MA-11A Álgebra **5 de Julio, 2001**

Pauta Control 3

PROBLEMA 1:

(i).- Las soluciones de la ecuación $z^3 - 9z^2 + 33z = 65$ son las raíces del polinomio $p(z) = z^3 - 9z^2 + 33z - 65$. Como este polinomio es a coeficientes reales, sus raíces en $\mathbb{C} \setminus \mathbb{R}$ (de las cuales hay a lo más 2) vienen en pares conjugados, digamos α y $\overline{\alpha}$. Del enunciado se tiene que $|\alpha|^2 = 13$. Por el teorema fundamental del álgebra, p tiene tres raíces (contando multiplicidades). Luego, necesariamente, la otra raíz de p está en $\mathbb{R}$. Llamemos a esta última raíz β. Sigue que

$$\begin{aligned} z^3 - 9z^2 + 33z - 65 &= p(z) \\ &= (z-\alpha)(z-\overline{\alpha})(z-\beta) \\ &= (z^2 - 2\mathbb{R}e(\alpha)z + |\alpha^2|)(z-\beta) \\ &= z^3 - (\beta + 2\mathbb{R}e(\alpha))z^2 + (2\mathbb{R}e(\alpha)\beta + |\alpha|^2)z - |\alpha^2|\beta\,. \end{aligned}$$

Sigue que $z^3 - 9z^2 + 33z - 65 = z^3 - (\beta + 2\mathbb{R}e(\alpha))z^2 + (2\mathbb{R}e(\alpha)\beta + 13)z - 13\beta$.

Igualando coeficientes o evaluando en $z = 0$ se obtiene que $65 = 13\beta$, i.e., $\beta = 5$. Sigue que $z^3 - 9z^2 + 33z - 65$ es divisible por $z - 5$. De hecho,

$$z^3 - 9z^2 + 33z - 65 = (z-5)(z^2 - 4z + 13)\,.$$

Sigue que α y $\overline{\alpha}$ deben ser raíces de $z^2 - 4z + 13$, es decir son $(4 \pm 6i)/2 = 2 \pm 3i$.

(ii).- Observemos primero que las raíces de $x^2 + x + 1$ son, por fórmula conocida, $\alpha = (-1 + i\sqrt{3})/2$ y $\overline{\alpha} = (-1 - i\sqrt{3})/2$. Luego, $x^2 + x + 1 = (x-\alpha)(x-\overline{\alpha})$. Por resultado conocido, sabemos que para concluir que el polinomio $p(x) = x^{2n} + 1 + (x+1)^{2n}$ es divisible por $x^2 + x + 1$ basta verificar que dicho polinomio es divisible por $(x-\alpha)$ y por $(x-\overline{\alpha})$, o lo que es lo mismo, que α y $\overline{\alpha}$ son raíces de p. En efecto, como $\alpha^2 + \alpha + 1 = 0$, se tiene que $\alpha + 1 = -\alpha^2$, por lo que

$$p(\alpha) = \alpha^{2n} + 1 + (\alpha+1)^{2n} = \alpha^{2n} + 1 + (-\alpha^2)^{2n} = \alpha^{2n} + 1 + \alpha^{4n}$$

Luego, dado que $\alpha = e^{i4\pi/3}$, $\overline{\alpha} = e^{-i4\pi/3}$, y $n = 3k \pm 1$, sigue que

$$p(\alpha) = e^{i8(3k\pm1)\pi/3} + 1 + e^{i16(3k\pm1)\pi/3}\,.$$

Sigue que

$$\begin{aligned} p(\alpha) &= e^{i8k\pi \pm i8\pi/3} + 1 + e^{i16k\pi \pm i16\pi/3} \\ &= e^{\pm i2\pi/3} + 1 + e^{\pm i4\pi/3} \\ &= 1 + e^{i2\pi/3} + e^{i4\pi/3} \\ &= 0\,, \end{aligned}$$

donde la última igualdad se tiene puesto que 1, $e^{i2\pi/3}$, $e^{i4\pi/3}$ son las raíces cúbicas de la unidad, luego su suma es nula.

Además, como p es un polinomio a coeficientes reales, $p(\overline{\alpha}) = p(\alpha) = 0$. Sigue que α y $\overline{\alpha}$ son raíces de p como se buscaba comprobar.

PROBLEMA 2:

(i).- Primero observar que $i^{17} = (i^4)^4 i = 1^4 i = i$. Luego, debemos determinar $(1-i)^{17}/(1+i)$.

