MA1101-3 Introdución al Álgebra.
Profesor: Marcos Kiwi.
Auxiliar: Benjamín Jauregui.
Fecha: 15 de agosto de 2018.

Pauta auxiliar 12

Grupos, anillos y cuerpos.

P1.- i) Para ver que $(X^2, \bigoplus, \bigotimes)$ es anillo conmutativo hay que verificar que

a) $(X^2, \bigoplus)$ sea grupo abeliano.
b) $\bigotimes$ sea conmutativa.
c) $\bigotimes$ sea asociativa
d) $\bigotimes$ distribuya respecto $\bigoplus$.

Por enunciado, $(X^2, \bigoplus)$ es grupo abeliano (verificarlo!).
Para ahorrar **matraca** verifiquemos primero la conmutatividad.
Conmutatividad: Sea $(a,b),(x,d) \in X^2$.

$$\begin{aligned}(a,b)\bigotimes(c,d) &= (a\cdot c, 0)\\ &= (c\cdot a, 0)\\ &= (c,d)\bigotimes(a,b)\end{aligned}$$

Asociativdad: Sean $(a,b),(c,d),(e,f) \in X^2$.

$$\begin{aligned}(a,b)\bigotimes\Big[(c,d)\bigotimes(e,f)\Big] &= (a,b)\bigotimes(c\cdot e, 0)\\ &= (a(\cdot c\cdot e), 0)\\ &= ((a\cdot c)\cdot e, 0)\\ &= \Big[(a,b)\bigotimes(c,d)\Big]\bigotimes(e,f)\end{aligned}$$

Distributividad de $\bigotimes$ respecto $\bigoplus$: Propuesto.

Por lo tanto, como se cumple a,b,c y d se tiene que $(X^2, \bigoplus, \bigotimes)$ es un anillo conmutativo. □

ii) **Unidad:** Se tiene que un elemento (a_1, a_2) es unidad ssi

$$(a_1,a_2)\bigotimes(c,d) = (c,d) \forall (c,d) \in X^2$$

Pero para eso, se necesitaría que $(a_1,a_2)\bigotimes(c,d) = (a\cdot c, 0) = (c,d)$, con lo cual $a\cdot c = c$ y $d = 0$, esto últumo no cumpliendose necesariamente, ya que tomando $b \neq 0$ se tiene que no se cumple la igualdad (lol). Por lo tanto, $\bigotimes$ no tiene unidad.

Divisores del cero: Recordemos que un elementos (d_1,d_2) es divisor del 0[1] ssi $\exists (a,b) \in X^2\backslash\{(0,0)\}, (a,b)\bigotimes(d_1,d_2$ $(0,0)$.

Por lo tanto, se necesita que que ambas coordenadas luego de componer con $\bigotimes$ sean 0:

$$\begin{aligned}a\cdot d_1 = 0 &\implies a = 0\\ 0 = 0 &\implies b \in X\end{aligned}$$

Por lo tanto, eligiendo $(a,b) = (0,y), y \in X\backslash\{0\}$, se tiene que todo elemento es divisor del 0.
Finalmente, se tiene que $(X^2, \bigoplus, \bigotimes)$ no es un cuerpo ya que no tiene unidad.

P2.- i) Veamos que $\langle g\rangle$ es subgrupo de G, para eso se necesita que <g>sea subconjunto de G, el neutro pertenezca a $\langle g\rangle$, los inversos de los elementos de $\langle g\rangle$ viven también en él, y por último, que $\langle g\rangle$ sea cerrado para $\cdot$. So, empecemos.

[1] OJO: Es el cero correspondiente al neutro de la operación $\bigoplus$, que en este caso es el (0,0).

1) PDQ: $\langle g\rangle \subseteq G$

En efecto, sea $y \in \langle g\rangle$, entonces, $\exists n \in \mathbb{N}$ tal que $y = g^n$ (ya que lo elementos de $\langle g\rangle$>son las potencias de g). Luego como $\cdot$ es l.c.i y $g \in G$, entonces cualquier composición finita de g respecto a $\cdot$ pertenece a G, por lo tanto $y = g^n \in G$. Así tenemos que <g>$\subseteq G$.

2) PDQ: e $\in \langle g\rangle$. Como G es finito por enunciado y $\langle g\rangle \subseteq G$, entonces $\langle g\rangle$ debe ser finito. Por lo tanto $\exists m, n \in \mathbb{N}$ tal que $g^n = g^m$ (si no existieran, entonces todas las potencias de g serían distintas y por ende $\langle g\rangle$ seria infinito).

