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

Auxiliar 11: Estructuras Algebraicas II

05 de Junio de 2019

P1. Si $(G, *)$ es un grupo tal que $(a*b)^2 = a^2 * b^2$ para todo $a, b \in G$, donde $x^n = \underbrace{x * x * \cdots * x}_{n-veces}$. Muestre que G debe ser abeliano.

Solución 1. *Tenemos que G ya es grupo. Para que G sea grupo abeliano solo nos falta ver que $*$ conmuta. En efecto, sea $x, y \in G$ arbitrarios, notemos que se cumple $(x*y)^2 = x^2 * y^2$*

Luego

$$
\begin{array}{rcr}
 & (x*y)^2 = x^2 * y^2 & \textit{hipotesis} \\
\Rightarrow & (x*y)*(x*y) = x*x*y*y & / \ x^{-1}* \\
\Rightarrow & (x^{-1}*x)*y*(x*y) = (x^{-1}*x)*x*y*y & \textit{asociatividad} \\
\Rightarrow & e*y*x*y = e*x*y*y & / \ *y^{-1} \ \textit{neutro} \\
\Rightarrow & y*x*(y*y^{-1}) = x*y*(y*y^{-1}) & \textit{asociatividad} \\
\Rightarrow & y*x*e = x*y*e & \textit{neutro} \\
\Rightarrow & y*x = x*y &
\end{array}
$$

Luego G dado cualquier par de elementos $x, y \in G$, se tiene que $y*x = x*y$, es decir $*$ es conmutativo por lo que G es grupo abeliano.

P2. Sea $(G, *)$ una estructura asociativa, con neutro y tal que todos sus elementos son invertibles (a esto le llamaremos grupo).

a) Demuestre que cada fila y cada columna de la tabla de multiplicación de $(G, *)$ posee cada elemento de G una única vez.

b) Complete las siguientes tablas de multiplicación asumiendo que son la tabla de multiplicación de una estructura asociativa, con neutro y tal que todos sus elementos son invertibles.

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

$*$	p	q	r	s	t	u
p			q			
q	r					
r					r	
s		p				
t						
u	t					p

Solución 2.

a) *Supongamos que se repitiese un elemento en alguna fila, esto es:*

$*$	$\cdots$	a	$\cdots$	b	$\cdots$
$\vdots$		$\vdots$		$\vdots$	
c	$\cdots$	d	$\ldots$	d	$\cdots$
$\vdots$		$\vdots$		$\vdots$	

Con $a \neq b$. Es decir $c * a = d$ y $c * b = d$, luego $c * a = c * b \implies a = b$, lo que es una contradicción. El razonamiento es analogo para las columnas.

b) *Notemos que la tabla nos dice que $a * a = a$, además como es un grupo sabemos que a debe ser el neutro, completando esto:*

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

Notemos que ahora podemos rellenar la tercera fila, pues sólo falta un elemento (usando la regla de la parte a)).

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

Notemos que en la segunda fila debe ir un c y un d, además este c no puede ir en la tercera columna (pues este ya tiene uno), luego debe ir un c en la cuarta y un d en la tercera.

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

Por último completamos las columnas 2, 3 y 4 con la regla de la parte a):

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

Veamos la segunda tabla ahora. Vemos que $r * t = r$, es decir tenemos que t es el neutro.

$*$	p	q	r	s	t	u
p			q		p	
q	r				q	
r					r	
s		p			s	
t	p	q	r	s	t	u
u	t				u	p

Notemos que la única opción para $u? = q$ es que $u * s = q$, pues las otras columnas ya contienen a q. Luego $u * r$ no puede ser r, pues u no es el neutro, tenemos entonces que $u * r = s$ y que $u * q = r$.*

$*$	p	q	r	s	t	u
p			q		p	
q	r				q	
r					r	
s		p			s	
t	p	q	r	s	t	u
u	t	r	s	q	u	p

Notemos que $u * p = t$. Así que u y p son inversas unas de otras. Esto implica que $p * u = t$. Esto nos permite llenar la última columna, tal como hicimos antes con la última fila.

