MA1101-2 Introducción al Álgebra
Profesor: José Soto
Auxiliares: Arturo Merino, Nicolás Zalduendo

Pauta 12 : Lagrange, Morfismos y Anillos

21 de noviembre del 2016

P1. [Varios 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 $(G, *)$.

Solución 1.

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

$*$	1	x
1	1	x
x	x	1

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

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

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

$\Longrightarrow$

$*$	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. [El núcleo y la imagen]
Sean $(G,*)$, $(H\cdot)$ grupos con neutro e_G y e_H respectivamente. Sea también $\varphi : G \to H$ un morfismo.

a) Demuestre que $\varphi(G)$ es un subgrupo de H.

b) Definimos el *kernel* de φ como:

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

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

c) Demuestre que φ es inyectiva si y sólo si $\text{Ker}(\varphi) = \{e_G\}$.

d) Suponga que G y H son finitos y que $|G|$ es par y $|H|$ impar. Demuestre que no existe un morfismo inyectivo de G en H.

Solución 2.

a) Notemos que $\varphi(G) \neq \emptyset$, pues $e_H = \varphi(e_G) \in \varphi(G)$. Sea entonces $x, y \in \varphi(G)$, luego existen $a, b \in G$ tales que:

$$\varphi(a) = x \qquad \varphi(b) = y$$

Ocuparemos el teorema de caracterización de subgrupo, es decir demostraremos que $x * y^{-1} \in \varphi(G)$. En efecto:

$$x \cdot y^{-1} = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(\underbrace{a * b^{-1}}_{\in G}) \in \varphi(G)$$

Es decir $\varphi(G)$ es un subgrupo de H.

b) Notemos que $\text{Ker}(\varphi) \neq \emptyset$, pues $\varphi(e_G) = e_H$ (es decir $e_G \in \text{Ker}(\varphi)$). Sean $x, y \in \text{Ker}(\varphi)$, entonces:

$$\varphi(x * y^{-1}) = \varphi(x) \cdot \varphi(y^{-1}) = \varphi(x) \cdot \varphi(y)^{-1} = e_H \cdot e_H^{-1} = e_H$$

Es decir $x * y^{-1} \in \text{Ker}(\varphi)$. De esto concluimos que $\text{Ker}(\varphi)$ es un subgrupo de H.

c) Demostremos cada implicancia por separado:

- $(\implies)$:
  Es claro que $\{e_G\} \subseteq \text{Ker}(\varphi)$ (pues $\varphi(e_G) = e_H$), demostremos entonces que $\text{Ker}(\varphi) \subseteq \{e_G\}$. Sea $x \in \text{Ker}(\varphi)$, luego:
  $$\varphi(x) = e_H = \varphi(e_G)$$
  Como φ es inyectiva, tenemos que $x = e_G$ y por tanto $x \in \{e_G\}$.
- $(\impliedby)$:
  Sean x, y tales que $\varphi(x) = \varphi(y)$, luego:
  $$\begin{aligned} \varphi(x) &= \varphi(y) && / \cdot \varphi(x^{-1}) \\ \varphi(x) \cdot \varphi(x^{-1}) &= \varphi(y) \cdot \varphi(x^{-1}) \\ \varphi(\underbrace{x * x^{-1}}_{=e_G}) &= \varphi(y * x^{-1}) \\ e_H &= \varphi(y * x^{-1}) \end{aligned}$$
  Es decir $y * x^{-1} \in \text{Ker}(\varphi) = \{e_G\}$, es decir $y * x^{-1} = e_G$ de esto tenemos que $y = x$ y por tanto φ es inyectiva.

d) Supongamos que existe un morfismo $f : G \to H$ inyectivo. Como f es inyectiva $|f(G)| = |G|$, pues a cada elemento de G se le asocia un único elemento en $f(G)$. Además sabemos que $f(G)$ es un subgrupo de $(H,\cdot)$ (por la parte *a*)), por el teorema de Lagrange:

$$\frac{|H|}{|f(G)|} \in \mathbb{N} \implies \frac{|H|}{|G|} = \frac{2m-1}{2n} \in \mathbb{N}$$

Lo que es una contradicción.

P3. [Orden de un elemento]
Sea $(G, *)$ un grupo finito con neutro e. Definimos el orden de $x \in G$ como:

$$o(x) = \text{mín}\{n \in \mathbb{N} : x^n = e\}$$

a) Sea $g \in G$, demuestre que $o(x) = o(gxg^{-1})$.

b) Demuestre que $o(x)$ divide a $|G|$.

c) Sea $(H, \cdot)$ un grupo y $f : G \to H$ un isomorfismo. Demuestre que $o(x) = o(f(x))$.

P4. [Morfismos de Anillos]
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.

P5. **[Anillos Booleanos]**
Sea $(A, +, \cdot)$ un anillo booleano, es decir $(A, +, \cdot)$ es un anillo que verifica $a^2 = a$ 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 $(x \cdot y) \cdot (x + y) = 0$.

d) Ningún anillo booleano con más de tres elementos es cuerpo. ¿Que pasa si el anillo tiene dos elementos ?

Solución 3.

a) Notemos que lo anterior es lo mismo que demostrar que $x + x = 0$. En efecto:

$$(x + x) = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x$$

Luego:

$$x + x = x + x + x + x \implies x + x = 0$$

Que era lo buscado.

b) Veamos que:

$$(x^2 + y^2) = (x + y) = (x + y)^2 = (x + y)(x + y) = x^2 + xy + yx + y^2$$

De esto concluimos que:

$$0 = xy + yx \implies xy = -yx = (-y)x = yx$$

Donde se ocupo la propiedad demostrada anteriormente.

c) Ocuparemos las propiedades que ya demostramos:

$$xy(x + y) = xyx + xyy = x^2y + xy^2 = xy + xy = 0$$

d) Notemos que si un anillo tiene 3 elementos, alguno de ellos no es ni 0 ni 1. Como el anillo es booleano tenemos que dicho elemento es idempotente, es decir:

$$\begin{aligned} x^2 &= x \\ x^2 - x &= 0 \\ \underbrace{x}_{\neq 0}\underbrace{(x-1)}_{\neq 0} &= 0 \end{aligned}$$

De esto concluimos que este elemento es divisor del cero, y por tanto el anillo no puede ser un cuerpo. Si el anillo tiene 2 elementos la proposición falla pues basta con notar que $(\mathbf{Z}_2, +_2, \cdot_2)$ es booleano.