



Control 3

P1. a) Considere el anillo $(\mathbb{Z}_{15}, +, \cdot)$, donde la suma y la multiplicación son módulo 15.

i) (1.0 pto.) Encuentre un elemento invertible de $(\mathbb{Z}_{15}, \cdot)$ que sea distinto a su neutro.

Solución: Como vimos en clases, el neutro de $(\mathbb{Z}_{15}, \cdot)$ es $[1]_{15}$. Tomamos, por ejemplo, el elemento $[2]_{15}$, tenemos que $[2]_{15} \cdot [8]_{15} = [16]_{15} = [1]_{15}$ (**0.5 ptos.**). Entonces, como sabemos que $(\mathbb{Z}_{15}, \cdot)$ es conmutativo (o calculando que $[8]_{15} \cdot [2]_{15} = [1]_{15}$), se tiene que $[2]_{15}$ es invertible (**0.5 ptos.**).

ii) (1.0 pto.) Encuentre tres elementos distintos x, y, z que son divisores de 0 en $(\mathbb{Z}_{15}, +, \cdot)$.

Solución: Por ejemplo, podemos tomar $x = [3]_{15}$, $y = [5]_{15}$, $z = [10]_{15}$. Tenemos $0 \notin \{x, y, z\}$ y $x \cdot y = [3 \cdot 5]_{15} = [0]_{15} = [3 \cdot 10]_{15} = x \cdot z$, por lo que los tres son divisores de cero. (**1.0 pto.**).

iii) (1.5 ptos.) Se sabe que $(\mathbb{Z}_n, +)$ es un grupo para todo $n \in \mathbb{N}^+$ (no lo pruebe). Encuentre un subgrupo de $(\mathbb{Z}_{15}, +)$ que tenga exactamente 5 elementos. Justifique por qué es un subgrupo.

Solución: El subgrupo buscado es $G := \{[0]_{15}, [3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}\} = \{[3i]_{15} : i = 0, 1, 2, 3, 4\}$ (**0.3 ptos.**).

Primera Alternativa: Consideramos $f : \mathbb{Z}_5 \rightarrow \mathbb{Z}_{15}$ dada por $f([i]_5) = [3i]_{15}$. La imagen de f es G , y entonces, por una proposición, es suficiente mostrar que f es un homomorfismo (**0.4 ptos.**). Se verifica la propiedad del homomorfismo: Dados $[i]_5, [j]_5 \in \mathbb{Z}_5$ arbitrarios, tenemos $f([i]_5 + [j]_5) = f([i + j]_5) = [3(i + j)]_{15} = [3i + 3j]_{15} = [3i]_{15} + [3j]_{15} = f([i]_5) + f([j]_5)$ (**0.4 ptos.** por saber la definición del homomorfismo y **0.4 ptos.** por verificar la propiedad).

Segunda Alternativa: Verificar que G forma un subgrupo usando la caracterización de subgrupos: Para todo $x, y \in G$ se tiene que $x - y = x + (-y) \in G$ (**0.4 ptos** por conocer la caracterización y traducirla correctamente al contexto aditivo de G). Tomamos $x = [3i]_{15}, y = [3j]_{15} \in G$ arbitrarios. Observamos que el inverso aditivo de y es $-y = [15 - 3j]_{15}$ (**0.3 ptos**). Calculamos $x - y = [3i]_{15} - [15 - 3j]_{15} = [3i - 15 + 3j]_{15} = [3(i + j - 5)]_{15} \in G$ (**0.5 ptos**).

Tercera Alternativa: Verificar las propiedades de un grupo para G . Cerradura (**0.3 ptos**), asociatividad (**0.3 ptos**), existencia del neutro (**0.3 ptos**) y existencia de inversos (**0.3 ptos**).

b) Sea $(G, *)$ un grupo donde cada elemento es su propio inverso.

i) (1 pto.) Pruebe que G es abeliano.

