**MA1101-2 Introducción al Álgebra**
**Profesor:** Leonardo Sánchez C.
**Auxiliar:** Marcelo Navarro

# Auxiliar 12: Lagrange, Anillos y Cuerpos

11 de Junio de 2019

**P1.** Sea $(G, *)$ un grupo tal que $|G|$ es finito.

*a*) Demuestre que si existe $x \in G \setminus \{e\}$ 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*) **[Propuesto]** Suponga ahora que $|G| = 4$. Encuentre el máximo número de subgrupos para $(G, *)$.

**Solución 1.**

a) *Notemos que si existe un $x$ tal que $x = x^{-1}$ tenemos que $\{e, x\}$ es un subgrupo de $G$. En efecto mirando la tabla de la operación:*

| $*$ | $e$ | $x$ |
|---|---|---|
| $e$ | $e$ | $x$ |
| $x$ | $x$ | $e$ |

*Nos logramos convencer de esto. Llamemos al subgrupo anterior $H$, por el teorema de Lagrange sabemos que $|H|$ divide a $|G|$, es decir:*

$$|G| = k|H| \text{ para algún } k \in \mathbb{N}$$

*Como $|H| = 2$ concluimos que el cardinal de $G$ es par.*

b) *Supongamos que existe un $x$ tal que $x^4 = e$. Luego el conjunto $H = \{e, x, x^2, x^3\}$ (notemos que los elementos son diferentes, pues $x \neq e$ y $x^2 \neq e$) es un subgrupo de $(G, *)$, en efecto veamos su tabla:*

| $*$ | $e$ | $x$ | $x^2$ | $x^3$ |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $x^2$ | $x^3$ |
| $x$ | $x$ | $x^2$ | $x^3$ | $x^4 = e$ |
| $x^2$ | $x^2$ | $x^3$ | $x^4 = e$ | $x^5 = x$ |
| $x^3$ | $x^3$ | $x^4 = e$ | $x^5 = x$ | $x^6 = x^2$ |

*De esto podemos ver que $H$ es un grupo. Aplicando el teorema de Lagrange tenemos que:*

$$\frac{|G|}{|H|} \in \mathbb{N} \implies \frac{6}{4} \in \mathbb{N}$$

*Lo que es una contradicción.*

c) *Supongamos que $G = \{e, a, b, c\}$, encontremos el máximo numero de subgrupos. Si $(H, *)$ es un subgrupo de $(G, *)$, tiene que ocurrir que $\frac{4}{|H|} \in \mathbb{N}$ por el teorema de Lagrange. Tenemos entonces que $|H|$ puede ser $1, 2$ o $4$. Si $|H| = 1$, entonces $H = \{e\}$, mientras que si $|H| = 4$, entonces $H = G$. El caso interesante es cuando $|H| = 2$, como el $e$ tiene que estar en $H$, tenemos los siguientes potenciales subgrupos:*

$$\{e, a\} \qquad \{e, b\} \qquad \{e, c\}$$

*Construyamos las tablas de esos conjuntos*

| $*$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | ? |

| $*$ | $e$ | $b$ |
|---|---|---|
| $e$ | $e$ | $b$ |
| $b$ | $b$ | ? |

| $*$ | $e$ | $c$ |
|---|---|---|
| $e$ | $e$ | $c$ |
| $c$ | $c$ | ? |

*Notemos entonces que si $a^2 = e$, $b^2 = e$ y $c^2 = e$ los anteriores serían todos subgrupos, ¿Es esto posible? La respuesta es si, basta con rellenar la tabla del grupo original imponiendo estas condiciones:*

| $*$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | ? | ? |
| $b$ | $b$ | ? | $e$ | ? |
| $c$ | $c$ | ? | ? | $e$ |

$\implies$

| $*$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

*Donde los espacios faltantes se logran mediante la regla del Sudoku. Concluimos entonces que el número máximo de subgrupos de* $(G, *)$ *son 5.*
Obs: Es interesante notar que este grupo que acabamos de construir no es isomorfo a $(\mathbf{Z}_4, +_4)$.

**P2.** Sea $(G, *)$ es un grupo con neutro $e$.

*a*) Demuestre que si $H, K$ son subgrupos de $G$ entonces $H \cap K$ también lo es.

*b*) Demuestre que si $H, K$ son subgrupos de $G$, tales que $|H| = 38$ y $|K| = 55$. Demostrar que $H \cap K = \{e\}$.