Veremos dos maneras de hacer esto último.

- **Primera forma**: Pasando a forma polar. Tenemos que $1+i = \sqrt{2}e^{i\pi/4}$ y $1-i = \sqrt{2}e^{-i\pi/4}$. Luego,
$$\frac{(1-i)^{17}}{1+i} = \frac{2^{17/2}e^{-i17\pi/4}}{\sqrt{2}e^{i\pi/4}} = 2^8 e^{-i18\pi/4} = 256e^{-i\pi/2} = -256i\,.$$
- **Segunda forma**: Observar que $(1-i)^2 = 1 + i^2 - 2i = -2i$ por lo que $(1-i)^{17} = ((1-i)^2)^8(1-i) = (-2i)^8(1-i) = 2^8(1-i)$. Luego,
$$\frac{(1-i)^{17}}{1+i} = \frac{2^8(1-i)}{1+i} = 2^8\frac{(1-i)(1-i)}{|1+i|^2} = 2^8\frac{(-2i)}{2} = -256i\,.$$

(ii).- Del enunciado y por el Teorema de la División se tiene que existen $Q, Q' \in \mathbb{K}[x]$ tales que $F = Q\cdot G\cdot H + R$, $R = Q'\cdot G + R'$, y el $grado(R') < grado(G)$. Sigue que $F = (Q\cdot H + Q')G + R'$ con $grado(R') < grado(G)$.

Por la unicidad del resto garantizada por el Teorema de la División sigue que el resto de dividir F por G es R'.

(iii.1).- Si $\omega = e^{i2\pi/n}$, las raíces n-ésimas de la unidad son $\omega_l = \omega^l$ con $l = 0,\ldots,n-1$. Luego,
$$\sum_{l=0}^{n-1}\omega_l^m = \sum_{l=0}^{n-1}(\omega^m)^l = \begin{cases} n\,, & \text{si } \omega^m = 1,\\ \dfrac{1-\omega^{mn}}{1-\omega^m}\,, & \text{si } \omega^m \neq 1.\end{cases}$$

Como $\omega^{mn} = (\omega^n)^m = 1^m = 1$ dado que ω es raíz n-ésima de la unidad, sigue que
$$\frac{1}{n}\sum_{l=0}^{n-1}\omega_l^m = \frac{1}{n}\sum_{l=0}^{n-1}(\omega^m)^l = \begin{cases} 1\,, & \text{si } \omega^m = 1,\\ 0\,, & \text{si } \omega^m \neq 1.\end{cases}$$

El resultado deseado se obtiene observando que $\omega^m = 1$ si y sólo si $2\pi m/n = 2k\pi$ para algún $k \in \mathbb{Z}$, i.e., si y sólo si n divide a m.

(iii.2).- Por (iii.1) el termino $(1/n)\sum_{l=0}^{n-1}\omega_l^k$ se anula para $k \in \{0,\ldots,n-1\}$ excepto cuando $k = 0$ (pues 0 es divisible por n) en cuyo caso la sumatoria vale 1. Luego,
$$\frac{1}{n}\sum_{k=0}^{n-1}P(\omega_l) = \frac{1}{n}\sum_{l=0}^{n-1}\sum_{k=0}^{m}a_k\omega_l^k = \sum_{k=0}^{m}a_k\left(\frac{1}{n}\sum_{l=0}^{n-1}\omega_l^k\right) = a_0\,.$$

PROBLEMA 3:

(i).- Hay dos formas de ver que f y g son biyectivas.

- **Primera Forma**: Como $f^2(z) = \overline{(\overline{z})} = z$, se tiene que f es invertible (su inversa es f). Luego, f es biyectiva. Análogamente, como $h : U \to U$ tal que $h(z) = -i \cdot z$ es tal que $g \circ h(z) = z$, se tiene que g es invertible (su inversa es h). Luego, g es biyectiva.
- **Segunda Forma**: Sean $z, z' \in U$. Si $f(z) = f(z')$, entonces $\overline{z} = \overline{z'}$. Conjugando, se obtiene que $z = z'$, i.e., f es inyectiva. Si $g(z) = g(z')$, entonces $i \cdot z = i \cdot z'$, luego $z = z'$ y sigue que g es inyectiva. Además, $f(\overline{z}) = z$ y $g(-i \cdot z) = z$ luego f y g son sobreyectivas.

