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 $G \times G \to G \ ; \ (a,b) \mapsto ab$ 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 $ab = ba \ \ \forall a, b \in G$. 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 $G \times G \to G : (a,b) \mapsto ab \quad ; \quad G' \times G' \to G' : (a',b') \mapsto a'b'$ el **producto cartesiano** $G'' = G \times G''$ es un grupo con operación $G'' \times G'' \to G'' : ((a,a'),(b,b')) = (ab, a'b')$. La asociatividad se mantiene, y se ve que $1_{G''} = (1_G, 1_{G'})$. Además, si G, G' son abelianos, G'' también lo es.

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. 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.

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

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

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 $\langle G\rangle = G$.

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 $k\geq 1$ 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