$*$	p	q	r	s	t	u
p			q		p	t
q	r				q	s
r					r	q
s		p			s	r
t	p	q	r	s	t	u
u	t	r	s	q	u	p

Ahora, como p y u son inversea, $u * s = q \implies p * u * s = p * q \implies s = p * q$. Aplicando esto podemos rellenar la primera fila y la primer columna (aplicando la regla de la parte a))

$*$	p	q	r	s	t	u
p	u	s	q	r	p	t
q	r				q	s
r	s				r	q
s	q	p			s	r
t	p	q	r	s	t	u
u	t	r	s	q	u	p

Tenemos que q es su propia inversa, pues $p * q = s \implies p = s * q^{-1}$ y $s * q = p$. Es decir $q * q = t$

$*$	p	q	r	s	t	u
p	u	s	q	r	p	t
q	r	t			q	s
r	s	u			r	q
s	q	p			s	r
t	p	q	r	s	t	u
u	t	r	s	q	u	p

$r = q * p \implies q * r = p$, *pues q es su propia inversa.*

$*$	p	q	r	s	t	u
p	u	s	q	r	p	t
q	r	t	p		q	s
r	s	u			r	q
s	q	p			s	r
t	p	q	r	s	t	u
u	t	r	s	q	u	p

De esto podemos rellenar el resto de la tabla con la propiedad de la parte a).

$*$	p	q	r	s	t	u
p	u	s	q	r	p	t
q	r	t	p	u	q	s
r	s	u	t	p	r	q
s	q	p	u	t	s	r
t	p	q	r	s	t	u
u	t	r	s	q	u	p

P3. Considere $(\mathbb{Z}_5, \cdot_5)$

a) Construya la tabla para la operación $\cdot_5$ en $\mathbb{Z}_5$

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

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

Solución 3.

a*) Notemos que* $\mathbb{Z}_5$ *tiene 5 elementos* $\{0, 1, 2, 3, 4\}$ *ya que* $5 \equiv_5 0$. *Donde ocupamos que*

$$x \equiv_5 y \iff y - x = 5k,\ k \in \mathbb{Z}$$

Para la tabla de la operación $\cdot_5$ *primero sigamos la lógica de la multiplicación usual.*

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	6	8
3	0	3	6	9	12
4	0	4	9	12	16

Ahora sobre esta tabla, ocupemos modulo congruencia 5 sobre los elementos, es decir, en vez de poner 6 *pondremos* 1 *ya que* $6 - 1 = 5 \iff 6 \equiv_5 1$. *y lo mismo para los otros elementos.*

$\cdot_5$	[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 es grupo ya que si bien es asociativo y el* [1] *es neutro, no todos los elementos son invertibles, por ejemplo* [0] *no es invertible ya que no hay ningún elemento en* $\mathbb{Z}_5$ *que al multiplicarse con* [0] *de* [1]

c*) Para ver que* $(\mathbb{Z}_5 \setminus \{[0]\}, \cdot_5)$ *es grupo abeliano veremos su tabla de multiplicación.*

$\cdot_5$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

Notar que es asociativa pues esto se hereda de la asociatividad de $(\mathbb{Z}_5, \cdot_5)$, *es decir, como* $(\mathbb{Z}_5, \cdot_5)$ *es asociativo también lo será cualquier subconjunto de* $\mathbb{Z}_5$ *dotado del mismo operador. Además, por la tabla el neutro es* [1] *y como la tabla es simetrica con respecto a la diagonal se tiene que es conmutativo. Por ultimo, notemos que el inverso de* [1] *es si mismo. El de* [2] *es* [3] *ya que* $[2] \cdot_5 [3] = [1]$. *El de* [3] *es* [2] *(mismo argumento anterior), y por ultimo el inverso de* [4] *es si mismo, ya que por la tabla* $[4] \cdot_5 [4] = [1]$.

