MA1101-5 Introducción al Álgebra
Profesor: Mauricio Telias
Auxiliar: Arturo Merino

Auxiliar 13 : Grupos y Anillos

15 de julio del 2017

Recordemos:

- Si $(G,*)$ es una estructura algebraica asociativa, con neutro y tal que todo elemento es invertible, entonces diremos que $(G,*)$ es un grupo. Si ademas la operación $*$ es conmutativa, diremos que es un grupo abeliano.
- Sea $(G,*)$ un grupo, entonces:
  1. El inverso de cada elemento es único.
  2. $(\forall x \in G)$, $(x^{-1})^{-1} = x$.
  3. $(\forall x, y \in G)$, $(x * y)^{-1} = y^{-1} * x^{-1}$.
  4. Todo elemento $x \in G$ es cancelable.
  5. Para todo $a, b \in G$, las ecuaciones:
  $$a * x_1 = b$$
  $$x_2 * a = b$$
  tienen solución única. Ellas son $x_1 = a^{-1} * b$ y $x_2 = b * a^{-1}$.
  6. El **único** elemento idempotente de G es su neutro.
- Sea $(G,*)$ un grupo, y sea $H \subseteq G$. Diremos que H es subgrupo de G si $(H,*)$ también es grupo.
- **Caracterización de Subgrupo:** Sea $H \neq \emptyset$, entonces:

  $(H,*)$ subgrupo de $(G,*)$ $\Leftrightarrow$ $(\forall x, y \in H)$ $x*y^{-1} \in H$
- $(\mathbf{Z}_n, +_n)$ es un grupo abeliano.
- **Teorema de Lagrange:** Sea $(G,*)$ un grupo finito y $(H,*)$ un subgrupo de $(G,*)$. Entonces $|H|$ divide a $|G|$.
- Sea $(G,*)$ un grupo. A $|G|$ le llamaremos el orden del grupo.
- Si $f : G \to H$ es un morfismo y tanto $(G,*)$ como $(H,*)$ son grupos, entonces:
  1. $f(e_G) = e_H$.
  2. $f(a^{-1}) = f(a)^{-1}$
- A una estructura $(A, +, \cdot)$ le llamaremos anillo si satisface:
  1. $(A, +)$ es un grupo abeliano.
  2. $\cdot$ es asociativa.
  3. $\cdot$ distribuye con respecto a $+$.
- $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con unidad.
- Si $(A, +, \cdot)$ es un anillo con unidad y $|A| \geq 2$, entonces $0 \neq 1$.
- Sea $(A, +, \cdot)$ un anillo, entonces:
  1. 0 es absorbente.
  2. $(\forall x, y \in A)$, $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$.
  3. $(\forall x, y \in A)$, $(-x) \cdot (-y) = x \cdot y$.
  4. Si A tiene unidad:
  $$(\forall x \in A)\ -x = (-1) \cdot x = x \cdot (-1)$$
- $(\mathbf{Z}_n, +_n, \cdot_n)$ es un anillo conmutativo con unidad.

P1. [Varios]
Sea $(G,*)$ un grupo con neutro e.

a) Sea $f : G \to G$, definida por $f(x) = x^{-1}$. Demuestre que:
$$f \text{ es morfismo} \iff (G,*) \text{ es abeliano}$$
En caso de que $(G,*)$ sea abeliano ¿Es f un isomorfismo?.

b) Suponga que $\forall x \in G$ se tiene que $x * x = e$, demuestre que G es abeliano.

c) Sean $a, b \in G$. Demuestre que si $\exists n \in \mathbb{N}$ tal que $(a * b)^n = e$, entonces $(b * a)^n = e$.
Obs : Ojo que $(G,*)$ no es necesariamente abeliano.

P2. [Subgrupos]
Sea $(G, *)$ un grupo y $a \in G$. Demuestre que los siguientes son subgrupos de $(G, *)$:

a) Definimos el centro de G como:

$$Z(G) = \{x \in G : x * y = y * x,\ \forall y \in G\}$$

Demuestre que el centro de G es un subgrupo abeliano de G.

b) $\langle a \rangle = \{a^n : n \in \mathbb{N}\}$, con el supuesto extra de que G es finito.
Obs: Considere la convención $a^0 = e$.

c) Sea (H, Δ) otro grupo y $\varphi : G \to H$ un morfismo. Definimos el *kernel* de φ como:

$$\mathrm{Ker}(\varphi) = \{g \in G : \varphi(g) = e_H\}$$

Demuestre que $\mathrm{Ker}(\varphi)$ es un subgrupo de G.

P3. [Teorema de Lagrange]
Sea $(G, *)$ un grupo tal que $|G|$ es finito.

a) Demuestre que si existe $x \in G \setminus \{1\}$ tal que $x = x^{-1}$, entonces $|G|$ es par.

b) Suponga ahora que $|G| = 6$. Demuestre que no existe $x \in G$, tal que $x^4 = e$ y $x \neq e$, $x^2 \neq e$.

c) Suponga ahora que $|G| = 4$. Encuentre el máximo número de subgrupos para $(G, *)$.

d) Suponga ahora que $|G| = 4$. Pruebe que $\forall\, a \in G \setminus \{e\},\ a^3 \neq e$ $(a^3 = a * a * a)$.

e) Sea ahora (H, Δ) un grupo y asuma que $|G|$ es par y $|H|$ impar. Demuestre que no existe un morfismo inyectivo de G en H.

P4. [Grupos de orden 4]

a) Construya la tabla para la operación $\cdot_5$ en $\mathbf{Z}_5$

b) Explique por que $(\mathbf{Z}_5, \cdot_5)$ no es un grupo.

c) Muestre que $(\mathbf{Z}_5 \setminus \{[0]\}, \cdot_5)$ es un grupo abeliano.

d) Encuentre los subgrupos de $(\mathbf{Z}_5 \setminus \{[0]\}, \cdot_5)$. Explique.

e) Demuestre que $(\mathbf{Z}_5 \setminus \{[0]\}, \cdot_5) \cong (\mathbf{Z}_4, +_4)$.

f) Demuestre que $(\mathbf{Z}_4, +_4)$ no es isomorfo a $(\mathbf{Z}_2, +_2) \otimes (\mathbf{Z}_2, +_2)$.

g) Demuestre que si $(G, *)$ es un grupo tal que $|G| = 4$, entonces $(G, *) \cong (\mathbf{Z}_2, +_2) \otimes (\mathbf{Z}_2, +_2)$ o $(G, *) \cong (\mathbf{Z}_4, +_4)$.

P5. [Subanillos y el Centro]
Sea $(A, +, \cdot)$ un anillo con unidad.

a) Demuestre que la intersección finita de subanillos es un subanillo.
Hint: Argumente por que basta con demostrar que la intersección de dos subanillos es un subanillo.

b) Definimos el centro $(A, +, \cdot)$ como:

$$Z(A) = \{z \in A : za = az,\ \forall a \in A\}$$

Demuestre que $Z(A)$ es un subanillo de $(A, +, \cdot)$ que contiene la unidad.

c) Suponga ahora que $(A, +, \cdot)$ satisface para todo $a \in A$:

$$a^2 = 0 \implies a = 0$$

Demuestre que todo elemento idempotente esta en $Z(A)$.

d) Suponga ahora que $(A, +, \cdot)$ satisface para todo $a \in A$:

$$a^2 - a \in Z(A)$$

Demuestre que $(A, +, \cdot)$ es conmutativo.