Resolución Aux #12

P1 a) Por contradicción. Supongamos que hay un elemento que aparece 2 veces en una fila. Por ejemplo

*	a	b	c	d	e	...
a						
b						
c		g		g		
d						
e						
⋮						

OJO, esto es sencillamente un ejemplo, en el caso general se usará "x,y,z,w".

se puede hacer la siguiente comparación
1) x=c (pues representa la fila)
2) y=b (pues representa una columna)
3) z=e (pues representa otra columna distinta)
4) w=g (ya que representa el valor

Luego si se repite un elemento en una fila
$\Rightarrow \exists x, y, z, w \in G$ con $y \neq z$ tq

$$x * y = g \quad \wedge \quad x * z = g$$

donde x representa la fila

$\Rightarrow$ $x * y = x * z$) G es grupo todos sus elementos son cancelables

$\Rightarrow$ $y = z$

$\Rightarrow\Leftarrow$

Luego la tabla de G posee un unico elemento de G por cada fila.
Para las columnas lo mismo.

↳ $a*a=a$ / $b*b=a$ / $c*b=d$ / $c*d=b$

b)

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

fila1 fila2 fila3 fila4

Notemos que $a*a=a$
$\Rightarrow$ a es idempotente $\Rightarrow$ a es neutro ya que el unico elemento idempotente es el neutro (en grupo)

$\Rightarrow$

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

Ahora por (a), cada fila y columna debe tener una unica vez los elementos de G
$\Rightarrow d*b=c$ y $c*c=a$

$\Rightarrow$

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

Notemos que en la fila 2, faltan c y d. Por lo que rellenando usando la parte (a) se obtiene que $b*c=d$ y $b*d=c$

$\Rightarrow$

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

Finalmente concluimos por (a)

$\Rightarrow$

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

obs: $*$ resulto ser conmutativo !!

Continuación

b)

Δ	p	q	r	s	t	u
p			q			
q	r					
r				r		
s		p				
t						
u	t				p	

Notemos que

$$r * t = r \quad / r^{-1} *$$

$$\Rightarrow (r^{-1} * r) * t = (r^{-1} * r)$$

$$\Rightarrow e * t = e$$

$$\Rightarrow t = e$$

Luego t es el neutro

Δ	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

Veamos la fila de u. faltan 3 espacios. De los cuales los dos primeros pertenecen a columnas que ya tienen q. Luego por la parte (a).

Δ	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			q	u	p

Luego estamos en condiciones para completar la fila de "u". ya que falta poner "r" pero una columna ya lo tiene

Ojo! Todos los $*$ deberían ser Δ de aquí en adelante

$\Rightarrow$

Δ	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 $u * p = t$ donde t es el neutro.

$\Rightarrow \quad u * p = t \quad / * p^{-1}$

$\rightarrow \quad u * (p * p^{-1}) = p^{-1}$

$\Rightarrow \quad u * t = p^{-1}$

$\Rightarrow \quad u = p^{-1}$

$\Rightarrow \quad p * u = t$

$\Rightarrow$

Δ	p	q	r	s	t	u
p			q		p	t
q	r				q	
r					r	
s		p			s	
t	p	q	r	s	t	u
u	t	r	s	q	u	p

Por (a) seguimos rellenando.

$s * u = r$

$\Rightarrow \quad r * u = q$

$\Rightarrow \quad q * u = s$

Además $u * p = t \quad / u *$

$\Rightarrow \quad (u * u) * p = u * t$

$\Rightarrow \quad p * p = u$

$\Rightarrow$

Δ	p	q	r	s	t	u
p	u		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

Seguimos rellenando ... y seguimos y seguimos

Completemos la fila 1 y columna 1.