Solución: Sean $a, b \in G$ arbitrarios. Tenemos $a = a^{-1}$ y $b = b^{-1}$ por hipótesis. Entonces $a * b = a^{-1} * b^{-1} = (b * a)^{-1}$ **(0.5 ptos.)**. Como también $b * a = (b * a)^{-1}$ por hipótesis, se obtiene $a * b = (b * a)^{-1} = b * a$ **(0.5 ptos.)**.

- ii) (1.5 ptos.) Asuma ahora que $|G| \geq 3$. Pruebe que para todo $n \in \mathbb{N}$ se tiene que $(G, *)$ no es isomorfo a $(\mathbb{Z}_n, +)$.

Solución: Por contradicción. Asumimos que existe un $n \in \mathbb{N}$ tal que los grupos $(G, *)$ y $(\mathbb{Z}_n, +)$ son isomorfos **(0.1 pto.)**. Entonces existe un isomorfismo $f : \mathbb{Z}_n \rightarrow G$. En particular, como f es biyectiva, tenemos que $n = |\mathbb{Z}_n| = |G| \geq 3$ **(0.1 pto.)**. Por lo tanto, $[1]_n \neq [0]_n$ **(0.1 pto.)**, por lo que tiene inverso $[n-1]_n$ **(0.1 pto.)**, y este cumple con $[n-1]_n \neq [1]_n$ porque $n-1 \geq 2$ **(0.2 ptos.)**. Como f es homomorfismo, tenemos que $f([n-1]_n)$ es inverso de $f([1]_n)$ **(0.4 ptos.)**. Por unicidad de los inversos, y la propiedad de G (cada elemento es su propio inverso) sigue que $f([n-1]_n) = f([1]_n)$ **(0.3 ptos.)**, lo que contradice la inyectividad de la función f **(0.2 ptos.)**.

- P2.** a) Sea $\mathcal{F} = \{f : A \rightarrow A : f \text{ es biyectiva}\}$. Se sabe que que $(\mathcal{F}, \circ)$ es un grupo, donde $\circ$ es la composición de funciones. Para cada $a \in A$, un elemento fijo, definimos $\mathcal{F}_a = \{f \in \mathcal{F} : f(a) = a\}$.
i) (1.5 ptos.) Pruebe que, para todo $a \in A$, $(\mathcal{F}_a, \circ)$ es subgrupo de $(\mathcal{F}, \circ)$.

Solución:

Primera Alternativa: Verificar que $\mathcal{F}_a$ es subgrupo mediante la caracterización. Es decir, que $\mathcal{F}_a \neq \emptyset$ y que para todo $f, g \in \mathcal{F}_a$ se tiene que $g \circ f^{-1} \in \mathcal{F}_a$. **(0.3 ptos.)**

Primero, notamos que $id_A \in \mathcal{F}_a$, dado que $id_A(a) = a$, por lo que $\mathcal{F}_a \neq \emptyset$. **(0.4 ptos.)**

Por otro lado, sean $f, g \in \mathcal{F}_a$. Notemos que como $f(a) = a$, para $f^{-1} \in \mathcal{F}$, tenemos que $f^{-1}(a) = a$. **(0.5 ptos.)**

Luego, $g(f^{-1}(a)) = g(a) = a$, de donde se tiene que $g \circ f^{-1} \in \mathcal{F}_a$. **(0.3 ptos.)**

Segunda Alternativa: Verificar las propiedades de un grupo para G . Cerradura **(0.3 ptos)**, asociatividad **(0.3 ptos)**, existencia del neutro **(0.3 ptos)** y existencia de inversos **(0.3 ptos)**.

- ii) (1.5 ptos.) Sean $a, b \in A$, con $a \neq b$. ¿Son $\mathcal{F}_a \cap \mathcal{F}_b$ y $\mathcal{F}_a \cup \mathcal{F}_b$ subgrupos? En caso de que alguno no lo sea, muestre un contraejemplo tomando $A = \{1, 2, 3\}$.