Por todo lo anterior se tiene que $(\mathbb{Z}_5 \setminus \{[0]\}, \cdot_5)$ *es asociativo, tiene neutro, todos sus elementos son invertibles y además es conmutativo, es decir,* $(\mathbb{Z}_5 \setminus \{[0]\}, \cdot_5)$ *es un grupo abeliano.*

P4. Considere $\mathbb{Z}_2 \times \mathbb{Z}_3$ con la operación $\oplus$ definida por

$$(a, b) \oplus (c, d) = (a +_2 c, b +_3 d)$$

a) Pruebe que $(\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$ es una estructura algebraica, asociativa, que tiene neutro y que todos sus elementos son invertibles.

b) Construya un isomorfismo $f : (\mathbb{Z}_6, +_6) \to (\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$ tal que $f([1]_6) = ([1]_2, [1]_3)$. Concluya que es único.

Solución 4.

a*) Vamos paso por paso*

- *Veamos que es una estructura algebraica, es decir, que $\oplus$ es lci. En efecto, sea $([a]_2, [b]_3), ([c]_2, [d]_3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ arbitrarios, entonces $([a]_2, [b]_3) \oplus ([c]_2, [d]_3) = ([a]_2 +_2 [c]_2, [b]_3 +_3 [d]_3) = ([a + c]_2, [b + d]_3)$. Y este ultimo pertenece a $\mathbb{Z}_2 \times \mathbb{Z}_3$ pues $a + c$ y $b + d$ son enteros y $[a + c]_2 \in Z_2$ y $[b + d]_3 \in Z_3$. De ahora en adelanto solo ocuparemos que*

$$([a]_2, [b]_3) \oplus ([c]_2, [d]_3) = ([a + c]_2, [b + d]_3)$$

  Para ahorrarnos trabajo.
- *Veamos que es asociativa. En efecto, sea $([a]_2, [b]_3), ([c]_2, [d]_3), ([e]_2, [f]_3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ arbitrarios. Entonces*

$$\begin{aligned}
[([a]_2, [b]_3) \oplus ([c]_2, [d]_3)] \oplus ([e]_2, [f]_3) &= ([a + c]_2, [b + d]_3) \oplus ([e]_2, [f]_3) \\
&= ([(a + c) + e]_2, [(b + d) + f]_3) \\
&= ([a + (c + e)]_2, [b + (d + f)]_3) \\
&= ([a]_2, [b]_3) \oplus ([c + e]_2, [d + f]_3) \\
&= ([a]_2, [b]_3) \oplus [([c]_2, [d]_3) \oplus ([e]_2, [f]_3)]
\end{aligned}$$

  Por lo tanto es asociativa
- *En virtud de la definición de $\oplus$ defino, por inspección, mi candidato a ser neutro como $([0]_2, [0]_3)$. Ya que, si $([a]_2, [b]_3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ entonces*

$$([a]_2, [b]_3) \oplus ([0]_2, [0]_3) = ([a + 0]_2, [b + 0]_3) = ([a]_2, [b]_3)$$

  y por otro lado

$$([0]_2, [0]_3) \oplus ([a]_2, [b]_3) = ([0 + a]_2, [0 + b]_3) = ([a]_2, [b]_3)$$

  Por lo tanto $([0]_2, [0]_3)$ es neutro para $\oplus$
- *Veamos que todos sus elementos son invertibles. Para esto veremos que siempre es posible encontrar un inverso dado cualquier elemento en $(\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$.*
  En efecto, sea el par $([a]_2, [b]_3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ arbitrario, defino mi candidato a ser inverso como $([-a]_2, [-b]_3)$ que claramente vive en $\mathbb{Z}_2 \times \mathbb{Z}_3$ pues como $a, b \in \mathbb{Z}$ entonces sus inversos aditivos tambien.
  Luego, $([a]_2, [b]_3) \oplus ([-a]_2, [-b]_3) = ([a + (-a)]_2, [b + (-b)]_3) = ([0]_2, [0]_3)$
  Y por otro lado, $([-a]_2, [-b]_3) \oplus ([a]_2, [b]_3) = ([(-a) + a]_2, [(-b) + b]_3) = ([0]_2, [0]_3)$
  Como $([a]_2, [b]_3)$ fueron arbitrarios, se tiene que cualquier elemento de la estructura es invertible. y su forma es $([-a]_2, [-b]_3)$.

