MA-11A Algebra **8 y 29 de Junio, 2000**

Pauta Control No. 3

PROBLEMA 1:

(i).- Por definición de f, $f^2(x,y) = f \circ f(x,y) = f(-x,y) = (x,y) = id(x,y)$. Análogamente, por definición de g, $g^4(x,y) = g^3 \circ g(x,y) = g^3(-y,x) = g^2 \circ g(-y,x) = g^2(-x,-y) = g \circ g(-x,-y) = g(y,-x) = (x,y) = id(x,y)$.

Hay dos formas de ver que f y g son biyectivas.

- **Primera Forma**: Como $f^2 = id$, entonces $f \circ f = id$, luego f es invertible (tiene como inversa f) y por lo tanto biyectiva. Como $g^4 = id$, entonces $g \circ g^3 = id$, luego g es invertible (tiene como inversa g^3) y por lo tanto biyectiva.
- **Segunda Forma**: Sean $x, x', y, y' \in \mathbb{R}$. Si $f(x,y) = f(x',y')$, entonces $(-x,y) = (-x',y')$. Sigue que $x = x'$ e $y = y'$ y que f es inyectiva. Si $g(x,y) = g(x',y')$, entonces $(-y,x) = (-y',x')$. Sigue que $x = x'$ e $y = y'$ y que g es inyectiva. Además, $f(-x,y) = (x,y)$ luego f es epiyectiva y $g(y,-x) = (x,y)$ luego g es epiyectiva.

Finalmente, notar que $g^{-1}(x,y) = (y,-x)$. Luego, $g \circ f(x,y) = g(-x,y) = (-y,-x)$ y $f \circ g^{-1}(x,y) = f(y,-x) = (-y,-x)$. Por lo tanto, $g \circ f = f \circ g^{-1}$.

(ii).- Probemos primero que $\forall p \in \mathbb{Z}$, $f^p = id$ si p es par y $f^p = f$ si p es impar. Hay dos formas de hacerlo.

- **Primera Forma**: Probando primero, por inducción, que $\forall p \in \mathbb{N}$, $f^p = id$ si p es par y $f^p = f$ si p es impar. En efecto, como $f^0 = id$ 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 $f^{p+1} = f^p \circ f = f \circ f = id$. Análogamente, si $p+1$ es impar, p es par, luego $f^{p+1} = f^p \circ f = id \circ f = f$. 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 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, $f^p = (f^2)^k = id^k = id$. Observando que si p es impar, entonces existe $k \in \mathbb{Z}$ tal que $p = 2k+1$. Luego, $f^p = (f^2)^k \circ f = id^k \circ f = f$.

Hay dos formas de probar que $(\{f^p : \mathbb{R}^2 \to \mathbb{R}^2 \ : \ p \in \mathbb{Z}\}, \circ)$ es isomorfo a $(\{-1,+1\}, \cdot)$.

- **Primera Forma**: Observamos que $\{f^p : \mathbb{R}^2 \to \mathbb{R}^2 \ : \ p \in \mathbb{Z}\} = \{id, f\}$. Luego, $\phi : \{id, f\} \to \{-1,+1\}$ tal que $\phi(id) = +1$ y $\phi(f) = -1$ es claramente biyectiva además

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

Sigue que ϕ es un isomorfismo, i.e., $\{f^p{:}\mathbb{R}^2 \to \mathbb{R}^2 \,:\, p \in \mathbb{Z}\}$ y $\{-1,+1\}$ son isomorfos.

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

(iii).- Para probar que $\forall n \in \mathbb{N}$, $g^n \circ f = f \circ g^{-n}$ se puede proceder por inducción. Como $g^0 \circ f = id \circ f = f = f \circ id = f \circ g^0$ se cumple la base de la inducción. Supongamos que la propiedad se cumple para n y veamos que se tiene para $n+1$. En efecto, por (i), $g^{n+1} \circ f = g^n \circ (g \circ f) = g^n \circ (f \circ g^{-1}) = (g^n \circ f) \circ g^{-1}$. Luego, por hipótesis inductiva $g^{n+1} \circ f = (f \circ g^{-n}) \circ g^{-1} = f \circ g^{-(n+1)}$. Esto concluye la inducción. (Siendo menos riguroso uno puede observar que se cumple la siguiente recurrencia: $g^n \circ f = (g^{n-1} \circ f) \circ g^{-1} = (g^{n-2} \circ f) \circ g^{-2} = \ldots = f \circ g^{-n}$, y que de ella se deduce fácilmente el resultado deseado — la formalización de este argumento pasa por usar inducción).