Solución:

- Veamos primero que $\mathcal{F}_a \cap \mathcal{F}_b$ es subgrupo **(0.2 ptos.)**. Para ello, notemos que si $f \in \mathcal{F}_a \cap \mathcal{F}_b$, entonces $f(a) = a$ y $f(b) = b$. Luego, un argumento análogo al ítem anterior se puede aplicar (caracterización por subgrupos o verificar todas las propiedades). **(0.4 ptos.)**
- Por otro lado, $\mathcal{F}_a \cup \mathcal{F}_b$ no es subgrupo **(0.2 ptos.)**. Para ello, tomemos $A = \{1, 2, 3\}$ y notemos que el conjunto $\mathcal{F}_1 \cup \mathcal{F}_2$ no es cerrado para la composición de funciones. **(0.2 ptos.)**. En efecto, si $f \in \mathcal{F}_1$ es tal que $f(1) = 1, f(2) = 3$ y $f(3) = 2$ y $g \in \mathcal{F}_2$ es tal que $g(1) = 3, g(2) = 2$ y $g(3) = 1$, entonces $(g \circ f)(1) = 3, (g \circ f)(2) = 1$ y $(g \circ f)(3) = 2$, de donde $g \circ f \notin \mathcal{F}_1 \cup \mathcal{F}_2$. **(0.5 ptos.)**

- b) Sea $z = a + bi \in \mathbb{C}$.

- i) (1.5 ptos.) Sea $\lambda \in \mathbb{R}$, $\lambda > 0$. Diga qué condiciones tienen que satisfacer los reales a y b para que $|z + \lambda| = |z| + \lambda$.

Solución:

Primero, notemos que $|z + \lambda|^2 = (a + \lambda)^2 + b^2 = a^2 + b^2 + \lambda^2 + 2\lambda a$. **(0.2 ptos.)**. Por otro lado, $(|z| + |\lambda|)^2 = a^2 + b^2 + \lambda^2 + 2|\lambda||z| = a^2 + b^2 + \lambda^2 + 2\lambda|z|$. **(0.2 ptos.)**.

Luego, para la igualdad se debe cumplir que $a = |z|$, es decir, que $a = \sqrt{a^2 + b^2}$. **(0.4 ptos.)**.

Para que esto se satisfaga, se necesita que $b = 0$ y $a \geq 0$ **(0.7 ptos.)**.

- ii) (1.5 ptos.) Pruebe que $|z| - 1 \leq |z - 1| \leq |z| + 1$.

Solución:

▪ $|z - 1| \leq |z| + |-1| = |z| + 1$. **(0.5 ptos.)**.

▪ $|z| = |(z - 1) + 1| \leq |z - 1| + |1|$. De aquí se tiene que $|z| - 1 \leq |z - 1|$. **(1.0 pto.)**.

P3. Sea $\tilde{\mathbb{Q}} = \{a + bi, |a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$. El propósito de esta pregunta es determinar todos los posibles homomorfismos de $\tilde{\mathbb{Q}}$ en $\mathbb{C}$. Para ello, considere una función no nula $\varphi : \tilde{\mathbb{Q}} \rightarrow \mathbb{C}$ tal que:

$$\forall x, y \in \tilde{\mathbb{Q}}, \quad \varphi(x \cdot y) = \varphi(x)\varphi(y) \wedge \varphi(x + y) = \varphi(x) + \varphi(y).$$

a) Pruebe que una función φ con estas características satisface que:

- i) (1.4 ptos.) $\varphi(0) = 0$ y $\varphi(1) \neq 0$. A partir de esto, muestre que $\varphi(1) = 1$ y $\varphi(-1) = -1$.

Indicación: Tenga en cuenta que $0 + 0 = 0$ y que existe $x \in \tilde{\mathbb{Q}}$ tal que $\varphi(x) \neq 0$.