Δ	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

Notemos que

$p * q = s \Rightarrow p = s * q^{-1}$ (1)

pero $p = s * q$ (2)

$\Rightarrow s * q = s * q^{-1}$

$\Rightarrow q = q^{-1}$

$\Rightarrow q * q = e$

o

Δ	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

$r = q * p \quad / q *$

$\Rightarrow q * r = q * q * p$

$\Rightarrow q * r = p$

$\Rightarrow q * s = u$ pues es la última opción

Δ	p	q	r	s	t	u
p	u	s	q	r	p	t
q	r	t	p	u	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

$\Rightarrow$ De aquí

$s * r = u$ ya que en la fila de r y la columna de s ya está

y con esto completamos

Δ	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

$\Rightarrow$

obs: No es ABELIANO

P2 $(G, *)$ grupo abeliano, $H, K \leq G$ subgrupos

pdq: $H * K = \{h * k : h \in H, k \in K\}$ es subgrupo

En efecto. Usemos la caracterización (Def compacta) la cual es

(A, Δ) es subgrupo de $(B, \Delta) \iff$ (i) $A \neq \emptyset$
(ii) $A \subseteq B$
(iii) $\forall x, y \in A \quad x \Delta y^{-1} \in A$

Entonces probemos (i), (ii) y (iii)

(i) pdq $H * K \neq \emptyset$

En efecto, por definición un subgrupo es $\neq \emptyset$

$\Rightarrow$ Como H es subgrupo $\rightarrow$ $H \neq \emptyset \rightarrow \exists h \in H$
Análogamente $\exists k \in K$

$\Rightarrow$ $h * k \in H$ donde $h \in H$, $k \in K$

obs: tambien pueden ver de que el neutro de G esta en $H * K$

(ii) pdq $H * K \subseteq G$

En efecto, Sea $a \in H * K$ arbitrario tratemos de probar que $a \in G$

$\Rightarrow$ Como $a \in H * K \Rightarrow \exists h \in H$ y $\exists k \in K$ tq $a = h * k$

Ahora como $h \in H$ y $H \subseteq G$ (pues H es Subgrupo de G)

$\Rightarrow h \in G$, del mismo modo se tiene que

$\Rightarrow k \in G$ pues $K \subseteq G$

Luego como $*$ es Lc: en G

$\Rightarrow a = h * k \in G$ pues $h, k \in G$

Es decir, tenemos que

$a \in H * K \Rightarrow a \in G$

iii) pdq $(\forall a,b \in H*K)\ a*b^{-1} \in H*K$

En efecto, sea $a,b \in H*K$ arbitrarios

Como $a \in H*K \Rightarrow a = h_1 * k_1$ $\quad h_1 \in H,\ k_1 \in K$

y $b \in H*K \Rightarrow b = h_2 * k_2$ $\quad h_2 \in H,\ k_2 \in K$

(Por definición del ejto)

Debemos probar que $a*b^{-1} = (h_1*k_1)*(h_2*k_2)^{-1}$ pertenece a $H*K$.

Primero notemos que hablar de $(h_2*k_2)^{-1}$ tiene sentido pues $h_2, k_2 \in G$ y por ende poseen inversos. Luego es directo que

$$(h_1*k_1)*(h_2*k_2)^{-1} \in G$$

Pues $(G,*)$ es grupo

Ahora sí! probemos que $a*b^{-1} \in H*K$

En efecto, $a*b^{-1} = (h_1*k_1)*(h_2*k_2)^{-1}$

$= (h_1*k_1)*(k_2^{-1}*h_2^{-1})$) Conmuto y Asocio Pues estoy en G grupo abeliano

$= (h_1*h_2^{-1})*(k_1*k_2^{-1})$

$\in H \qquad \in K$

PROARTES $\Rightarrow a*b^{-1} \in H$ pues $h_1*h_2^{-1} \in H$ ya que H es grupo

y $k_1*k_2^{-1} \in K$ " " K " "

$\therefore (H * K, *)$ es subgrupo de $(G, *)$

P3 Sea $(G, *)$ grupo con $|G| = 4$ con neutro e

pdq $\forall a \in G \setminus \{e\}$ $a^3 \neq e$

Por contradicción, $\exists a \in G \setminus \{e\}$ tal que

$$a^3 = e$$

Podemos concluir muchas cosas

1) $a \neq e$ ya que $a \in G \setminus \{e\}$

2) $a^2 \neq a$ ya que si esto no fuera así

$a^2 = a$ $/ * a^{-1}$ a^{-1} existe pues $a \in G$ y $(G, *)$ es grupo

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

$\Rightarrow a * e = e \Rightarrow a = e$ $\Rightarrow\Leftarrow$ ya que por (1) $a \neq e$

