#Estructuras/Practico, #Estructuras

5) Son la misma tabla

3) contraejemplo

1) a) $(G, *)$ $\quad a * b = a^b \quad a, b \in \mathbb{R}_{>0}$

I) $(a \cdot b)c = (a^b)^c \neq a^{(b^c)} = a(b \cdot c)$

$\Rightarrow G$ no es semigrupo

b) $G = \mathbb{Z} \times \mathbb{Z} \quad (m, n) \cdot (r, s) = (m + (-1)^n r, n + s)$

$((a_1, b_1)(a_2, b_2))(a_3, b_3) = (a_1 + (-1)^{b_1} a_2, b_1 + b_2)(a_3, b_3)$

paja

c)

2) d) •) los complejos son son asociativos en particular las raíces lo son

•) $e_{G_n} = 1$, $1 = e^{\frac{2k\pi i}{n}}$ con $k = 0$

$\Rightarrow 1 \in G_n$

•) Sea $z \in G_n \Rightarrow z = e^{\frac{2k\pi i}{n}}$

$\Rightarrow z^{-1} = e^{-\frac{2k\pi i}{n}}$ trivial

$\Rightarrow$ por teorema G_n grupo

e) Sale igual

$z \in \bigcup G_n \Rightarrow z \in G_n \Rightarrow \exists z^{-1}$

y 1 inverso

3) b) La recíproca vale por 3) a) dado $a \in G$

$L_a(x)$ biyectiva

$\Rightarrow ax = c$ tiene sol

$L_a(x) = e$

Análogo $R_a(x) \Rightarrow G$ grupo (por 3) a))

Ahora queremos ver 3) b) $\Rightarrow L_a$ y R_a biyectiva

•) inyectiva sale directo de la ley cancelativa

•) sobre $|G| = n \Rightarrow G = \{a_1, \dots, a_n\}$

como L_{a_j} inyectiva

$\Rightarrow L_{a_j}(a_n) \neq L_{a_j}(a_m) \ \forall n \neq m$

Sea $A = \{L_{a_j}(a_1), \dots, L_{a_j}(a_n)\}$

$A \subseteq G$ y $|A| = n = |G| \Rightarrow A = G$

Supongo $\exists a_j \ / \ L_{a_j}$ no es sobre

$\Rightarrow \exists a_k \ / \ L_{a_j}(x) \neq a_k$

$\Rightarrow L_{a_j}(a_i) \neq a_k \quad \forall i = 1, \dots, n$

$\Rightarrow a_n \in A \Rightarrow a_n \notin A$ abs!

$\Rightarrow$ La_i es sobre $\forall i < 1, \ldots n$

No vale con infinito

$(\mathbb{N}, +)$ es semigrupo infinito

·) si $n+a = n+b \Rightarrow a=b$

supongo $a \neq b \Rightarrow n+a \neq n+b$

4) ($\Rightarrow$) Sea $\mathbb{Z}_n^*$. $(\mathbb{Z}_n^* = \{1, \ldots n-1\})$

supongo n no primo

$\Rightarrow n = p_1 \cdot p_2$ primos $p_1 < n$
$p_2 < n$

$\Rightarrow p_1, p_2 \in \mathbb{Z}_n^*$

pero $p_1 \cdot p_2 \notin \mathbb{Z}_n^*$

$\Rightarrow$ · no es cerrada

$\Rightarrow$ No es grupo absurdo

($\Leftarrow$) Sea p primo $\Rightarrow$ $\mathbb{Z}_p$ (la operación es $a * b = r_p(a \cdot b)$)

·) cumple asoc (siempre)

·) 1 es neutro

Sea $a \in \mathbb{Z}_p^*$ $\Rightarrow$ $a \perp p$ por p primo y $a < p$, $a \neq 0$

$\Leftrightarrow$ $ax \equiv 1 \ (p)$ tiene sol

5)

