MA1101-6 Introducción al Álgebra
Profesor: Martín Matamala
Auxiliar: Matías Azócar Carvajal

Auxiliar 12: Subgrupo x Anillo x Cuerpo

8 de agosto de 2018

- **Def:** Sea $(G,*)$ un grupo, y sea $H \subseteq G$, $H \neq \emptyset$. Diremos que H es *subgrupo* de G si $(H,*)$ también es grupo.
- Sea $(G,*)$ un grupo, y $(H,*)$ un subgrupo de él. Un par de propiedades bacanes son las siguientes:
  - Si $e \in G$ es el neutro de G y $e_H \in H$ es el neutro de H, entonces $e = e_H$. (Se hereda el neutro)
  - Además, sea $x \in H$. Si $x^{-1} \in G$ es el inverso de x en $(G,*)$ y $x_e \in H$ es el inverso de x en $(H,*)$, entonces $x^{-1} = x_e$. (Se hereda el inverso)
- **Caracterización de subgrupos:** Sea $H \neq \emptyset$. Entonces $(H,*)$ es subgrupo de $(G,*)$ $\Leftrightarrow$ $\forall x,y \in H, x * y^{-1} \in H$.
- **Traslaciones de un subgrupo** Sea H subgrupo de $(G,*)$. Una *traslación* por la izquierda de H en $a \in G$, es el conjunto $a * H$ definido por $a * H = \{a * h : h \in H\}$.
- Sea H un subgrupo de $(G,*)$. Entonces, el conjunto de las traslaciones de H particiona G. **Además**, el cardinal de cada traslación coincide con el cardinal de H.
- **Def**: Sea $(G,*)$ un grupo. Diremos que es un grupo finito si G es un conjunto finito. A $|G|$ se le llama *orden del grupo*. Por ejemplo, $\mathbb{Z}_3$ es un grupo finito de orden 3.
- **Teorema de Lagrange:** Si $(H,*)$ es subgrupo del grupo finito $(G,*)$, entonces $|H|$ divide a $|G|$.
- **Def**: *Anillo* es una estructura $(A,+,\cdot)$ que cumple lo siguiente:
  - $(A,+)$ es grupo abeliano.
  - $\cdot$ es asociativa.
  - $\cdot$ distribuye con respecto a $+$.
  - (Con unidad) Si es que existe neutro para $\cdot$.
  - (Conmutativo) Si $\cdot$ conmuta.
- Por convención, $e_+ = 0$ y $e_. = 1$
- Si $(A,+,\cdot)$ es un *anillo con unidad* con $|A| \geq 2$, entonces $0 \neq 1$. O sea, los neutros de ambas operaciones son distintos.
- **Homomorfismo de anillos** Sean $(A,+,\cdot)$ y $(B,+,\cdot)$ dos anillos con unidad. Un homomorfismo de $(A,+,\cdot)$ en $(B,+,\cdot)$, es una función $f : A \to B$ que cumple $\forall x,y \in A, f(x+y) = f(x)+f(y),\ f(x \cdot y) = f(x) \cdot f(y)$ y $f(1) = 1$.
- **Divisores de cero** Sea $(A,+,\cdot)$ un anillo. Un elemento $a \in A$, $a \neq 0$ es un divisor de cero si existe $y \in A \setminus \{0\}$ tal que $a \cdot y = 0$ o $y \cdot a = 0$. Notamos que cuando esto ocurre, y también es un divisor de cero.
- **Def:** *Cuerpo* será una estructura $(K,+,\cdot)$ si se tienen las siguientes dos:
  - $(K,+,\cdot)$ es anillo conmutativo con unidad
  - Todo elemento $x \in K \setminus \{0\}$ es invertible para $\cdot$.

  (o equivalentemente, si se tienen las siguientes 3)
  - $(K,+)$ es grupo abeliano.
  - $(K \setminus \{0\},\cdot)$ es grupo abeliano.
  - $\cdot$ distribuye con respecto a $+$.
- Si $(K,+,\cdot)$ es cuerpo $\Rightarrow$ $(K,+,\cdot)$ no tiene divisores de cero.
- Si $(K,+,\cdot)$ no tiene divisores de cero y $|K| < \infty \Rightarrow$ $(K,+,\cdot)$ es cuerpo.