**Solución 2.**

a) *Notemos primero que $H \cap K$ es subconjunto de $G$ pues $H$ y $K$ lo son (y por ende su intersección). Además, como en todo grupo debe existir el neutro y, $H$ y $K$ son subgrupos de $G$, se tiene que el neutro de $G$, desde ahora denotado por $e$, pertenece a $H$ y $K$ simultaneamente, es decir $e \in H \cap K$. Luego $H \cap K \neq \emptyset$. En virtud de lo anterior podemos ocupar la caracterización de subgrupos.*
*Sea $x, y \in H \cap K$. debemos probar que $x * y^{-1} \in H \cap K$.*
*En efecto, como $x, y \in H \cap K$, se tiene que*

$$x \in H \quad \wedge \quad y \in H \quad \wedge \quad x \in K \quad \wedge \quad y \in K$$

*De lo anterior podemos concluir que como $H$ y $K$ son subgrupos de $G$ (en particular son grupos). Se tiene que si $y \in H \Rightarrow y^{-1} \in H$ y lo mismo para $K$, es decir, $y \in K \Rightarrow y^{-1} \in K$*
*Con lo anterior se tiene para $H$ que*

$$x \in H \wedge y \in H \Rightarrow x \in H \wedge y^{-1} \in H$$

*Luego como $*$ es una lci, se tiene que $x * y^{-1} \in H$.*
*Analogo para $K$ se tiene que $x * y^{-1} \in K$.*
*Como $x * y^{-1} \in H$ y $x * y^{-1} \in K$. se concluye que $x * y^{-1} \in H \cap K$*
*Y por caracterización de subgrupos se concluye que $H \cap K$ es subgrupo de $G$.*

b) *Por la parte a) sabemos que $H \cap K$ es subgrupo de $G$, es decir $H \cap K$ es un grupo.*
*Además como $H \cap K \subseteq H$ se concluye que $H \cap K$ es subgrupo de $H$ tambien. (pues por defınción un cjto $A$ es subgrupo de $B$ si $A$ es grupo y $A \subseteq B$). Del mismo modo $H \cap K \subseteq K$.*
*Luego por teorema de lagrange sabemos que*

$$\frac{|H|}{|H \cap K|} \in \mathbb{N} \quad \wedge \quad \frac{|K|}{|H \cap K|} \in \mathbb{N}$$

*que equivale a*

$$\frac{38}{|H \cap K|} \in \mathbb{N} \quad \wedge \quad \frac{55}{|H \cap K|} \in \mathbb{N}$$

*de lo anterior podemos concluir que $|H \cap K|$ divide a 38 y 55 al mismo tiempo. si vemos los divisores de 38 y 55 podemos darnos cuenta que el unico divisor en comun es el 1 ya que:*
$div_{38} = \{1, 38, 19, 2\}$ *y* $div_{55} = \{1, 55, 11, 5\}$
*Entonces* $div_{38} \cap div_{55} = \{1\}$
*Por lo tanto $|H \cap K| = 1$ y el unico grupo de cardinal 1 que se puede formar es el grupo que contiene unicamente al elemento neutro, es decir, $H \cap K = \{e\}$*

**P3.** En $\mathbb{Z}^2$ se definen las siguientes leyes de composición interna:

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

Sabiendo que $(\mathbb{Z}^2, \oplus)$ es grupo Abeliano (no lo demuestre).

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

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

**P4.** Sean $(A, +, \cdot)$ y $(B, \oplus, \odot)$ dos anillos con unidad. Sea $f : A \to B$ un morfismo de anillos, es decir:

$$f(x+y) = f(x) \oplus f(y) \qquad f(x \cdot y) = f(x) \odot f(y) \qquad f(1_A) = 1_B$$

*a*) Demuestre que para todo $a \in A$, $f(a^{-1}) = f(a)^{-1}$.

*b*) Demuestre que $f(0_A) = 0_B$.

*c*) Demuestre que si todo $a \in A$ es invertible salvo $0_A$, entonces $f$ es inyectiva.