Luego, sin perdida de generalidad, digamos que $m < n$, por lo tanto $g^m = g^m g^{n-m}$. Aplicando g^{-m} a ambos lados de la iguadlad se tiene que:

$$g^{-m} \cdot g^m = g^{-m} g^m g^{n-m}$$

Usando que $g^{-m} \cdot g^m = e$ se obtiene que

$$e = g^{n-m}$$

Por lo tanto, e es una potencia de g y asi $e \in \langle g\rangle$.

3) PDQ: $\forall y \in \langle g\rangle, x^{-1} \in \langle g\rangle$

Para demostrar que los inversos de los elementos de $\langle g\rangle$ viven también en él debemos llegar a que los inversos son alguna potencia de g.

Con esto en mente, notemos que como $e \in \langle g\rangle$, entonces $\exists n \in \mathbb{N}$ tal que $g^n = e$, pero puede haber más de uno! Entonces, denotemos por n_0 al menor natural tal que $g^{n_0} = e$.

Luego, desde ese n_0 no hay elementos nuevos en $\in \langle g\rangle$. (Osea, $\forall m \geq n_0, \exists n \leq n_0, g^m = g^n$).

Con esto, sea $y \in \langle g\rangle$, entonces $\exists k \in \mathbb{N}$ tal que $y = g^k$. Además, $\exists j \in \mathbb{N}$ tal que $n_0 \cdot jk$ (si $n_0 > k$, tomamos j=1, sino, iterativamente se puede encontrar el j que sirva (para este caso solo nos importa saber que existe!)). Entonces, $n_0 \cdot j - k \in \mathbb{N}$. Por lo tanto

$$g^{jn_0 - k} = g^{jn_0} g^{-k}$$

Finalmente, notando que $g^{n_0 j} = (g^{n_0})^j = e^j = e$, entonces se tiene que $g^{-k} = g^{n_0 j - k}$ con $n_0 j - k$ natural, por lo tanto g^{-k} es una potencia de g y así $g^{-k} \in \langle g\rangle$. Así, $\forall y \in \langle g\rangle$, $y^{-1} \in \langle g\rangle$.

4) PDQ: $\forall y, z \in \langle g\rangle$, $y \cdot z \in \langle g\rangle$.

En efecto, sea $y, z \in \langle g\rangle$, entonces se tiene que, nuevamente, $\exists n, m \in \mathbb{N}$ tal que $y = g^n$ y $z = g^m$. Luego, se tiene que $y \cdot z = g^n \cdot g^m = g^{m+n}$ con $m + n \in \mathbb{N}$. Así, $y \cdot z = g^{n+m} \in \langle g\rangle$ (ya que es una potencia de g).

ii) Razonando por contradicción supongamos que $g^3 = e$. Con esto, como se concluyó en el item anterior, no hay .[el]ementos nuevos.[a] partir de $n = 3$. Por lo tanto,

$$\langle g\rangle = \{g, g \cdot g, g \cdot g \cdot g\}$$

.

Y así se tiene que $|\langle g\rangle| = 3$. Pero $|G| = 4$ y $\langle g\rangle$ es subgrupo de G, por lo que por Teorema de Lagrange $|\langle g\rangle|$ debiese ser divisor de $|G|$, pero 3 no es divisor 4. **Contradiccion!**.

Por lo tanto, si $|G| = 4$, entonces necesariamente se tiene que $g^3 \neq e$. □

P3.- I) i) **PDQ:** $f(0_k) = 0_A$.

Como $0_K esneutropara+$, entonces $0_K = 0_K + 0_k$, por lo tanto

$$f(0_K) = f(0_K + 0_K)$$

Luego, como $f(\cdot)$ es morfismo entre $(K, +)$ y $(A, \bigoplus)$, entonces

$$\begin{aligned} f(0_K) &= f(0_K + 0_K) \\ &= f(0_K) \bigoplus f(0_k) \end{aligned} \tag{1}$$

Además, $f(0_K) \in A$, el cual es grupo abeliano para la suma $\bigoplus$, por lo tanto el inverso de $f(0_K)$ pertenece a A (OJO! Ahora los inversos para la operación "suma"se denotarán $-x$ y los inversos para la operación "multiplicación"se denotarán x^{-1})

Entonces podemos sumar $-f(0_k)$ a ambos lados de la igualdad en (1). Así tenemos que:

$$f(0_K) = f(0_K) \bigoplus f(0_k) \text{ || sumando } -f(0_K) \text{ a ambos lados}$$
$$-f(0_K) \bigoplus f(0_K) = -f(0_k) \bigoplus (f(0_K) \bigoplus f(0_k))$$

