\beta(G) = n - k$.