Solución:

▪ Notemos que $\varphi(0 + 0) = \varphi(0) \Rightarrow \varphi(0) + \varphi(0) = \varphi(0) \Rightarrow \varphi(0) = 0$. **(0.2 ptos.)**

▪ Sea $x \in \tilde{\mathbb{Q}}$ tal que $\varphi(x) \neq 0$. Se tiene que $\varphi(x) = \varphi(1 \cdot x) = \varphi(1) \cdot \varphi(x)$. Si $\varphi(1) = 0$ se tendría $\varphi(x) = 0$, una contradicción. **(0.4 ptos.)**

▪ Notemos que $\varphi(1) = \varphi(1 \cdot 1) = (\varphi(1))^2$. Se sigue que $\varphi(1)(\varphi(1) - 1) = 0$. Como $\varphi(1) \neq 0$ se tiene $\varphi(1) = 1$ (los complejos, al ser cuerpo, no tienen divisores de cero). **(0.4 ptos.)**

▪ Notemos que $\varphi(0) = \varphi(1 + (-1)) = \varphi(1) + \varphi(-1) = 1 + \varphi(-1)$. Como $\varphi(0) = 0$, se concluye que $\varphi(-1) = -1$. **(0.4 ptos.)**

- ii) (0.8 ptos.) Para todo $n \in \mathbb{N}$ se tiene $\varphi(n) = n$ y que, si además $n \neq 0$, $\varphi(\frac{1}{n}) = \frac{1}{n}$.

Solución: Se puede argumentar por inducción. Para $n = 1$, ya sabemos $\varphi(1) = 1$. Además, si asumimos que para todo $n \in \mathbb{N}$, $\varphi(n) = n$, entonces $\varphi(n+1) = \varphi(n) + \varphi(1) = n + 1$. **(0.4 ptos.)**

Cuando $n \neq 0$, tenemos que $1 = \varphi(n/n) = \varphi(n)\varphi(1/n) = n \cdot \varphi(1/n)$. Se concluye que $\varphi(1/n) = 1/n$. **(0.4 ptos.)**

- iii) (0.8 ptos.) Para todo $b \in \mathbb{Z}$, $\varphi(b) = b$. Usando lo anterior, muestre que $\varphi(x) = x$, para todo $x \in \mathbb{Q}$.

Solución: El ítem anterior muestra que basta probarlo para $b = -n$ para $n \in \mathbb{N}$. Se tiene que $\varphi(-n) = \varphi((-1)n) = \varphi(-1) \cdot \varphi(n) = (-1)n = -n$. **(0.4 ptos.)**. Sea $x \in \mathbb{Q}$ con $x = p/q$. se tiene $\varphi(x) = \varphi(p/q) = \varphi(p) \cdot \varphi(1/q) = p/q = x$. **(0.4 ptos.)**

b) Para probar que solo hay dos posibles homomorfismos:

i) (2.0 ptos.) Pruebe que $\varphi(i) \in \{i, -i\}$.

Solución: Notemos que $(\varphi(i))^2 = \varphi(i^2) = \varphi(-1) = -1$ **(1.0 pto.)**. Luego, se sigue que $\varphi(i) = i$ o $\varphi(i) = -i$. **(1.0 pto.)**

ii) (1.0 pto.) Determine qué expresiones puede tomar $\varphi(a + bi)$ y concluya.

Solución: Los únicos homomorfismos son $\varphi(z) = z$ o $\varphi(z) = \bar{z}$ **(0.4 ptos.)**. En efecto, para $z = a + bi$ tenemos que $\varphi(z) = \varphi(a + bi) = \varphi(a) + \varphi(b)\varphi(i) = a + b\varphi(i)$. Por lo tanto $\varphi(a + bi) = a \pm bi$. **(0.6 ptos.)**

Duración: 3 horas.

Nota: Recuerde justificar adecuadamente sus argumentos; si está usando resultados conocidos, indíquelo claramente y verifique las hipótesis.