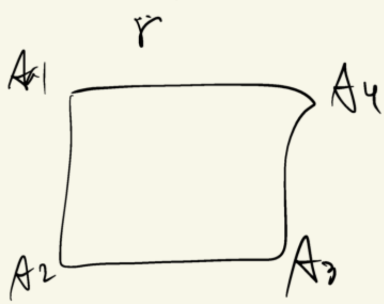
	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

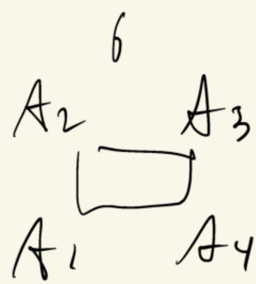
	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

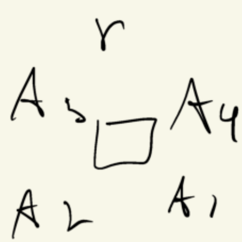
no son isomorfos

6)

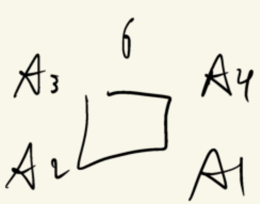
	r	r^2	r^3	r^4	$r\circ\sigma$	$r^2\circ\sigma$	$r^3\circ\sigma$	$r^4\circ\sigma$
r	r^2							
r^2	r^3							
r^3	e							
r^4	r^1							
$r\circ\sigma$	σ							
$r^2\circ\sigma$	$r\circ\sigma$							
$r^3\circ\sigma$	$r^2\circ\sigma$							
$r^4\circ\sigma$	$r^3\circ\sigma$							







$r\circ\sigma\circ r$ $\rightarrow$



$\Rightarrow \sigma = r\circ\sigma\circ r$

7) $GL(2,\mathbb{Z}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$

$|GL(2,\mathbb{Z}_2)| = (2^2-1)(2^2-2) = 3 \cdot 2 = 6$

La tabla de fiaca pero notar

$GL(2,\mathbb{Z}_2) = SL(2,\mathbb{Z}_2)$ asique sus

Tablas serán identicas

⇒ también cancelativa ⇒ no se pueden repetir

1ero deducir e identidad

8)

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

$da = e$

$\Rightarrow ad = e$

⇒) porq no se puede repetir en Fila

si pusiera

⇒ iría c ab!

9) a) $a = a^{-1} \iff a^2 = e$

$(\Rightarrow)$ $a^2 = a \cdot a = a \cdot a^{-1} = e$

$(\Leftarrow)$ $a^2 = e \Rightarrow a \cdot a = e \Rightarrow a = a^{-1}$

b) $a^m = a^n \Rightarrow m = n$

$(\Rightarrow)$ No vale ejemplo $(\mathbb{Z}_4, \cdot) \Rightarrow 2^2 = 0 = 8 = 2^3$

c) $(ab)^{-1} = a^{-1}b^{-1} \Leftrightarrow ab = ba$

$(\Leftarrow)$ $(ab)^{-1} = (ba)^{-1}$ pero $(ba)^{-1} = a^{-1}b^{-1}$

pq $ba\,a^{-1}b^{-1} = beb^{-1} = bb^{-1} = e$

$(\Rightarrow)$ $(ab)^{-1} = a^{-1}b^{-1} \Rightarrow ab\,a^{-1}b^{-1} = e$

$\Rightarrow aba^{-1} = b$ (opero por b a derecha)

$ab = ba$

10) •) $a^2 = e \Rightarrow a = a^{-1}$

•) $e = (ab)^2 = abab \Rightarrow a^{-1} = bab \Rightarrow b^{-1}a^{-1} = ab$

$\begin{pmatrix} a = a^{-1} \\ b = b^{-1} \end{pmatrix} \Rightarrow ba = ab$

11) Supongo cada $a \in G$ / $a \neq e$ tiene inverso distinto que a $\Rightarrow G - \{e\}$ tiene $2n$ elementos

lo que es $a^2 \neq e$

$\Rightarrow G$ tiene $2n+1$ $\underline{\text{abs!}}$

b) $\cdot$) G abeliano $\Rightarrow$ $(ab)^2 = a^2b^2$

$$(ab)^2 = abab \overset{\text{abel}}{=} abba = ab^2a \overset{\text{abel}}{=} a \cdot a \cdot b^2 = a^2b^2$$

