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

Pauta 13 : Grupos y Anillos

15 de julio del 2017

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.

Solución 1.

a) Partamos por demostrar cada implicancia por separado:

- $(\implies)$:
Notemos que si f es un morfismo, entonces $\forall x, y \in G$:

$$f(x * y) = (x * y)^{-1} = y^{-1} * x^{-1}$$

Por otro lado tenemos que:

$$f(x * y) = f(x) * f(y) = x^{-1} * y^{-1}$$

Entonces $\forall x, y \in G$ tenemos la siguiente propiedad $x^{-1} * y^{-1} = y^{-1} * x^{-1}$. Sean, entonces $a^{-1}, b^{-1} \in G$, aplicando la propiedad tenemos:

$$(a^{-1})^{-1} * (b^{-1})^{-1} = (b^{-1})^{-1} * (a^{-1})^{-1} \implies a * b = b * a$$

Como esto se verifica para todo a, b vemos que el grupo es abeliano.

- $(\impliedby)$:
Supongamos ahora que el grupo es abeliano, luego:

$$f(x * y) = (x * y)^{-1} = y^{-1} * x^{-1} = \underbrace{f(y) * f(x)}_{\text{Conmutatividad}} = f(x) * f(y)$$

De donde concluimos que f es un morfismo.

Notemos que en caso de serlo, f es un isomorfismo pues $f \circ f = I_G$, es decir f es invertible y por tanto es biyectiva.

b) Notemos que:

$$(x * y) * (x * y) = 1$$

y por otro lado:

$$(x * x) * (y * y) = 1 * 1 = 1$$

Es decir $x * y * x * y = x * x * y * y$, luego:

$$\begin{array}{rcll} x * y * x * y & = & x * x * y * y & /x^{-1} * \\ y * x * y & = & x * y * y & / * y^{-1} \\ y * x & = & x * y & \end{array}$$

Como lo anterior es válido para todo x, y, entonces el grupo es abeliano.

c) Supongamos existe $n \in \mathbb{N}$ tal que $(a * b)^n = e$, entonces $a * (b * a)^{-1} * b = e$, esto nos dice que a y $(b * a)^{-1} * b$ son inversos entre si y por tanto conmutan, luego: $(b * a)^n = (b * a)^{-1} * b * a = e$ que era lo pedido.

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.

Solución 2.

a) Ocuparemos el teorema de caracterización de subgrupos. Notemos que $Z(G) \neq \emptyset$ pues $e \in Z(G)$ (el neutro conmuta con todos los elementos). Sea entonces $x, y \in Z(G)$, y sea $z \in G$. Luego como $x, y \in Z(G)$:

$$\begin{array}{rcll} x * z &=& z * x & \\ x * \underbrace{(y^{-1} * y)}_{=e} * z &=& z * x & \\ x * y^{-1} * z * y &=& z * x & / * y^{-1} \\ (x * y^{-1}) * z &=& z * (x * y^{-1}) & \end{array}$$

Es decir $(x * y^{-1})$ conmuta con todos los elementos, por tanto $(x * y^{-1}) \in Z(G)$. Concluimos que $Z(G)$ es un subgrupo de G.

b) Notemos que como G es finito, entonces $\langle a \rangle$ repite elemtentos a partir de un punto, es decir $a^i = a^j$ con $j > i$ (sino $\langle a \rangle$ sería infinito). Luego:

$$\langle a \rangle = \{e, a, a^2, \ldots, a^i, \ldots a^j\}$$

Notemos que:

$$\begin{aligned} a^i &= a^j \\ a^i &= a^i * a^{j-i} \\ e &= a^{j-i} \end{aligned}$$

