PAUTA CONTROL 3 - MA11A-ALGEBRA

(1999)

Pregunta 1.

(a)

(i)

$$
\begin{aligned}
S + iS' &= \sum_{k=0}^{n} \binom{n}{k} cos(k \cdot \alpha) + i \sum_{k=0}^{n} \binom{n}{k} sen(k \cdot \alpha) \\
&= \sum_{k=0}^{n} \binom{n}{k} (cos\ k\ \alpha + \ i\ sen\ k\alpha) \\
&= \sum_{k=0}^{n} \binom{n}{k} (cos\ \alpha\ +\ i\ sen\ \alpha)^k \cdot 1^{n-k} \\
&= (1\ +\ cos\ \alpha\ + i\ sen\ \alpha)^n
\end{aligned}
$$

(ii)

$$
\begin{aligned}
1\ +\ cos(\alpha)\ + i\ sin\ \alpha &= 1 +\ cos(2\frac{\alpha}{2}) +\ i\ sen(2\frac{\alpha}{2}) \\
&= 1\ +\ cos^2(\frac{\alpha}{2}) - sen^2(\frac{\alpha}{2}) +\ i \cdot\ 2\ sen(\frac{\alpha}{2})\ cos(\frac{\alpha}{2}) \\
&= 2cos^2(\frac{\alpha}{2}) +\ i\ 2sen(\frac{\alpha}{2})\ cos(\frac{\alpha}{2}) \\
&= 2cos(\frac{\alpha}{2})[cos(\frac{\alpha}{2}) + i\ sen(\frac{\alpha}{2})] \\
&= 2cos(\frac{\alpha}{2}) e^{i\frac{\alpha}{2}}
\end{aligned}
$$

Luego,

$$
\begin{aligned}
(1 + cos(\alpha) + isen(\alpha))^n &= (2cos(\frac{\alpha}{2}) e^{i\frac{\alpha}{2}})^n \\
&= (2cos(\frac{\alpha}{2}))^n \cdot (e^{i\frac{\alpha}{2}})^n \\
&= 2^n cos^n(\frac{\alpha}{2})[cos(n\frac{\alpha}{2}) + isen(n\frac{\alpha}{2})]
\end{aligned}
$$

$$
\begin{aligned}
\Rightarrow S &= 2^n cos^n(\frac{\alpha}{2}) cos(n\frac{\alpha}{2}) \\
S' &= 2^n cos^n(\frac{\alpha}{2}) sen(n\frac{\alpha}{2})
\end{aligned}
$$

(b) Las raíces de la unidad son:

$$w_j = e^{i \cdot j \cdot \frac{2\pi}{n}} \qquad j = 0, \cdot\cdot, n-1$$

$$\begin{aligned}
\Rightarrow \prod_{j=0}^{n-1} w_j = \prod_{j=0}^{n-1} e^{i \cdot j \cdot \frac{2\pi}{n}} &= e^{i \cdot \frac{2\pi}{n}} \cdot \sum_{j=0}^{n-1} j \\
&= e^{i \cdot \frac{2\pi}{n} \cdot \frac{(n-1)n}{2}} \\
&= e^{i \cdot (n-1) \cdot \pi} \\
&= (e^{i\pi})^{n-1} = (-1)^{n-1}
\end{aligned}$$

Pregunta 2.

(i)

Cerradura de * en B: Sean $a, b \in B$, luego existen $\overline{a}, \overline{b} \in A$ tales que $a * \overline{a} = \overline{a} * a = e$, $b * \overline{b} = \overline{b} * b = e$. Además dado que $*$ es asociativa entonces $\overline{a}$ y $\overline{b}$ son únicos.

$$\text{Luego: } (a * b) * (\overline{b} * \overline{a}) = (a * (b * \overline{b}) * \overline{a})$$
$$= a * (e * \overline{a}) = a * \overline{a} = e$$

(usando asociatividad).

$$y \qquad (\overline{b} * \overline{a}) * (a * b) = \overline{b} * (\overline{a} * a) * b$$
$$= \overline{b} * (e * b)$$
$$= \overline{b} * b = e$$

Lo que dice que $(a * b)$ tiene inverso en A para $*$ que es $\overline{b} * \overline{a}$. Si $(A, *)$ es asoc. y tiene neutro y $a, b \in A$ son invertibles para $*$ entonces $a * b$ también y su inverso es $b^{-1} * a^{-1}$.

(B, *) es grupo:

→ Como $*$ es asoc. en A también lo es en B.

→ Como $e * e = e$ entonces $e \in B$.

→ Sea $b \in B$, entonces existe $\overline{b} \in A$ tal que $b * \overline{b} = \overline{b} * b = e$ y $\overline{b}$ es el único inverso de b por asoc. y existencia de neutro. Además $\overline{b} \in B$ por la igualdad anterior.

$$\Rightarrow (B, *) \text{es grupo}$$

(ii)

Se sabe que $(\mathbb{Z}_{13} \backslash \{0\}, \cdot_{13})$ es un Grupo Abeliano pues $(\mathbb{Z}_{13}, +_{13}, \cdot_{13})$ es un cuerpo. Luego si A_1, A_2 o A_3 son subgrupos de $(\mathbb{Z}_{13} \backslash \{0\}, \cdot_{13})$ entonces por Teorema de Lagrange su cardinal debe dividir a $\underline{12} = (\#\mathbb{Z}_{13} \setminus \{0\})$.