Observar ahora que $g^n \circ f = f \circ g^{-n}$ implica que $f = g^{-n} \circ f \circ g^{-n}$, que a su vez implica que $f \circ g^n = g^{-n} \circ f$, i.e., $g^{-n} \circ f = f \circ g^n$. Luego, $\forall n \in \mathbb{N}$, $g^n \circ f = f \circ g^{-n}$ implica que $\forall n \in \mathbb{Z}$, $g^n \circ f = f \circ g^{-n}$.

Finalmente notar que si p es par, entonces $f^p = id$ y

$$(f^m \circ g^n) \circ (f^p \circ g^q) = f^m \circ g^{n+q} \in \mathcal{G}\,.$$

Si por el contrario, p es impar, entonces $f^p = f$ y

$$(f^m \circ g^n) \circ (f^p \circ g^q) = f^m \circ (g^n \circ f) \circ g^q = f^m \circ (f \circ g^{-n}) \circ g^q = f^{m+1} \circ g^{-n+q} \in \mathcal{G}\,.$$

(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**: Verificando que $\mathcal{G} \neq \emptyset$ y que $\forall m, n, m', n' \in \mathbb{Z}$, $(f^m \circ g^n) \circ (f^{m'} \circ g^{n'})^{-1} \in \mathcal{G}$.
  Lo primero es obvio ya que $f^0 \circ g^0 = id \circ id = id \in \mathcal{G}$. Lo segundo se comprueba observando que

  $$(f^m \circ g^n) \circ (f^{m'} \circ g^{n'})^{-1} = (f^m \circ g^n) \circ (g^{n'})^{-1} \circ (f^{m'})^{-1} = f^m \circ g^n \circ g^{-n'} \circ f^{-m'} = f^m \circ g^{n-n'} \circ f^{-m'}\,.$$

  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 $(f^m \circ g^n) \circ id = id \circ (f^m \circ g^n) = f^m \circ g^n$ y $id = f^0 \circ g^0 \in \mathcal{G}$, se tiene que id 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 observar que $g \circ f(x,y) = g(-x,y) = (-y,-x)$ y que $f \circ g(x,y) = g(-y,x) = (y,x)$, luego $g \circ f \neq f \circ g$.

PROBLEMA 2:

(i).- Primero veamos el caso de $(1-i)^4(1+i)^4$.

- **Primera Forma:** Como $(1-i)(1+i)=2$, sigue que $(1-i)^4(1+i)^4=2^4$.
- **Segunda Forma:** Como $1-i=\sqrt{2}e^{-i\pi/4}$ y $1+i=\sqrt{2}e^{i\pi/4}$, sigue que $(1-i)^4(1+i)^4=\sqrt{2^8}e^{-i\pi}e^{i\pi}=2^4$.

En el caso de $1+i+(i-1)/(|1-i|^2+i)$, observar que $|1-i|^2=2$, luego

$$\frac{i-1}{|1-i|^2+i} \;=\; \frac{(i-1)(2-i)}{|2+i|^2} \;=\; \frac{-1+3i}{5}\,.$$

Luego,

$$1+i+\frac{i-1}{|1-i|^2+i} \;=\; \frac{4}{5}+\frac{8}{5}i\,.$$

(ii).- Para encontrar la forma polar de $z=(1+i\sqrt{3})/2$ basta notar que $\rho=|z|=\sqrt{(1/2)^2+(\sqrt{3}/2)^2}=1$ y que $\theta=\arccos(1/2)=\pi/3$, luego

$$\frac{1+i\sqrt{3}}{2} \;=\; e^{i\pi/3}\,.$$

Supongamos primero que $m\in\mathbb{N}$ es divisible por 6, i.e., $m=6k$ para algún $k\in\mathbb{N}$. Sigue que

$$\left(\frac{1+i\sqrt{3}}{2}\right)^m+\left(-\frac{1+i\sqrt{3}}{2}\right)^m \;=\; \left(e^{i\frac{\pi}{3}}\right)^{6k}+\left(-e^{i\frac{\pi}{3}}\right)^{6k} \;=\; e^{2\pi ki}+e^{2\pi ki} \;=\; 2\,.$$

Supongamos ahora que

$$\left(\frac{1+i\sqrt{3}}{2}\right)^m+\left(-\frac{1+i\sqrt{3}}{2}\right)^m \;=\; 2\,.$$

