Problema 2:

Considere el conjunto $\mathbb{Z}_2 \times \mathbb{Z}_2$ con las operaciones

$$(a,b) + (c,d) = (a+c, b+d)$$
$$(a,b) \cdot (c,d) = (a \cdot c, b \cdot d),$$

donde $+$ y $\cdot$ son la suma y la multiplicación usual en $\mathbb{Z}_2$.

Definamos también la operación

$$(a,b) * (c,d) = (a \cdot c + b \cdot d, a \cdot b + b \cdot c + b \cdot d).$$

Usando el hecho de que $(\mathbb{Z}_2, +, \cdot)$ es un cuerpo pruebe que:

a) $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$ es un anillo conmutativo y con unidad ¿Es un cuerpo? Justifique su respuesta.

(2 ptos.)

b) $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, *)$ es un cuerpo.

(2 ptos.)

c) Pruebe que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, *)$ no es isomorfo a $(\mathbb{Z}_4, +, \cdot)$, es decir, no existe ningun morfismo biyectivo entre $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, *)$ y $(\mathbb{Z}_4, +, \cdot)$.

(2 ptos.)

Solución:

a) En primer lugar veamos que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$ es un anillo conmutativo con unidad. En efecto:

Veamos que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ es un grupo Abeliano.

Sean $(a,b),(c,d),(e,f) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, es claro que $+$ y $\cdot$ son l. c. i. para $\mathbb{Z}_2 \times \mathbb{Z}_2$ ya que $(\mathbb{Z}_2, +, \cdot)$ es un cuerpo y cada componente de la suma y la multiplicación son combinaciones y productos de elementos de $\mathbb{Z}_2$.

En primer lugar podemos ver que $+$ y $\cdot$ son operaciones conmutativas, en efecto

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d) && \text{def. de la suma} \\ &= (c+a, d+b) && \text{conmutatividad de } + \text{ en } \mathbb{Z}_2 \\ &= (c,d) + (a,b) && \text{def. de la suma} \end{aligned}$$

y además

$$\begin{aligned} (a,b) \cdot (c,d) &= (a \cdot c, b \cdot d) && \text{def. del producto} \\ &= (c \cdot a, d \cdot b) && \text{conmutatividad de } \cdot \text{ en } \mathbb{Z}_2 \\ &= (c,d) \cdot (a,b) && \text{def. del producto} \end{aligned}$$

Además, si 0 es el neutro aditivo de $(\mathbb{Z}_2, +)$ entonces $(0,0)$ es el neutro aditivo de $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, en efecto

$$\begin{aligned} (a,b) + (0,0) &= (a+0, b+0) && \text{def. de la suma} \\ &= (a,b) && 0 \text{ es neutro aditivo } + \text{ en } \mathbb{Z}_2, \end{aligned}$$

y dado que $+$ es conmutativo, se completa la demostración.

Por otra parte, si dado $a \in \mathbb{Z}_2$ entonces existe $-a \in \mathbb{Z}_2$ el inverso aditivo de a. Así dado $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces $(-a,-b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ es el inverso aditivo de (a,b). En efecto,

$$\begin{aligned} (a,b) + (-a,-b) &= (a + (-a), b + (-b)) && \text{def. de la suma} \\ &= (0,0) && -a, -b \text{ son los inversos aditivos } + \text{ en } \mathbb{Z}_2 \end{aligned}$$

Finalmente nos queda ver la asociatividad,luego

$$\begin{aligned} (a,b) + ((c,d) + (e,f)) &= (a,b) + (c+e, d+f) && \text{def. de la suma} \\ &= (a + (c+e), b + (d+f)) && \text{def. de la suma} \\ &= ((a+c) + e, (b+d) + b) && \text{asociatividad de } + \text{ en } \mathbb{Z}_2 \\ &= (a+c, b+d) + (e,f) && \text{def. de la suma} \\ &= ((a,b) + (c,d)) + (e,f) && \text{def. de la suma} \end{aligned}$$

Lo que prueba que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ es un grupo Abeliano. Por otra parte, si 1 es el neutro multiplicativo de $\cdot$ en $\mathbb{Z}_2$, entonces $(1,1)$ es el inverso multiplicativo de $\cdot$ en $\mathbb{Z}_2 \times \mathbb{Z}_2$, ya que dado $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces

$$\begin{array}{lll} (a,b)\cdot(1,1) & = (a\cdot 1, b\cdot 1) & \text{def. del producto} \\ & = (a,b) & 1 \text{ es neutro de } \cdot \text{ en } \mathbb{Z}_2 \end{array}$$

Veamos la distribituvidad del producto con respecto a la suma. En efecto

$$\begin{array}{lll} (a,b)\cdot((c,d)+(e,f)) & = (a,b)\cdot(c+e,d+f) & \text{def. de } + \\ & = (a\cdot(c+e), b\cdot(d+f)) & \text{def. de } \cdot \\ & = (a\cdot c + a\cdot e, b\cdot d + b\cdot f) & \text{distribitividad en } \mathbb{Z}_2 \\ & = (a\cdot c, b\cdot d) + (a\cdot e, +b\cdot f) & \text{def. de } + \\ & = (a,b)\cdot(c,d) + (a,b)\cdot(e,f) & \text{def. de } \cdot, \end{array}$$

lo que prueba la distributividad.

Así $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$ es un anillo conmutativo con unidad.

