MATE6201-0U1
Prof. Luis A. Medina
10.00 - 11.20
CNL-A-207

Algebra Moderna

Alec Zabel-Mena

Universidad de Puerto Rico, Recinto de Rio Piedras

17.08.2022

Lectura 1: Grupos y Subgrupos

Definición. Sea G un conjunto no vacio junto a una operación binaria $\cdot$. Decimos que el par $(G, \cdot)$ es un **grupo** si:

(1) $a \cdot b \in G$ para $a, b \in G$.

(2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para $a, b, c \in G$

(3) Existe un $e \in G$ tal que $a \cdot e = e \cdot a = a$ para toda $a \in G$.

(4) Para toda $a \in G$, existe una $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Si $a \cdot b = b \cdot a$ para toda $a, b \in G$, entoces decimos que G es un grupo **Abeliano**.

Ejemplo 1. (1) Los naturales $\mathbb{N}$ junto a la multiplicación es satisface los primeros tres axiomas, pero no es un grupo.

(2) El grupo mas pequeño es el conjunto $\{e\}$, que denotamos como $\langle e \rangle$. $\langle e \rangle$ es un grupo Abeliano.

(3) Los enteros $\mathbb{Z}$ junto con adición $+$ forma un grupo Abeliano.

(4) El conjunto $GL(n, \mathbb{R})$ de matrices $n \times n$ con entradas reales, nosingular forman un grupo con respecto a multiplicación de matrices. $GL(n, \mathbb{R})$ no es un grupo Abeliano.

(5) Sea S cualquier conjunto y $A(S)$ el conjunto de todas las permutaciones de de elementos de S. Entonces $A(S)$ es un grupo no Abeliano con respecto a composicion de funciónes, $\circ$. Si S tiene n elementos, entonces $A(S) = S_n$.

Definición. Sea G un grupo. El **orden** de un grupo es su cardinalidad, y escribimos $\operatorname{ord} G = |G|$. Decimos que G es **finito** si $\operatorname{ord} G$ es finito; de lo contrario, G es **infinito**.

Definición. Sea G un grupo, y $a \in G$. El **orden** de a, denotado $\operatorname{ord} a$, es el menor entero positivo n tal que $a^n = e$ y escribimos $\operatorname{ord} a - n$. Si tal n no existe, entonces decimos que a es de orden **infinita**, y decimos que a es un elemento **torsión**.

Ejemplo 2. (1) Considera $\mathbb{C}^* = \mathbb{C} \backslash 0$, entonces $\mathbb{C}^*$ tiene orden infinita, note que si $\exp(\frac{2i\pi}{5}) \in \mathbb{C}^*$, entonces $\alpha \neq 1$, para $j \neq 1, 2, 3, 4$, pero $\alpha^5 = 1$. Entonces $\operatorname{ord} \alpha = 5$.

(2) Considere $A \in GL(6, \mathbb{R})$ con la forma

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Entonces

$$A^3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

entonces, $A^3 = I$.

(3) En $\mathbb{R}^* = \mathbb{R} \backslash 0$, $\mathbb{R}^*$ es infinito, y $\operatorname{ord} 2$ es infinito.

Definición. Sea G un grupo y $H \subseteq G$ no vacio. Entonces decimos que H es un **subgrupo** de G si H es un grupo bajo la misma opearación de G. Escribimos $H \leq G$.

Ejemplo 3. (1) Considere $GL(n, \mathbb{R})$ y sea $SL(n, \mathbb{R})$ los elementos $A \in GL(n, \mathbb{R})$ tales que $\det A = 1$. Entonces $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$.

(2) Sea $C(\mathbb{R})$ el conjunto de todas las funciones continuas sobre $\mathbb{R}$. Entonces $C(\mathbb{R})$ es un grupo bajo la suma de funciónes $+$. Sea $C^1(\mathbb{R})$ el conjunto primer difirenciable continua de funciones sobre $\mathbb{R}$. Observe lo siguiente:

(a) $(f + g)' = f' + g'$

(b) $f' + (g + h)' = (f + g)' + h'$.

(c) $c' = 0$, entonces $0 \in C^1(\mathbb{R})$

(d) $f' - f' = -f' + f' = 0$.

Como todos los funciones de arriba tambien son continuas, vemos que $C^1(\mathbb{R}) \leq C(\mathbb{R})$.

Lema 1. *Sea G un grupo y $H \subseteq G$ no vacio. Si tenemos que $ab \in H$, implicat que $ab^{-1} \in H$, entonces $H \leq G$.*

Proof. Como $H \neq \emptyset$, sea $a \in H$. Entonces $aa^{-1} = e \in H$. Luego, tambien tenemos qie $ea^{-1} = a^{-1} \in H$. Finalmente, tenemos que si $b \in H$, entonces $ab^{-1} \in H$, por lo tanto $b^{-1} \in H$, entonces $a(b^{-1})^{-1} = ab \in H$. ■

Ejemplo 4. (1) Considere a los enteros pares $2\mathbb{Z}$. Sean $2n, 2m \in 2\mathbb{Z}$. Noten que $2n-2m = 2(n-m) \in 2\mathbb{Z}$. Entonces $2\mathbb{Z} \leq \mathbb{Z}$.

(2) Si G es un grupo, entonces $\langle e \rangle$ y G son subgrupos de G. Llamamos a $\langle e \rangle$ el grupo **trivial**.

(3) Si G es un grupo, y $a \in G$, entonces el conjunto $\langle a \rangle = \{a^j : j \in \mathbb{Z}\}$ es un subgrupo de G, llamado el **subgrupo generado por** a.

(4) Si G es un grupo, y $a \in G$, entonces $C(a) = \{g \in G : ag = ga\}$ y $Z(G) = \{g \in G : ag = ga \text{ para toda } a \in G\}$ son subgrupos. Nota que $Z(G) = \bigcap C(a)$. Llamamos a $C(a)$ el **cnetralizador** de a y $Z(G)$ el **centro** de G.

(5) Sea G un grupo y $H \leq G$, y sea $a \in G$, entonces $a^{-1}Ha \leq G$. Llamamos a $a^{-1}Ha$ el **conjugado** de H **con respecto** a a.

Definición. Suponga que G y H son grupos. Un mapa $\phi : G \to H$ se llama un **homomorphismo** si para toda $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$. Si ϕ es $1-1$ y sobre, entonces lo llamamos un **isomorphismo**. Si ϕ es un isomorphismo, y $G = H$, entonces llamamos a ϕ un **automorphismo**.