Como $g \circ f(z) = g(\overline{z}) = i \cdot \overline{z}$ y $f \circ g(z) = f(i \cdot z) = \overline{i \cdot z} = -i\overline{z}$, se tiene que $g \circ f(1) \neq f \circ g(1)$, por lo que $g \circ f \neq f \circ g$.

Probaremos ahora que $g^p(z) = i^p \cdot z$ para todo $p \in \mathbb{Z}$. Primero estableceremos, por inducción, que $g^p(z) = i^p \cdot z$ para todo $p \geq 0$. El caso base, $p = 0$, es obvio. Supongamos que la propiedad se cumple para p y veamos que se tiene para $p+1$. Luego, $g^{p+1}(z) = g^p(g(z)) = i^p(i \cdot z) = i^{p+1} \cdot z$. Esto concluye la inducción. Para ver que la propiedad se tiene para todo $p \in \mathbb{Z}$ basta notar que $g^{-1}(z) = -i \cdot z = i^{-1} \cdot z$. Luego, si $p < 0$, entonces $g^p(z) = (g^{-1})^{|p|}(z) = i^{-|p|} \cdot z = i^p \cdot z$ donde la penúltima igualdad se obtiene de un argumento inductivo similar al utilizado para concluir que $g^p(z) = i^p \cdot z$ para todo $p \geq 0$.

Veamos ahora que para todo $p \in \mathbb{Z}$ se tiene que $f^p = id_U$ si p es par y $f^p = f$ si p es impar. Hay dos formas de hacerlo.

- **Primera Forma**: Probando primero, por inducción, que para todo $p \in \mathbb{N}$, $f^p = id_U$ si p es par y $f^p = f$ si p es impar. En efecto, como $f^0 = id_U$ y 0 es par se tiene la base de la inducción. Supongamos que la propiedad se cumple para p y veamos que se tiene para $p+1$. En efecto, si $p+1$ es par, p es impar, luego $f^{p+1} = f^p \circ f = f \circ f = id_U$. Análogamente, si $p+1$ es impar, p es par, luego $f^{p+1} = f^p \circ f = id_U \circ f = f$. Esto concluye la inducción. Para ver que la propiedad se tiene para todo $p \in \mathbb{Z}$ basta notar que $f^{-1} = f$. Luego, si $p < 0$, entonces $f^p = (f^{-1})^{|p|} = f^{|p|}$ que es igual a id_U o a f despendiendo de si $|p|$ (luego p) es par o impar respectivamente.
- **Segunda Forma**: Observando que si p es par, entonces existe $k \in \mathbb{Z}$ tal que $p = 2k$. Luego, $f^p = (f^2)^k = id_U^k = id_U$. Observando que si p es impar, entonces existe $k \in \mathbb{Z}$ tal que $p = 2k+1$. Luego, $f^p = (f^2)^k \circ f = id_U^k \circ f = f$.

(ii).- Hay dos formas de probar que $(\{f^p : U \to U \ : \ p \in \mathbb{Z}\}, \circ)$ es isomorfo a $(\{-1, +1\}, \cdot)$.

- **Primera Forma**: Observamos que $\{f^p : U \to U \ : \ p \in \mathbb{Z}\} = \{id_U, f\}$. Luego, $\phi : \{id_U, f\} \to \{-1, +1\}$ tal que $\phi(id_U) = +1$ y $\phi(f) = -1$ es claramente biyectiva además

$$\begin{array}{rcccccl} \phi(id_U \circ id_U) & = & \phi(id_U) & = & +1 & = & +1 \cdot +1 \ = \ \phi(id_U) \cdot \phi(id_U) . \\ \phi(id_U \circ f) & = & \phi(f) & = & -1 & = & +1 \cdot -1 \ = \ \phi(id_U) \cdot \phi(f) . \\ \phi(f \circ id_U) & = & \phi(f) & = & -1 & = & -1 \cdot +1 \ = \ \phi(f) \cdot \phi(id_U) . \\ \phi(f \circ f) & = & \phi(id_U) & = & +1 & = & -1 \cdot -1 \ = \ \phi(f) \cdot \phi(f) . \end{array}$$

Sigue que ϕ es un isomorfismo, i.e., $\{f^p : U \to U \ : \ p \in \mathbb{Z}\}$ y $\{-1, +1\}$ son isomorfos.

- **Segunda Forma**: Observamos que $\{f^p : U \to U : p \in \mathbb{Z}\} = \{id_U, f\}$ y recordamos que existe un único (salvo isomorfismo) grupo de cardinalidad 2. Luego, $(\{id_U, f\}, \circ)$ y $(\{-1, +1\}, \cdot)$ deben necesariamente ser isomorfos.