Finalmente, usando la asociatividad de $\bigoplus$[2] y que $-f(0_K) \bigoplus f(0_K) = 0_A$, entonces tenemos que

$$0_A = f(0_K) \quad \square$$

ii) **PDQ:** $f(-x) = -f(x) \forall x \in K$.
Siempre en estas preguntas de varios items, debemos preguntarnos si es que alguna parte interior nos sirve. En este caso, usaremos la parte ii).
Notemos que $\forall x \in K, x + (-x) = 0_K$. Por lo tanto

$$f(x + (-x)) = f(0_K) = 0_A$$

En donde en la segunda igualdad se usó el resultado obtenido en la parte ii). Así obtuvimos que $f(x + (-x)) = 0_A$. Pero además $f(\cdot)$ es morfismo, por lo tanto:

$$f(x + (-x)) = f(x) \bigoplus f(-x)$$

Juntando ambas igualdades obtenidas para $f(x + (-x))$ tenemos que

$$f(x) \bigoplus f(-x) = 0_A$$

Es decir, $f(x)$ es el inverso de $f(-x)$ en A. Por lo tanto $-f(-x) = f(x)$, con lo cual concluimos que $-f(x) = f(-x)$. $\square$

iii) **PDQ:** $(f(K), \bigoplus)$ es subgrupo de $(A, \bigoplus)$.
Usaremos la caracterización compacta para ver que $(f(K), \bigoplus)$ es subgrupo.
$PDQ : \forall z, y \in f(K), z \bigoplus (-y) \in f(K)$ (Acá usamos que el inverso de y es -y en vez de y^{-1} ya que estamos trabajando con la operación $\bigoplus$, la cual usaremos la notación de $-a$ para los inversos).
Entonces, sea $z, y \in f(K)$, por tanto, $\exists a, b \in K$ tal que $f(a) = z$ y $f(b) = y$.
Con esto, tenemos que

$$z \bigoplus (-y) = f(a) \bigoplus f(b)$$

Luego, como $f(\cdot)$ es morfismo, se tiene que $f(a) \bigoplus f(b) = f(a + b)$[3], con lo cual

$$x \bigoplus y = f(a + b)$$

Finalmente, como + es una l.c.i, entonces a+b $\in K$, entonces $x \bigoplus (-y)$ es la imagen mediante f de un elemento de K, por lo tanto $x \bigoplus (-y) \in f(K)$.
Como esta es válido para para todo z,y en f(K), concluimos que $(f(K), \bigoplus)$ es subgrupo de $(A, \bigoplus)$. $\square$

II) **PDQ:** $f(x) = 0_A \iff x = 0_K$
Como todas nuestras equivalencias, lo haremos con doble implica.
$(\Longleftarrow)$
Ya lo hicimos en la parte i) de la I) jeje.
$(\Longrightarrow)$
Hagamoslo por contradicción, supongamos que $\exists x \neq 0_K$ tal que $f(x) = 0_A$.
Como $x \neq 0_K$ y K es cuerpo, entonces $x^{-1} \in K$ tal que $x \cdot x^{-1} = 1_K$[4],entonces se tiene que

$$f(x \cdot x^{-1}) = f(1_K) = 1_A \tag{2}$$

La última igualdad por indicación de enunciado (que $f(1_K) = 1_A$).

[2]Es asociativa solo porque sabemos que $(A, \bigoplus, \bigotimes)$ es anillo
[3]Si una función f es morfismo, f^{-1} también lo es.
[4]Si es que $x = 0_K$ esta afirmación no es cierta, ya que 0_K no tiene inverso para $\cdot$, por cual todo el argumento que sigue se cae

Pero además f es morfismo, por lo que $f(x \cdot x^{-1}) = f(x) \bigotimes f(x^{-1})$. Pero por hipotesis tenemos que $f(x) = 0_A$, entonces

$$f(x \cdot x^{-1}) = f(x) \bigotimes f(x^{-1}) = 0_A \bigotimes f(x^{-1}) = 0_A \tag{3}$$

Así, juntando las igualdades de (2) y (3) se llega a que

$$0_A = 1_A$$

Pero por enunciado tenemos que $0_A \neq 1_A$. **CONTRADICCION.**

Por lo tanto, como asumiendo que si $x \neq 0_K$ se llegó a una contradicción, entonces necesariamente tenemos que $x = 0_K$. □

III) **PDQ:** $f(\cdot)$ es inyectiva.

Sean $x, y \in K$ tal que $f(x) = f(y)$.