Esto descarta a A_2 pues $\#A_2 = 7$ y no descarta aún a A_1 ni A_3 pues $\#A_1, = 2, \#A_3 = 4$.

Veamos A_2:

$1 \in A_2, *_{13}$ es asociativa y $12 \cdot_{13} 12 = 1 \Rightarrow (12)^{-1} = 12$

$$1 \cdot_{13} 1 = 1 \Rightarrow (1)^{-1} = 1$$
$$12 \cdot_{13} 1 = 12$$
$$1 \cdot_{13} 12 = 12$$

$\Rightarrow (A_2, \cdot_{13})$ es un grupo (cerradura, neutro, asoc. e inversos).

Veamos A_3:

- Cerradura:

$\cdot_{13}$	1	5	8	12
1	1	5	8	12
5	5	12	1	8
12	12	8	5	1

- Asociatividad: Se hereda de $\cdot_{13}$

- $1 \in A_3 \Rightarrow$ neutro

- $5^{-1} = 8, 1^{-1} = 1, 8^{-1} = 5, 12^{-1} = 12 \Rightarrow$ inversos.

$$\Rightarrow (A_3, \cdot_{13}) \text{ es un grupo.}$$

Pregunta 3.

(a)

(i)

Forma larga:

- <u>Cerradura</u>:

Sean $Z_1, Z_2 \in S_1 \Rightarrow Z_1 \cdot Z_2 \in \mathbb{C}$ y $|Z_1 \cdot Z_2| = |Z_1| \cdot |Z_2|$

$$= 1 \cdot 1$$
$$= 1$$

$$\Rightarrow Z_1 \cdot Z_2 \in S_1$$

- <u>Asoc.</u>: se hereda de $\mathbb{C}$

- <u>Neutro</u>: $1 \in S$ puesto $|1| = 1, 1 \in \mathbb{C}$.

- <u>Inversos</u> :
Dado $Z \in S_1 \Rightarrow Z = a + bi = e^{i\Theta}$.

$$\Rightarrow Z^{-1} = \frac{+a}{a^2+b^2} + \frac{-b}{a^2+b^2} i = e^{-i\Theta}$$

pues $a^2 + b^2 = 1 \Rightarrow Z^{-1} = a - bi = e^{-i\Theta}$

$$\Rightarrow |Z^{-1}| = a^2 + b^2 = |e^{-i\Theta}| = 1.$$

$\Rightarrow Z^{-1} \in S_1$

pueden usar que: $|Z^{-1}| = \frac{1}{|Z|}$ si $\in \mathbb{C} \setminus \{0\}$

Forma compacta:

Sean $Z_1, Z_2 \in S_1 \Rightarrow Z_1 \cdot Z_2^{-1} \in \mathbb{C}$ y $|Z_1 \cdot Z_2^{-1}| = |Z_1| \cdot |Z_2^{-1}|$

$$(\text{como} Z_2 \neq 0) = |Z_1| \cdot |Z_2|^{-1}$$
$$= 1 \cdot 1 = 1$$

$$\Rightarrow Z_1 \cdot Z_2^{-1} \in S_1$$
$$\Rightarrow (S_1, \cdot) \text{ es subgrupo}$$

(ii)

$w^3 = 1$.

$\rightarrow$Probemos que $f(a) \in S_1$: en efecto $f(a) \in \mathbb{C}$ y $|f(a)| = |w^a| = |w|^a = 1^a = 1$.
Luego$f(a) \in S_1$.

$\rightarrow$morfismo : $P.d.$: $f(a +_3 b) = f(a) \cdot f(b)$

Sea $c = (a +_3 b) \Rightarrow f(a +_3 b) = w^c$ y $c = a + b + k \cdot 3$ para un cierto $k \in \mathbb{Z}$. Luego,

$$
\begin{aligned}
f(a +_3 b) = w^{a+b+k\cdot 3} = w^{a+b} \cdot w^{k\cdot 3} &= w^{a+b} \cdot (w^3)^k \\
&= w^{a+b} \cdot 1^k \\
&= w^{a+b} = w^a \cdot w^b \\
&= f(a) \cdot f(b)
\end{aligned}
$$

(iii)

Si $g : (\mathbb{Z}, +_3) \rightarrow (S_1, \cdot)$ es un homomorfismo entonces $g(0) = 1$ pues ambos son grupos. Además si llamamos $g(1) = w$ se tendrá

$$
\begin{aligned}
& g(2) = g(1 +_3 1) = g(1) \cdot g(1) = w^2 \\
y \quad & g(0) = g(1 +_3 2) = g(1) \cdot g(2) = w \cdot w^2 = w^3 = 1
\end{aligned}
$$

$$
\begin{aligned}
\Rightarrow & g(0) = w^0 \\
& g(1) = w^1 \\
& g(2) = w^2 \qquad y \qquad w^3 = 1
\end{aligned}
$$