P1.- Considere $(\mathbb{Z}_5, \cdot_5)$.

a) Explique por qué $(\mathbb{Z}_5, \cdot_5)$ no es un grupo.

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

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

P2.- En $\mathbb{Z} \times \mathbb{Z}$ se definen las siguientes *l.c.i.* $\forall (a,b),(c,d) \in \mathbb{Z}^2$:

$$(a,b) \oplus (c,d) = (a+c, b+d)$$

$$(a,b) \odot (c,d) = (ac, 0)$$

Sabiendo que $(\mathbb{Z}^2, \oplus)$ es grupo abeliano.

a) Verifique que $(\mathbb{Z}^2, \oplus, \odot)$ es anillo.

b) Averigüe si $(\mathbb{Z}^2, \oplus, \odot)$ tiene unidad o divisores de cero. ¿Es $(\mathbb{Z}^2, \oplus, \odot)$ un cuerpo?

P3.- Se define en $\mathbb{R}$ la *l.c.i.* $\star$ por $x \star y = (\sqrt[3]{x} + \sqrt[3]{y})^3$. Se pide:

a) Probar que $(\mathbb{R}, \star, \cdot)$ es cuerpo. (Donde $\cdot$ es el producto usual en $\mathbb{R}$)

b) Demostrar que $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = \sqrt[3]{x}$ es un *isomorfismo* de $(\mathbb{R}, \star, \cdot)$ en $(\mathbb{R}, +, \cdot)$.

P4.- *a*) Sea $(G, *)$ un grupo abeliano y H, $K \subseteq G$ dos subgrupos de G. Probar que el conjunto

$$H * K = \{h * k | h \in H, k \in K\}$$

es subgrupo de $(G, *)$.

b) Sea $(G, *)$ un grupo finito de orden 4, con neutro $e \in G$. Pruebe que $\forall a \in G \setminus \{e\}, a * a * a \neq e$
Indicación: Argumente por contradicción y use el Teorema de Lagrange.

P5.- Sea $(K, +, \cdot)$ un cuerpo y $(A, \oplus, \odot)$ un anillo con unidad. Sea $f : K \to A$ una función tal que $f : (K, +) \to (A, \oplus)$ y $f : (K, \cdot) \to (A, \odot)$ son morfismos y $f(1_K) = 1_A$ con $1_A \neq 0_A$. Pruebe que:

a) $f(0_K) = 0_A$.

b) $\forall x \in K, f(-x) = -f(x)$.

c) $(f(K), \oplus)$ es un subgrupo de $(A, \oplus)$

d) $f(x) = 0_A \Leftrightarrow x = 0_K$

e) $f(x)$ es inyectiva. (O sea, f es un monomorfismo)

P6.- **[Propuesto]** Sea $(K, \oplus, \odot)$ un cuerpo. Se sabe que $(K \times K, \oplus, \odot)$ con $(x_1, y_1) \oplus (x_2, y_2) = (x_1 \oplus x_2, y_1 \oplus y_2)$ y $(x_1, y_1) \odot (x_2, y_2) = (x_1 \odot x_2, y_1 \odot y_2)$ es un anillo conmutativo con unidad (no es necesario que lo demuestre).

a) Encuentre neutro para $\oplus$ y neutro para $\odot$ en $K \times K$.

b) Demuestre que para $(a,b) \neq 0_{K \times K}$: (a,b) es invertible $\Leftrightarrow$ (a,b) no es un divisor del cero.

c) ¿Es $(K \times K, \oplus, \odot)$ cuerpo?. Justifique

P7.- **[Propuesto]** Sea $(A, +, \cdot)$ un anillo conmutativo con unidad. Se tiene $G \subseteq A$ por

$$G = \{a \in A | \text{ a tiene inverso para } \cdot\}$$

a) Mostrar que $(G, \cdot)$ es grupo abeliano.

b) Sea $H = \{a^2 | a \in G\}$. Pruebe que H es subgrupo de G.

c) Si $A = \mathbb{Z}_8$, encuentre G y H.