Es decir $\langle a \rangle$ es:

$$\langle a \rangle = \{e, a, a^2, \ldots a^{j-i-1}\}$$

Pues a partir de a^{j-i} comienza denuevo desde e. Llamemos $m = j - i$ para ahorra notación, notemos que esto nos dice que $a^{-1} = a^{m-1}$. Demostremos que $\langle a \rangle$ es subgrupo de G, en efecto $\langle a \rangle \neq \emptyset$ pues $e = a^0 \in \langle a \rangle$. Sean $x, y \in \langle a \rangle$, es decir $x = a^k$ e $y = a^l$ para algún k y algún l. Luego:

$$\begin{aligned} x * y^{-1} &= a^k * (a^l)^{-1} \\ &= a^k * (\underbrace{a * \cdots * a}_{l \text{ veces}})^{-1} \\ &= a^k * (\underbrace{a^{-1} * \cdots * a^{-1}} \\ &= a^k * (a^{-1})^l \\ &= a^k * (a^{m-1})^l \\ &= a^k * a^{l(m-1)} \\ &= a^{k+l(m-1)} \end{aligned}$$

Es decir $x * y^{-1} \in \langle a \rangle$ y por tanto $\langle a \rangle$ es subgrupo.

c) Notemos que $\mathrm{Ker}(\varphi) \neq \emptyset$, pues $\varphi(e_G) = e_H$ (es decir $e_G \in \mathrm{Ker}(\varphi)$). Sean $x, y \in \mathrm{Ker}(\varphi)$, 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 $x * y^{-1} \in \mathrm{Ker}(\varphi)$. De esto concluimos que $\mathrm{Ker}(\varphi)$ es un subgrupo de H.

P3. [Teorema de Lagrange]
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) 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.

Solución 3.

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 $(\mathbf{Z}_4, +_4)$.

d) Supongamos que existe un a tal que $a^3 = e$. Luego $\{1, a, a^2\}$ es un subgrupo de G, en efecto veamos su tabla:

$*$	e	a	a^2
e	e	a	a^2
a	a	a^2	$a^3 = e$
a^2	a^2	$a^3 = e$	$a^4 = a^3 * a = a$

De esto podemos ver que $\{1, a, a^2\}$ es un grupo. Notemos que esto contradecería el teorema de Lagrange, por tanto no puede existir un a tal que $a^3 = e$.

e) Supongamos que existe un morfismo $f : G \to H$ inyectivo. Como f es inyectiva, tenemos que si pensamos a f como $f : G \to f(G)$ es una biyección, es decir, $|f(G)| = |G|$. Además sabemos que $f(G)$ es un subgrupo de $(H, \cdot)$, 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.

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 $(G, *) \cong (\mathbf{Z}_4, +_4)$.

Solución 4. Para esta pregunta $\cdot = \cdot_5$ (para ahorra escritura).

a)

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

b) No todos los elementos son invertibles, en particular viendo la tabla vemos que no existe un y tal que $y \cdot 0 = 1$, es decir 0 no es invertible.

c) Sabemos que $\cdot$ es asociativa para todo $x, y, z \in \mathbf{Z}_5$, en particular si $x, y, z \in \mathbf{Z}_5 \setminus \{0\}$. Construyamos la tabla de la operación:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Aca notamos que 1 es neutro y que todo elemento es invertible (pues en toda fila y en toda columna hay un 1), es decir $(\mathbf{Z}_5 \setminus \{0\}, \cdot)$ es un grupo. Además como la tabla es simétrica respecto a la diagonal el grupo es abeliano.

d) Por el teorema de Lagrange sabemos que los subgrupos pueden ser de orden 1, 2 o 4. Además todos los grupos deben contener al neutro, luego el único subgrupo de orden 1 es $\{1\}$. De orden 4 tiene que ser $\{1, 2, 3, 4\}$ pues no hay más elementos. Nuevamente recordando que el 1 tiene que estar en todos los subgrupos, nuestros candidatos para subgrupos de orden 2 serán $\{1, 2\}$, $\{1, 3\}$ y $\{1, 4\}$. Observando la tabla notamos que el único de esos que es grupo es $\{1, 4\}$. En resumen los subgrupos de $(\mathbf{Z}_5 \setminus \{0\}, \cdot)$ son $\{1\}$, $\{1, 4\}$ y $\{1, 2, 3, 4\}$.

e) PENDIENTE.

f) PENDIENTE.

g) PENDIENTE.

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.

Solución 5. PENDIENTE