$\Rightarrow a^2 \neq a$

3) $a^2 \neq e$, ya que si esto no fuera así:

$a^2 \neq e \quad / * a$

$\Rightarrow a^3 = a$, pero por hipotesis

$a^3 = e \quad$ y $\quad a \neq e \quad \Rightarrow\Leftarrow$

$\Rightarrow a^2 \neq e$

$\Rightarrow$ el cjto $H = \{e, a, a^2\}$ dotado con la Ley $*$ es grupo

y como $e, a, a^2 \in G \Rightarrow H$ es subgrupo de G

pero... $|H| = 3$ y $|G| = 4$

lo que contradice al teo de Lagrange

pues 3 no divide a 4

$\Rightarrow\Leftarrow$

$\therefore \forall a \in G \setminus \{e\} \; a^3 \neq e \quad (a^3 = a * a * a)$

OBS: ***H*** es grupo ya que
1) hay neutro que es "e"
2) es asociativo por herencia del grupo ***G*** *(compruebelo)*
3) hay inverso de todos los elementos, $e^{-1}=e$ y $a^{-1}=a^2$

P4 $(A,+,\cdot)$ Anillo booleano $a^2=a \quad \forall a\in A$

a) pdq $\forall x\in A \quad x=-x$

En efecto, esto es equivalente a probar que

$$\forall x\in A \quad x+x=0$$

probemos esto último, sea $x\in A$

$\Rightarrow 2x=(x+x)\in A$ pues $(A,+)$ es grupo

$\Rightarrow (x+x)=(x+x)^2$ ya que $\forall a\in A\ a^2=a$

$= x^2+x^2+x^2+x^2$ ↘ Distribución

$= x+x+x+x$ ↘ $\forall a\in A\ a^2=a$

$\Rightarrow x+x=x+x+x+x \quad /+(-x)+(-x)$

$\Rightarrow 0=x+x \iff -x=x$ ∎

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

probemos que $\cdot$ es conmutativo

es decir, pdq $\forall x,y \in A,\ x\cdot y = y\cdot x$

En efecto, sea $x, y \in A$

$\Rightarrow (x^2 + y^2) = (x+y) = (x+y)^2$

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

$\Rightarrow x^2+y^2 = x^2 + xy + yx + y^2$

$x^2, y^2 \in A$ son cancelables

$\Rightarrow 0 = xy + yx$

$\rightarrow xy = -yx = (-y)x = yx$ ya que $-y = y$ por (a)

$\Rightarrow xy = yx$

$\therefore (A,+,\cdot)$ es conmutativo

Pda

c) $\forall x,y \in A \quad xy(x+y) = 0$

Sea $x, y \in A$ arbitrarios

$\Rightarrow xy(x+y) = xyx + xy^2$ / Distribución

$= x^2y + xy^2$ / Conmuto

$= xy + xy$ / $\forall a \in A \; a^2 = a$

$= xy + (-x)y$ / por (a)

$= xy - xy$

$= 0$ ∎

d) Sea $(A, +, \cdot)$ anillo booleano de 3 elementos

- Si no tiene unidad, inmediatamente no es dominio de integridad
- Si tiene unidad

$\Rightarrow A = \{0, 1, a\}$ con $a \neq 0$, $a \neq 1$ donde 0 es el neutro de $+$ y 1 es el neutro de $\cdot$.

Ahora como $a \in A$ y $(A, +, \cdot)$ es booleano

$\Rightarrow \quad a^2 = a$

$\Rightarrow \quad a^2 - a = 0$

$\Rightarrow \quad a(a-1) = 0$ pero $a \neq 0$ y $a \neq 1$

$\Rightarrow$ a es divisor del cero

y un dominio de integridad no los tiene