Claramente m no puede ser impar pues si lo fuera el término de la izquierda en la anterior igualdad sería

$$\left(\frac{1+i\sqrt{3}}{2}\right)^m+\left(-\frac{1+i\sqrt{3}}{2}\right)^m \;=\; \left(\frac{1+i\sqrt{3}}{2}\right)^m-\left(\frac{1+i\sqrt{3}}{2}\right)^m \;=\; 0\;\neq\;2\,.$$

Luego, m debe ser par, y por lo tanto

$$\left(\frac{1+i\sqrt{3}}{2}\right)^m+\left(-\frac{1+i\sqrt{3}}{2}\right)^m \;=\; 2\left(\frac{1+i\sqrt{3}}{2}\right)^m\,.$$

Sigue que

$$1 \;=\; \left(\frac{1+i\sqrt{3}}{2}\right)^m \;=\; e^{i\frac{m\pi}{3}}\,.$$

Por lo tanto, $m(\pi/3)=2\pi k$ para algún $k\in\mathbb{Z}$. Sigue que $m=6k$ para algún $k\in\mathbb{Z}$, i.e., $6|m$.

(iii).- Hay varias formas de abordar este problema, veremos tres de ellas.

- **Primera Forma:** Sea $\alpha = (1-\rho e^{i\frac{\pi}{2}})^n + (1+\rho e^{i\frac{\pi}{2}})^n$. Bastará demostrar que $\alpha = \bar{\alpha}$. En efecto, como $e^{i\frac{\pi}{2}} = i$, entonces $\alpha = (1-\rho i)^n + (1+\rho i)^n$. Como el conjugado de la suma es la suma de los conjugados y el conjugado del producto es el producto de los conjugados, sigue que $\bar{\alpha} = (1+\rho i)^n + (1-\rho i)^n = \alpha$.

- **Segunda Forma:** Como $e^{i\frac{\pi}{2}} = i$, por Moivre se tiene que

$$\begin{aligned}(1-\rho e^{i\frac{\pi}{2}})^n &= (1-\rho i)^n = \sum_{j=0}^{n}\binom{n}{j}(-\rho i)^j\,, \quad \text{y}\\ (1+\rho e^{i\frac{\pi}{2}})^n &= (1+\rho i)^n = \sum_{j=0}^{n}\binom{n}{j}(\rho i)^j\,.\end{aligned}$$

  Luego,

$$(1-\rho e^{i\frac{\pi}{2}})^n + (1+\rho e^{i\frac{\pi}{2}})^n = 2\sum_{j=0:j\text{ par}}^{n}\binom{n}{j}(\rho i)^j = 2\sum_{j=0:j\text{ par}}^{n}\binom{n}{j}\rho^j(-1)^{j/2} \in \mathbb{R},$$

  donde la última igualdad se tiene puesto que cuando j es par $i^j = (-1)^{j/2}$.

- **Tercera Forma:** Observar que $e^{i\frac{\pi}{2}} = i$. Sea $re^{i\theta}$ la forma polar de $1-\rho i$. Es fácil ver que la forma polar de $1+\rho i$ debe ser $re^{-i\theta}$. Luego,

$$(1-\rho e^{i\frac{\pi}{2}})^n + (1+\rho e^{i\frac{\pi}{2}})^n = r^n e^{in\theta} + r^n e^{-in\theta} = r^n(e^{in\theta}+e^{-in\theta}) = 2r^n\cos(n\theta) \in \mathbb{R}.$$

PROBLEMA 3:

(i.1).- **(Sec. 04, 06)** Para $n \in \mathbb{N}$, sea $a_n = \underbrace{1+1+\ldots+1}_{n \text{ veces}}$. Como A es anillo, $a_n \in A$ cualquiera sea $n \in \mathbb{N}$. Como A es finito debe existir $n \neq 0$ tal que $a_n \in \{a_1, \ldots, a_{n-1}\}$. Luego, existen $n > m > 0$ tales que $a_n = a_m$, i.e., $\underbrace{1+1+\ldots+1}_{n \text{ veces}} = \underbrace{1+1+\ldots+1}_{m \text{ veces}}$. Por lo tanto, $\underbrace{1+1+\ldots+1}_{n-m \text{ veces}} = 0$.