b*) Primero que todo queremos un morfismo $f : (\mathbb{Z}_6, +_6) \to (\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$ tal que $f([1]_6) = ([1]_2, [1]_3)$. En efecto, como sabemos que los neutros se corresponden entre las estructuras podemos decir que $f([0]_6) = ([0]_2, [0]_3)$. Ahora nos faltan los otros elementos del dominio, considerando $Z_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$. Ahora notando que $f([2]_6) = f([1]_6 +_6 [1]_6)$ y como queremos que f sea morfismo, podemos imponer que $f([1]_6 +_6 [1]_6) = f([1]_6) \oplus f([1]_6)$ y esto ultimo es enunciado es igual a $([1]_2, [1]_3)$. Entonces*

$$f([2]_6) = f([1]_6 +_6 [1]_6) = f([1]_6) \oplus f([1]_6) = ([1]_2, [1]_3) \oplus ([1]_2, [1]_3) = ([2]_2, [2]_3) = ([0]_2, [2]_3)$$

Donde se ocupo que $[2]_2 = [0]_2$.

Resumiendo, tenemos hasta el momento lo siguiente

- $f([0]_6) = ([0]_2, [0]_3) \rightarrow$ *Por correspondencia de neutros*
- $f([1]_6) = ([1]_2, [1]_3) \rightarrow$ *Por enunciado.*
- $f([2]_6) = ([0]_2, [2]_3) \rightarrow$ *Debido a que* $[2]_6 = [1]_6 +_6 [1]_6$

Siguiendo con el argumento de imponer que sea morfismo, podemos decir que

$$f([3]_6) = f([2]_6 + [1]_6) = f([2]_6) \oplus f([1]_6) = ([0]_2, [2]_3) \oplus ([1]_2, [1]_3) = ([1]_2, [3]_3) = ([1]_2, [0]_3)$$

Del mismo modo podemos concluir que $f([4]_6) = ([0]_2, [1]_3)$ *y* $f([5]_6) = ([1]_2, [2]_3)$

Finalmente, por construcción podemos decir que f *es único (ya que solo hay una unica manera de asignar los valores segun nuestra lógica). Ahora hay que ver si* f *es morfismo y que es biyectivo. Primero veamos que es biyectivo haciendo un resumen de todas las imagenes que generamos.*

- $f([0]_6) = ([0]_2, [0]_3)$
- $f([1]_6) = ([1]_2, [1]_3)$
- $f([2]_6) = ([0]_2, [2]_3) = ([2]_2, [2]_3)$
- $f([3]_6) = ([1]_2, [0]_3) = ([3]_2, [3]_3)$
- $f([4]_6) = ([0]_2, [1]_3) = ([4]_2, [4]_3)$
- $f([5]_6) = ([1]_2, [2]_3) = ([5]_2, [5]_3)$

Es decir, podemos notar que $f([n]) = ([n]_2, [n]_3)$ *(verifiquelo dandose números). Luego, cada imagen tiene una unica preimagen y cada elemento del codominio es alcanzado por alguna preimagen. Por lo tanto es biyectiva (ojo que este tipo de razonamiento solo lo podemos hacer porque hay una cantidad muy pequeña de elementos).*

Falta ver que es morfismo, pero por como lo construimos esto esta garantizado. De todas formas podemos probarlo:

$$f([n]_6 +_6 [m]_6) = f([n+m]_6) = ([n+m]_2, [n+m]_3) = ([n]_2, [n]_3) \oplus ([m]_2, [m]_3) = f([n]_6) \oplus f([m]_6)$$

Finalmente, como es morfismo y es biyectivo se tiene que es isomorfismo.