$\cdot$) $(ab)^2 = a^2b^2 \to (ab)^{-1} = a^{-1}b^{-1}$

$\hookrightarrow \quad abab = a^2b^2$

$bab = a^{-1}aa \cdot b^2$

$ba = ab$ por 9) c) ($\Leftarrow$) Lo probé

$(ab)^{-1} = a^{-1}b^{-1}$

$\cdot$) $(ab)^{-1} = a^{-1}b^{-1} \Rightarrow (ab)^n = a^nb^n \quad \forall n \in \mathbb{Z} \quad \forall a,b \in G$

$$(ab)^{-1} = a^{-1}b^{-1} \overset{9)c)}{\Rightarrow} ab = ba$$

$$(ab)^n = \overbrace{(ab)(ab) \cdots (ab)}^{n\text{-veces}}$$

$$= a(bb)a \cdots (ab)$$

$$= ab^2a \cdots ab$$

$$= a^2b^2 \underbrace{\cdots ab}_{n-2 \text{ veces}}$$

(inducción)

$$= a^2b^2 \, a^{n-2}b^{n-2} = a^nb^n$$

·) $(ab)^n = a^n b^n \Rightarrow (ab)^n = (ab)^n$ para tres enteros consecutivos

$\forall a, b \in G$

·) Si vale $\forall n \in \mathbb{Z}$ en particular vale para tres enteros consecutivos

·)

$$(ab)^n = \underbrace{ab \ldots ab}_{n}$$

$$= a^n b^n = a \ldots \overbrace{a b \ldots b}^{n-1}$$

$$ba \ldots ab = \overbrace{a - a}b \ldots b$$

$$\underbrace{ba - ba}_{n-1} = a \ldots a \overbrace{b - b}^{n-1}$$

$$(ba)^{n-1} = \underbrace{ab \ldots ab}_{n-1}$$

$$(ab)^{n-1}$$

$$(ab)^{n-2} = b^{-1}(ab)^{n-1}a^{-1}$$

13) I) $\frac{a}{b} + \frac{c}{d} = \frac{da+cb}{db}$ qvq $bd \perp p$

$b \perp p$ $d \perp p$ p primo trivial si no lo fuera

$\exists p_0$ primo / $p_0 | p \Rightarrow p_0 = p$

$p_0 | bd \Rightarrow p | bd = p_1 \dots p_n$

$\Rightarrow p | p_j \wedge (p_j | b \vee p_j | d)$

abs!

Asoc e inversa vale pq $\mathbb{Q}$ grupo

.) 0 es neutro $(0 = \frac{0}{b}$ con $b \perp p)$

$\Rightarrow 0 \in R_p$

II) qvq $bd = p^i$ pero $b = p^{i_1}$ $d = p^{i_2}$

$\Rightarrow bd = p^{i_1+i_2}$

.) Asoc e inversa lo mismo

.) 0 neutro $0 = \frac{0}{p^i}$ para cualquier $i \geq 0$

$\Rightarrow 0 \in R^p$

14)

Caso base trivial

Supongo vale $a^{r^n} = b^n a b^{-n}$ qvq $a^{r^{n+1}} = b^{n+1} a b^{-n-1}$

$$a^{r^{n+1}} = (a^{r^n})^r = (b^n a b^{-n})^r$$
$$= b^n a^r b^{-n} = b^n b a b^{-1} b^{-n}$$
$$= b^{n+1} a b^{-n-1}$$