Notemos que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$ no es un cuerpo ya que tiene divisores de cero, en efecto

$$(1,0)\cdot(0,1) = (0,0).$$

Otro argumento para mostrar que no es un cuerpo es el hecho que el elemento $(1,0)$ no tiene inverso multiplicativo, en efecto $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces se tiene que

$$(1,0)\cdot(a,b) = (a,0) \neq (a,1) \qquad \forall (a,b).$$

b) De la parte anterior se tiene que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ es un grupo Abeliano. Nos resta probar que

$$(\mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{(0,0)\}, *)$$

es un grupo Abeliano.

En primer lugar podemos ver que $*$ es una ley de composición interna en $\mathbb{Z}_2 \times \mathbb{Z}_2$ ya que sus componentes son sumas y productos de elementos de $\mathbb{Z}_2$ y la suma y la multiplicación son l.c.i. para $\mathbb{Z}_2$, ya que $(\mathbb{Z}_2, +, \cdot)$ es un cuerpo.

Por otra parte podemos ver que $*$ es conmutativa, en efecto sean $(a,b),(c,d) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, luego

$$\begin{array}{lll} (a,b)*(c,d) & = (a\cdot c + b\cdot d, a\cdot d + b\cdot c + b\cdot d) & \text{def. de } * \\ & = (c\cdot a + d\cdot b, d\cdot a + c\cdot b + d\cdot b) & \text{conmutatividad de } \cdot \\ & = (c\cdot a + d\cdot b, c\cdot b + d\cdot a + d\cdot b) & \text{conmutatividad de } + \\ & = (c,d)*(a,b) & \text{def. de } *. \end{array}$$

Por otra parte, $(1,0)$ es el neutro de $*$. En efecto, sea $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, luego

$$\begin{array}{lll} (a,b)*(1,0) & = (a\cdot 1 + b\cdot 0, a\cdot 0 + b\cdot 1 + b\cdot 0) & \text{def. de } * \\ & = (a+0, 0+b+0) & 1 \text{ es neutro mult. y } 0 \text{ es neutro aditivo} \\ & = (a,b) & . \end{array}$$

Veamos que para cada $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{(0,0)\}$, existe un inverso multiplicativo. Podemos notar que

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{(0,0)\} = \{(1,0),(0,1),(1,1)\}$$

y puesto que $(1,0)$ es el neutro para $*$, entonces

$$(1,0)^{-1} = (1,0).$$

Veamos los inversos de $(0,1)$ y $(1,1)$. Como su segunda componente es 1, basta ver el caso $(a,1)$ con $a = 0, 1$.

Si $(c,d) = (a,1)^{-1}$, entonces

$$\begin{array}{lll} (a,1)*(c,d) = (1,0) & \iff (a\cdot c + 1\cdot d, a\cdot d + 1\cdot c + 1\cdot d) = (1,0) & \text{def. } * \\ & \iff (a\cdot c + d, a\cdot d + c + d) = (1,0) & \text{def. } *, \end{array}$$

es decir

$$a \cdot c + d = 1 \qquad a \cdot d + c + d = 0.$$

Luego si $a = 0$, entonces

$$d = 1 \qquad c + d = 0 \quad \Longrightarrow c = d = 1 \Longrightarrow (0,1)^{-1} = (1,1),$$

si $a = 1$ entonces

$$c+d=1 \quad d+c+d=0 \quad \Longrightarrow c+d=1 \quad c+2d=0 \Longrightarrow c+d=1 \quad c=0 \Longrightarrow d=1 \quad c=0 \Longrightarrow (1,1)^{-1} = (0,1).$$

Lo que prueba que cada elemento no nulo tiene inverso para $*$.

Nos resta ver la asociatividad de $*$. En efecto, sean $(a,b),(c,d),(e,f) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces se tiene que

$$(a,b) * [(c,d) * (e,f)] \quad = \ldots$$

Esto prueba que $(\mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{(0,0)\})$ es un grupo Abeliano.

Para probar que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, *)$ basta probar que se tiene la distributividad de $*$ con respecto a $+$, es decir, para todo $(a,b),(c,d),(e,f) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces

$$\begin{array}{lll}
(a,b) * [(c,d) + (e,f)] & = (a,b) * ((c+e, d+f)) & \text{def. } + \text{ y } * \\
& = (a \cdot (c+e) + b \cdot (d+f), a \cdot (d+f) + b \cdot ((c+e) + (d+f))) & \\
& = (a \cdot c + a \cdot e + b \cdot d + b \cdot f, a \cdot d + a \cdot f + b \cdot (c+d) + b \cdot (e+f)) & \text{distrib. en } \mathbb{Z}_2 \\
& = ((a \cdot c + b \cdot d) + (a \cdot e + b \cdot f), (a \cdot d + b \cdot (c+d)) + (a \cdot f + b \cdot (e+f)) & \text{asoc. y conmut. en } \mathbb{Z}_2 \\
& = (a \cdot c + b \cdot d, a \cdot d + b \cdot (c+d)) + (a \cdot e + b \cdot f, a \cdot f + b \cdot (e+f)) & \text{def. } + \\
& = (a,b) * (c,d) + (a,b) * (e,f) & \text{def. } *.
\end{array}$$

Lo que completa la demostración.

c) Notemos que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, *)$ y $(\mathbb{Z}_4, +, \cdot)$ no son isomorfos ya que el primero es un cuerpo y el segundo no lo es ($(\mathbb{Z}_p, +, \cdot)$) es un cuerpo si y sólo si p es un número primo.