MA1101-1 Introducción al Álgebra
Profesor: Leonardo Sánchez C.
Auxiliar: Marcelo Navarro

Auxiliar 12: Grupos y Anillos

15 de junio de 2017

P1. Sea $(G, *)$ y $(H, \triangle)$ grupos. Considere las siguientes tablas (incompletas) que definen a las operaciones $*$ y $\triangle$.

$*$	a	b	c	d
a	a			
b		a		
c		d		b
d				

$\triangle$	p	q	r	s	t	u
p			q			
q	r					
r					r	
s		p				
t						
u	t					p

a) Sea $(G', \bullet)$ un grupo arbitrario. Demuestre que cada fila y cada columna de la tabla del grupo $(G', \bullet)$ posee cada elemento de G' una única vez.

b) Complete las tablas.

P2. 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 $(G, *)$

P3. Sea $(G, *)$ un grupo finito de orden 4, es decir $|G| = 4$, con neutro $e \in G$.
Muestre que $\forall a \in G$, $a^3 = a * a * a \neq e$.
Hint: *Razone por contradicción y use el Teorema de Lagrange.*

P4. Sea $(A, +, \cdot)$ un anillo booleano, es decir, $(A, +, \cdot)$ es un anillo que verifica que $a^2 = a$ para todo $a \in A$. Demuestre que:

a) Para todo $x \in A$ se tiene que $x = -x$

b) $(A, +, \cdot)$ es conmutativo.

c) Para todo $x, y \in A$ se tiene que $(x \cdot y)(x + y) = 0$

d) Ningún anillo booleano con más de 3 elementos es dominio de integridad (es decir, no posee divisores de cero). ¿Que pasa si el anillo tiene dos elementos?.

P5. **[Propuesto - Traslaciones]** Sea $(G, *)$ un grupo con neutro e. Defina $f : G \to G$ un homomorfismo y $H = \{a \in G : f(a) = e\}$. Demuestre que H es subgrupo de G y que $\forall a \in G, a * H = H * a$ (es decir, dado $a \in G$ la traslación por la izquierda y la traslación por la derecha de H son iguales).

P6. [Propuesto - 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. **hint**: sea $e \in G$ el neutro. Considere la estructura $(\{e, x\}, *)$. Compruebe que es subgrupo de G y use el teorema de lagrange

b) Suponga ahora que $|G| = 6$. Demuestre que no existe $x \in G$ tal que $x^4 = e$ y $x \neq e$, $x^3 \neq e$. **Hint:** Proceda por contradicción. Es decir asuma que existe un elemento que cumple las propiedades descritas. Encuentre un grupo adecuado y use teorema de lagrange

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

P7. [Lagrange] El objetivo de este problema, es demostrar que todo grupo $(G, *)$ no abeliano (con neutro $e \in G$) posee al menos 6 elementos. Para lograr esto, demostraremos que todo grupo con a lo más 5 elementos es necesariamente abeliano; procediendo como se detalla a continuación:

a) Antes de comenzar, ¿por qué probar que todo grupo con a lo más 5 elementos es necesariamente abeliano, equivale a demostrar el resultado que deseamos? Argumente en términos lógicos.

b) Justifique por que en el caso de $|G| = 1$, $(G, *)$ es claramente un grupo abeliano.

c) Dado un grupo $(G, *)$, decimos que G es cíclico si es que existe $a \in G$ tal que

$$G = \{a^k \ : \ k \in \mathbb{Z}\},$$

donde $a^k = \underbrace{a * a * \ldots * a}_{k \ veces}$. Muestre que si $|G| = p$ con p un número primo, entonces G es cíclico.
Hint: *Para $a \in G$ con $a \neq e$, defina*

$$H = \{a^k \ : \ k \in \mathbb{Z}\},$$

muestre que $(H, *)$ es subgrupo de $(G, *)$ y use el Teorema de Lagrange para concluir.

d) Muestre que si G es cíclico, entonces $(G, *)$ es un grupo abeliano.

e) De lo mostrado en la parte anterior, deduzca que sólo resta probar que para el caso $|G| = 4$, $(G, *)$ es un grupo abeliano. Demuestre entonces este caso faltante, y concluya nuestro objetivo.
Hint: *Note que volviendo a definir el subgrupo H para $a \in G$, $a \neq e$; al usar el Teorema de Lagrange aparecen ahora dos casos posibles, que debe estudiar por separado.*

P8. [Producto de grupos] Sean $(G, *)$ y $(H, \star)$ grupos con neutros e_G y e_H respectivamente. Se define en $G \times H$ la l.c.i. $\triangle$ por:

$$(a, b) \triangle (c, d) = (a * c, b \star d).$$

a) Demuestre que $(G \times H, \triangle)$ es grupo.

b) Demuestre que las funciones ϕ y ψ definidas por:

$$\begin{array}{rcl} \phi : G \times H & \to & G \\ (g, h) & \mapsto & \phi(g, h) = g, \end{array}$$

$$\begin{aligned} \phi : G \times H &\to H \\ (g,h) &\mapsto \phi(g,h) = h, \end{aligned}$$

son morfismos sobreyectivos.

c) Ahora considere $G = H$, $* = \star$ y la funcin $f : G \times G \to G$ definida por:

$$f(a,b) = (a * b)^{-1}, \quad \forall (a,b) \in G \times G.$$

Pruebe que f es morfismo de $(G \times G, \triangle)$ en $(G, *)$ si y slo si $(G, *)$ es un grupo abeliano.

- 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:
  $$\begin{aligned} a * x_1 &= b \\ x_2 * a &= b \end{aligned}$$
  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:
  $$(H,*) \text{ subgrupo de } (G,*) \Leftrightarrow (\forall x, y \in H)\ x*y^{-1} \in H$$
- $(\mathbf{Z}_n, +_n)$ 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 $+$.
- Sea $(A,+,\cdot)$ un anillo, tenemos la siguiente notación:
  1. Al neutro de $(A,+)$ se le suele denotar por 0, mientras que el inverso de x para $+$ se denota por $-x$.
  2. Si $(A,\cdot)$ tiene neutro a dicho neutro le llamaremos 1, más aún diremos que $(A,+,\cdot)$ es un anillo con unidad. Si $x \in A$ posee inverso para $\cdot$ lo denotaremos por x^{-1}.
  3. Si $\cdot$ es conmutativa, diremos que $(A,+,\cdot)$ es un anillo conmutativo.
- $(\mathbb{Z},+,\cdot)$ 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.
- Sea $(A,+,\cdot)$ un anillo. Si $x, y \in A \setminus \{0\}$ son tales que $x \cdot y = 0$, diremos que x e y son divisores del 0.