**Solución 3.**

a) *notemos que como $f$ es morfismo $f(a \cdot a^{-1}) = f(a) \odot f(a^{-1})$ y además por otro lado $f(a \cdot a^{-1}) = f(1_A) = 1_B$. Juntando lo anterior se tiene que*

$$1_B = f(a) \odot f(a^{-1})$$

*Es decir, $f(a)$ y $f(a^{-1})$ son inversos para $\odot$ entre si pues al operarse dan la unidad. luego $f(a^{-1}) = f(a)^{-1}$*

b) *la misma idea de la parte anterior. Notemos que $f(0) = f(0+0) = f(0) \oplus f(0)$. Entonces*

$$\begin{aligned}
f(0) &= f(0) \oplus f(0) && /operando \quad \oplus -f(0) \\
f(0) \oplus -f(0) &= f(0) \oplus [f(0) \oplus -f(0)] && f(0) \oplus -f(0) = 0_B \\
0_B &= f(0) \oplus 0_B && 0_B \text{ es neutro} \\
0_B &= f(0) && fin
\end{aligned}$$

c) *Idea: demuestren inyectividad como siempre. en el paso de $f(x) = f(y)$ ocupar morfismo y llegar a $f(x-y) = 0_B$, entonces $x - y = 0_A$ y concluir.*

**P5.** Sea $(\mathbb{K}, +, \cdot)$ un cuerpo. Definimos las siguientes operaciones sobre $\mathbb{K} \times \mathbb{K}$:

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

Se sabe (no lo demuestre) que $(\mathbb{K} \times \mathbb{K}, \oplus, \odot)$ es un anillo conmutativo con unidad.

*a*) Encuentre el neutro para $\oplus$ y el neutro para $\odot$.

*b*) Demuestre que $\forall(a, b) \in (\mathbb{K} \times \mathbb{K}) \setminus \{0_{\mathbb{K}\times\mathbb{K}}\}$:

$$(a, b) \text{ es divisor del } 0 \iff (a, b) \text{ no es invertible}$$

*c*) ¿Es $(\mathbb{K} \times \mathbb{K}, \oplus, \odot)$ un cuerpo? Argumente.

**Solución 4.**

a) *El neutro para $\oplus$ es $(0, 0)$, pues:*

$$(a, b) \oplus (0, 0) = (a + 0, b + 0) = (a, b)$$

*Y el neutro para $\odot$ es $(1, 1)$, pues:*

$$(a, b) \odot (1, 1) = (a \cdot 1, b \cdot 1) = (a, b)$$

Obs: Chequeamos solo por un lado, pues la operaciones son conmutativos.

b)
- $(\implies)$:
  *Como $(a, b)$ es divisor del 0, entonces existe $(c, d) \neq (0, 0)$ tal que $(a, b) \odot (c, d) = (0, 0)$. Supongamos que $(a, b)$ es invertible, luego:*

  $$(a, b) \odot (c, d) = (0, 0) \implies (a, b)^{-1} \odot (a, b) \odot (c, d) = (a, b)^{-1} \odot (0, 0) \implies (c, d) = (0, 0)$$

  *Lo que es una contradicción. Por tanto $(a, b)$ no es invertible.*
- $(\impliedby)$:
  *Notemos primero que:*

  $$\begin{aligned} & (a, b) \text{ es invertible} \\ \iff & \exists(c, d), \text{ tal que } (a, b) \odot (c, d) = (1, 1) \\ \iff & \exists(c, d), \text{ tal que } (a \cdot c, b \cdot d) = (1, 1) \\ \iff & \exists c, d \text{ , tal que } a \cdot c = 1 \text{ y } b \cdot d = 1 \\ \iff & a \text{ es invertible y } b \text{ es invertible} \\ \iff & a \neq 0 \text{ y } b \neq 0 \end{aligned}$$

  *Donde en el último paso ocupamos el hecho de que los elementos invertibles en un cuerpo son los distintos de 0. De esto tenemos que si $(a, b)$ no es invertible, entonces $a = 0$ o $b = 0$. Pongamonos en casos:*
  - ***Caso 1:** $(a = 0)$*
    *Si $a = 0$, entonces $(a, b) = (0, b)$, luego:*

    $$(0, b) \odot (1, 0) = (0 \cdot 1, b \cdot 0) = (0, 0)$$

    *Por tanto $(a, b)$ es un divisor del 0.*
  - ***Caso 2:** $(b = 0)$*
    *Si $b = 0$, entonces $(a, b) = (a, 0)$, luego:*

    $$(a, 0) \odot (0, 1) = (a \cdot 0, 0 \cdot 1) = (0, 0)$$

    *Por tanto $(a, b)$ es un divisor del 0.*

  *Concluimos entonces que en cualquier caso $(a, b)$ es divisor del 0.*

c) *No es un cuerpo, pues posee divisores del 0. Por ejemplo $(1, 0) \odot (0, 1) = (0, 0)$.*