(iii).- Veremos dos formas de hacer esta parte.

- **Primera Forma**: Por (i), si p es par, entonces $f^p = id_U$ y
$$(f^m \circ g^n) \circ (f^p \circ g^q) = f^m \circ g^{n+q}\,.$$
Si por el contrario, p es impar, entonces $f^p = f$. Recordando que $i = \overline{i^{-1}}$ tenemos que
$$g^n \circ (f^p \circ g^q)(z) = g^n \circ f \circ g^q(z) = g^n \circ f(i^q z) = i^n(\overline{i^q z}) = \overline{i^{q-n} z} = f \circ g^{q-n}(z)\,.$$
Luego, $(f^m \circ g^n) \circ (f^p \circ g^q) = f^{m+1} \circ g^{q-n}$. En cualquier caso, siempre existen enteros s y t tales que $(f^m \circ g^n) \circ (f^p \circ g^q) = f^s \circ g^t$.
- **Segunda Forma**: Recordando que $i = \overline{i^{-1}}$ se observa que $g^n \circ f = f \circ g^{-n}$.
Luego,
$$(f^m \circ g^n) \circ (f^p \circ g^q) = f^m \circ g^n \circ f^p \circ g^q = f^{m+p} \circ g^{q-n}$$
Luego, existen enteros s y t tales que $(f^m \circ g^n) \circ (f^p \circ g^q) = f^s \circ g^t$.

(iv).- Primero observemos que $\mathcal{G} \subseteq \mathcal{H}$. En efecto, por (i), tanto f como g son biyectivas, y por lo tanto f^{-1} y g^{-1} no sólo existen sino que también son biyectivas. Como composición de funciones biyectivas es biyectiva, sigue que f^m, g^n, y $f^m \circ g^n$ son biyectivas cualesquiera sean m y n en $\mathbb{Z}$, i.e., $\mathcal{G} \subseteq \mathcal{H}$.

Hay dos formas de probar que $(\mathcal{G}, \circ)$ es subgrupo de $(\mathcal{H}, \circ)$.

- **Primera Forma**: Probando que $\mathcal{G} \neq \emptyset$ y que $(f^m \circ g^n) \circ (f^{m'} \circ g^{n'})^{-1} \in \mathcal{G}$ para todo $m, n, m', n' \in \mathbb{Z}$.
Lo primero es obvio ya que $f^0 \circ g^0 = id_U \circ id_U = id_U \in \mathcal{G}$.
Lo segundo se comprueba observando que
$$\begin{aligned}(f^m \circ g^n) \circ (f^{m'} \circ g^{n'})^{-1} &= (f^m \circ g^n) \circ (g^{n'})^{-1} \circ (f^{m'})^{-1} \\ &= f^m \circ g^n \circ g^{-n'} \circ f^{-m'} \\ &= f^m \circ g^{n-n'} \circ f^{-m'}\,.\end{aligned}$$
Luego, $(f^m \circ g^n) \circ (f^{m'} \circ g^{n'})^{-1} = f^m \circ g^{n-n'} \circ f^{-m'} \circ g^0 \in \mathcal{G}$, donde la pertenencia se deduce de (iii).
- **Segunda Forma**: Verificando que $(\mathcal{G}, \circ)$ satisface las propiedades de grupo.
Claramente, por (iii), $\circ$ es ley de composición interna sobre $\mathcal{G}$. La asociatividad de $\circ$ en $\mathcal{G}$ se hereda de la asociatividad de la composición de funciones. Como $(f^m \circ g^n) \circ id_U = id_U \circ (f^m \circ g^n) = f^m \circ g^n$ y $id_U = f^0 \circ g^0 \in \mathcal{G}$, se tiene que id_U es neutro para $\circ$ sobre $\mathcal{G}$. Finalmente, $(f^m \circ g^n)^{-1} = (g^n)^{-1} \circ (f^m)^{-1} = g^{-n} \circ f^{-m}$ Luego, $(f^m \circ g^n)^{-1} = f^0 \circ g^{-n} \circ f^{-m} \circ g^0 \in \mathcal{G}$, donde la pertenencia se deduce de (iii).

Para ver que $(\mathcal{G}, \circ)$ es no–abeliano, basta recordar de (i) que $g \circ f \neq f \circ g$ y observar que tanto $g = f^0 \circ g^1$ como $f = f^1 \circ g^0$ están en $\mathcal{G}$.