# 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

22.08.2022

## Lectura 1: Grupos y Subgrupos

**Definición.** Sea $G$ un conjunto no vacío 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 se satisface los primeros tres axiomas, pero no es un grupo. De hecho, $\mathbb{N}$ forma un estructura llamado un "monoide".

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

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

(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 funciónes 1–1 y sobre llevando elementos de $S$ a elementos de $S$. Entonces $A(S)$ es un grupo no Abeliano con respecto a composición de funciónes, $\circ$. Si $S$ tiene $n$ elementos, entonces exscribimos $A(S) = S_n$. $A(S)$ también no se Abeliano ya que para funciónes cualquieras $f, g$, $f \circ g \neq g \circ f$.

**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 $\alpha = \exp(\frac{2i\pi}{5}) \in \mathbb{C}^*$, 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 vacío. 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 de funciónes primer diferenciables continuas sobre $\mathbb{R}$ Es decir, que $f'$ existe y es continua. 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) $f' - f' = -f' + f' = 0$.

Suponiendo que $f', g', h' \in C^1(\mathbb{R})$, son continuas, entonces vemos que los funciones de arriba tambien son continuas. Entonces $C'(\mathbb{R}) \leq C(\mathbb{R})$.

**Lema 1.** *Sea $G$ un grupo y $H \subseteq G$ no vacío. 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 $\phi$ es $1-1$ y sobre, entonces lo llamamos un **isomorphismo**. Si $\phi$ es un isomorphismo, y $G = H$, entonces llamamos a $\phi$ un **automorphismo**.

## Lectura 2: Grupos y Subgrupos

**Ejemplo 5.** (1) Considera $\mathbb{R}$ bajo la suma $+$ y $\mathbb{R}^+$ bajo la multiplicacón, $\cdot$. Sea $\phi : \mathbb{R} \to \mathbb{R}^+$ definido por $\phi : x \to \exp x$. Entonces $\phi$ es un homomorfismo, ya que

$\exp(x+y) = \exp x + \exp y$. De igual forma, nota que $\phi$ es $1-1$ y sobre, por lo tanto, existe inverso; de hecho, $\phi^{-1} = \log$, que tambien es un homomorfismo Pues, tenemos $\phi$ es un isomorphismo y que $\mathbb{R} \simeq \mathbb{R}^+$.

(2) Sea $\phi : GL(n, \mathbb{R}) \to \mathbb{R}^*$ dado por $\phi : A \to \det A$. Entonces $\phi$ es un homomorphismo ya que $\det AB = \det A \det B$. Nota que $GL(n, \mathbb{R})$ no es Abeliano, pero $\mathbb{R}^*$ si, por lo tanto $GL(n\mathbb{R}) \not\simeq \mathbb{R}^*$. Esto también dice que no existe inverso $\det^{-1}$. Esto nos dice que los homomorfismos solo preservan el estructura de grupos, pero nada mas de eso.

(3) Considere $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ dado por $\phi(m) = m \mod n$. Entonces $\phi(m+k) = (m+k) \mod n \equiv m \mod n + k \mod n = \phi(m) + \phi(k)$. Así que $\phi$ es un homomorfismo.

(4) Sea $G$ y $H$ grupos, y sea $\phi : G \to H$ un homomorfismo de $G$ sobre $H$. Entonces si $G$ es Abeliano, también lo es $H$. Nota que para $h, h' \in H$, exists $g, g' \in G$ con $\phi(g) = h$ y $\phi(g') = h'$. Entonces $hh' = \phi(g)\phi(g') = \phi(gg') = \phi(g'g) = \phi(g')\phi(g) = h'h$.

(5) Sea $\phi : \mathbb{Z} \to \mathbb{Z}$ dado por $x \to 5x$. Entonces $\phi(x+y) = 5(x+y) = 5x+5y = \phi(x)+\phi(y)$.

(6) Suponga que $G$ es Abeliano y defina $\phi : G \to G$ por la regla $\phi(a) = a^{-1}$. Entonces tenemos que $\phi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \phi(a)\phi(b)$. Así que $\phi$ es un homomorfismo. Nota también que por la ley de inversos de elementos, que $\phi$ es sobre. También tenemos que $\phi$ es $1-1$ ya que $a^{-1} = b^{-1}$ implica que $a = b$, por unicidad de inversos. Por lo tanto $\phi$ es un automorfismo.

(7) Sea $\phi : \mathbb{Z} \to \mathbb{Z}$ dado por $x \to x^2$. $\phi$ no es un homomorfismo ya que en general, $(x+y)^2 \neq x^2 + y^2$. Peros, si tomamos la mapa $\psi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ dado por la misma regla, entonces $\psi$ es un homomorfismo.

**Definición.** Sea $G$ y $H$ grupos, y $\phi : G \to H$ un homomorfismo de $G$ hacia $H$. Definimos el **kernel** de $\phi$ como el conjunto $\ker \phi = \{a \in G : \phi(a) = e'\}$ donde $e'$ es la identitad de $H$. Definimos también la **imagen** del homoorphismo como el conjunto $\Im\phi = \phi(G) = \{\phi(a) : a \in G\}$.

**Lema 2.** *Sea $G$ y $H$ grupos y $\phi : G \to H$ un homomorfismo de $G$ hacia $H$. Entonces $\ker \phi \leq G$ y $\phi(G) \leq H$.*

*Proof.* Nota por definicion qiue $\ker \phi \subseteq G$. Tambien tenemos que $e \in \ker \phi$ por el ley de homomorpfismo. Entonces $\ker \phi$ no es vacio. Ahora, sea $a, b \in \ker \phi$. Entonces, tenemos $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)(\phi(b))^{-1} = e'e' = e'$, pues $ab^{-1} \in \ker \phi$. ■

**Ejemplo 6.** (1) Considere $\phi : \mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ dado por $m \to m \mod 12$. Entonces $\ker \phi = \langle 12m \rangle = 12\mathbb{Z}$. Tambien $\phi(\mathbb{Z}) = \mathbb{Z}/12\mathbb{Z}$; pues $\phi$ es sobre.

(2) Considere $\phi : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ dado por $m \to 3m$. $\phi$ es un homomorfismo, y $\ker\phi = \{x \in \mathbb{Z}/12\mathbb{Z} : 3x \equiv_{12} 0\} = \{0, 4, 8\} = \langle 4\rangle$. De igual manera, $\phi(\mathbb{Z}/12\mathbb{Z}) = \{0, 3, 6, 9\} = \langle 3\rangle$.

(3) Sea $\phi : \mathbb{Z} \to \mathbb{Z}$ dado por $m \to 5m$. Entonces $\ker\phi = \langle 5m\rangle = \langle 0\rangle = 5\mathbb{Z}$. Nota que como $\phi$ es $1-1$, si $a \in 5\mathbb{Z}$, entonces $a = 5m \equiv_5 0$. Note tambien que $\phi(\mathbb{Z}) = 5\mathbb{Z}$, por lo tanto $\phi$ es sobre, asi que tenemos $\mathbb{Z} \simeq 5\mathbb{Z}$.

(4) Sea $D_n$ el grupo dihedral sobre un polygano regular de $n$-vertices. Recuerda que $r^n = t^2 = e$ y que $tr^j = r^{n-j}t$. Considere la homomorfismo $\phi : D_8 \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, donde $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ es un grupo bajo la suma de productos directos. Entonces si $\phi(r) = (1, 0)$ y $\phi(t) = (0, 1)$ entonces tenemos que $\ker\phi = \langle r^2\rangle$ y $\phi(D_8) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

## Lectura 3: Grupos y Subgrupos