(i.2).- **(Sec. 04, 06)** Por distributividad del $\cdot$ con respecto a $+$, se tiene que

$$\underbrace{1+1+\ldots+1}_{ab \text{ veces}} = (\underbrace{1+1+\ldots+1}_{a \text{ veces}})(\underbrace{1+1+\ldots+1}_{b \text{ veces}}).$$

Luego, como A no tiene divisores de cero,

$$\underbrace{1+1+\ldots+1}_{ab \text{ veces}} = 0 \implies \underbrace{1+1+\ldots+1}_{a \text{ veces}} = 0 \ \vee \ \underbrace{1+1+\ldots+1}_{b \text{ veces}} = 0\,.$$

(i).- **(Sec. 01, 02, 03, 05)** Por resultado visto en clase existe una constante $c \in \mathbb{C}$ tal que $p(z) = c(z-\alpha)(z-\beta)(z-\gamma)$, donde c es la constante que acompaña al término de mayor grado en $p(z)$. Como $p(z)$ es mónico, sigue que $c = 1$ y que $p(z) = (z-\alpha)(z-\beta)(z-\gamma)$. Luego, al expandir el producto obtenemos que

$$z^3 + az^2 + bz + c = z^3 - (\alpha+\beta+\gamma)z^2 + (\alpha\beta+\alpha\gamma+\beta\gamma)z - \alpha\beta\gamma\,.$$

Como dos polinomios son iguales sí y sólo si sus coeficientes lo son, se concluye que

$$\alpha\beta\gamma \;=\; -c\,, \quad \alpha\beta+\alpha\gamma+\beta\gamma = b\,, \quad \text{y} \quad \alpha+\beta+\gamma = -a\,.$$

Sigue que si $q(z) = z^3 - 11z^2 + 44z - 112$ tiene raíces $\alpha, \beta, \gamma \in \mathbb{C}$, entonces $\alpha\beta\gamma = 112$. Ahora, como $q(\cdot)$ es un polinomio a coeficientes reales, sus raíces complejas vienen en pares conjugados. Supongamos entonces que $|\alpha| = 4$ y $\beta = \bar{\alpha}$. Luego, $112 = \alpha\beta\gamma = |\alpha|^2\gamma = 16\gamma$, i.e., $\gamma = 7$. Para determinar α y β se puede proceder de dos maneras.

- **Primera Forma**: Observando que $q(z) = (z-7)(z^2-4z+16)$ y que las raíces de $z^2-4z+16$ son $(4 \pm \sqrt{4^2 - 4\cdot 16})/2 = 2 \pm i\sqrt{12}$.
- **Segunda Forma**: Observando que $11 = \alpha+\beta+\gamma = 2\mathbb{R}(\alpha)+7$, i.e., $\mathbb{R}(\alpha) = 2$, y como $|\alpha| = 4$, entonces $\mathbb{I}(\alpha) = \sqrt{4^2 - (\mathbb{R}(\alpha))^2} = \sqrt{12}$. Sigue que $\alpha = 2 + i\sqrt{12}$ y $\beta = 2 - i\sqrt{12}$.

(ii.1).- Si $k \in \mathbb{Z}_n$, $\phi_l(k) = e^{i\frac{2\pi l k}{n}}$, luego $|\phi_l(k)| = 1$. Sean $k, k' \in \mathbb{Z}_n$, entonces

$$\phi_l(k+k') \;=\; e^{\frac{2\pi l(k+k')}{n}i} \;=\; e^{\frac{2\pi l k}{n}i} e^{\frac{2\pi l k'}{n}i} \;=\; \phi_l(k)\phi_l(k')\,.$$

(ii.2).- Sabemos que $\chi(\underbrace{1+\ldots+1}_{n}) = \chi(0)$. Como χ es un caracter, es un homomorfismo, luego $\chi(\underbrace{1+\ldots+1}_{n}) = (\chi(1))^n$ y $\chi(0) = 1$. Sigue que $(\chi(1))^n = 1$, i.e., $\chi(1)$ es una raíz n–ésima de la unidad. Por lo tanto existe $l \in \{0, \ldots, n-1\}$ tal que $\chi(1) = e^{\frac{2\pi l}{n}i}$. Lo anterior implica que

$$\chi(k) \;=\; \chi(\underbrace{1+\ldots+1}_{k}) \;=\; (\chi(1))^k \;=\; e^{\frac{2\pi l k}{n}i}\,,$$

i.e., $\chi = \phi_l \in \{\phi_0, \ldots, \phi_{n-1}\}$.