Entonces, se tiene que $f(x) \bigoplus (-f(y)) = 0_A$, luego, usando que f es morfismo (de nuevo)

$$0_A = f(x) \bigoplus (-f(y)) = f(x + (-y))$$

Entonces, $z = x + (-y)$ cumple que $f(z) = 0_A$, por lo que por la parte II) se tiene que $z = 0_K$. Con esto obtenemos que $x + (-y) = 0_K$, lo tanto $x = y$. □

P4.- I) PDQ: $a \in A$ divisor del cero $\implies$ a no es invertible.

Razonando por contradicción, supongamos que a es invertible. Entonces $\exists y \in A$ tal que

$$x \cdot y = 1_A$$

Pero además a es divisor del cero, entonces $\exists z \in A \backslash \{0_K\}$ tal que

$$x \cdot z = 0_K \tag{4}$$

Luego, podemos multiplicar (4) por y (el inverso de x y obtenemos que

$$\begin{aligned} & y \cdot (a \cdot z) = y \cdot 0_K \\ \implies & (y \cdot x) \cdot z = 0_K \\ \implies & = 1_K \cdot z = 0_K \\ \implies & z = 0_K \end{aligned}$$

Es decir, se llega a que $z = 0_K$, pero por definición de que el elemento a sea divisor de cero, necesariamente $z \neq 0_K$. Alguien dijo...**CONTRADICCION? SI.**

Por lo tanto, si a es divisor del cero, a no puede ser invertible. □

II) Sea $x \in A$, no invertible, $x \neq 0_A$.

i) PDQ: $\forall m \in \mathbb{N}, x^m \neq 1_A$ Nuevamente por contradicción, supongamos que $\exists n \in \mathbb{N}$ tal que $x^n = 1_A$. Si es así, entonces

$$x^{n-1} \cdot x = 1_A$$

Entonces, x_{n-1} es inverso de x, lo cual es una contradicción ya que por enunciado x no es invertible. **NOTA:** Este último argumento es válido incluso si $n = 1$, ya que si $n = 1$ entonces $x = 1_A$, pero la unidad es trivialmente invertible (su inverso es el mismo) por lo que igual llegamos a una contradicción.

ii) Basándonos en la información extraída del problema 2, definamos

$$\langle x \rangle = \{x, x \cdot x, x \cdot x \cdot x, ...\} \text{ (Conjunto de las potencias de x)}$$

Este conjunto $\langle x \rangle$ es subconjunto de A, el cual es finito. Por lo tanto $\langle x \rangle$ es finito, y así debe existir $m, n \in \mathbb{N}$ tal que $x^n = x^m$ (sino, todas las potencias de x serían distintas y por lo tanto $\langle x \rangle$ sería infinito). □

iii) PDQ[5]: $\exists r, s \in \mathbb{N}$ tal que $x^r(1 - x^s) = 0$

Para demostrar que existen ese r y s, encontremos explícitamente cuales son.

En efecto, por la parte anterior, tenemos que $\exists m, n \in \mathbb{N}$ tal que $x^n = x^m$.

[5] Acá se relajó un poco la notación, en vez de 1 y 0, debiese estar 1_A y 0_K (unidad y cero del anillo)

Sin perdida de generalidad digamos que $m < n$ y así obtenemos que:

$$\begin{aligned} & x^m = x^n \\ \implies & x^m - x^n = 0 \\ \implies & x^m(1 - x^{n-m}) = 0 \end{aligned}$$

Y así, definiendo $r = m$ y $s = n - m$ (que sabemos pertenece a $\mathbb{N}$ ya que $m < n$) hemos encontrado los naturales r y s que cumplen que

$$x^r(1 - x^s) = 0 \quad \square$$

iv) PDQ: x es divisor de $0 \iff \exists y \in A$ tal que $x \cdot y = 0$
Por la parte anterior, tenemos que $\exists r, s \in \mathbb{N}$ tal que $x^r(1 - x^s) = 0$. Como $(A, +, \cdot)$ es anillo, entonces $1 - x^s = 1 + (-r^s) \in A$ [6]. Así, definiendo $y = 1 + (-r^s) \in A$ obtenemos que $x \cdot y = 0$, con lo cual se demuestra que x es divisor del cero. $\square$
NOTA: Note que en la parte I) y la iv) de la parte II), hemos probado la equivalencia, es decir $a \in A$ es divisor del cero $\iff$ a no es invertible.

[6] ya que por ser anillo, el inverso respecto la suma de x pertenece a A, y así $1 + (-x^r) \in A$ al ser + una l.c.i