

GRUPOS Y ANILLOS

- *Alto, policía, ha cometido usted un crimen.*
- *Lo asumo.*
- *Lo arresto.*

Índice de Contenidos

1	Resolucion Ejercicios	1
---	-----------------------	---

1 Resolución Ejercicios

Cualquiera podrá interpretar el propósito de esta sección a partir del encabezado. Se redactaran solo aquellos ejercicios que susciten un interés especial (bajo mi criterio).

1.1.7 *Demostrar que si $(X, *)$ es un monoide finito y $x \in X$ entonces las siguientes condiciones son equivalentes:*

- (i) *x es cancelable por un lado.*
- (ii) *x es cancelable.*
- (iii) *x tiene simétrico por un lado.*
- (iv) *x es simétrico.*

DEMOSTRACIÓN: El flujo de la prueba va a ser el siguiente: suponer x cancelable por la izquierda y concluir que x tiene simétrico por la derecha, para deducir, seguidamente, que x es cancelable por la derecha. Queda a las necesidades de cada uno convencerse de la suficiencia de este argumento.

Supongamos x cancelable por la izquierda y definamos la aplicación $f : X \rightarrow X$ dada por

$$f(a) = x * a.$$

Bajo éstas hipótesis, f es biyectiva. En efecto, para probar la inyectividad aplicamos el ser x cancelable y llegamos a que

$$f(a) = f(a') \Rightarrow x * a = x * a' \Rightarrow a = a'.$$

Más aún, gracias a un resultado del ejercicio 1.1.2, como X es un conjunto finito f es además sobreyectiva (o, si me permites, biyectiva). En consecuencia, para e el neutro de X , existe $a \in X$ cumpliendo $f(a) = e$, por lo que, en definitiva, nos queda

$$x * a = f(a) = e,$$

es decir, x tiene simétrico por la derecha.

Siguiendo esta línea, veamos que x es cancelable por la derecha, suponiendo para ello $y, z \in X$ arbitrarios tales que $y * x = z * x$. El único paso restante es comprobar que

$$y = y * e = y * x * a = z * x * a = z * e = z.$$

Q.E.D.

1.1.8 *Sea $*$ una operación en un conjunto X y supongamos que $*$ tiene un neutro y tres elementos a, b, c tales que $a \neq c$, b es el simétrico por la izquierda de a y c es el simétrico por la izquierda de b . Demostrar que $*$ no es asociativa.*

DEMOSTRACIÓN: Es un razonamiento directo, únicamente es necesario examinar la expresión $c * b * a$:

$$(c * b) * a = e * a = a \neq c = c * e = c * (b * a).$$

Q.E.D.

Concluir que si $(M, *)$ es un monoide en el que todo elemento tiene simétrico por la izquierda, entonces $(M, *)$ es un grupo.

DEMOSTRACIÓN: Sea $a \in M$ arbitrario. Por hipótesis, a tiene simétrico por la izquierda, digámosle b , y este, a su vez, tiene también simétrico por la izquierda c . No obstante, como $*$ es conmutativa, para no llegar a contradicción al aplicar el resultado anterior, se debe dar $a = c$. En consecuencia, para terminar, nos queda que

$$\begin{aligned} a * b &= c * b = e, \\ b * a &= e, \end{aligned}$$

por lo que a es invertible.

Q.E.D.

1.2.2 Sea $m \in \mathbb{Z}$. Demostrar que si m no es cuadrado en \mathbb{Z} , entonces tampoco es un cuadrado en \mathbb{Q} .

DEMOSTRACIÓN: Nos ocuparemos, en su lugar, de probar el contrarrecíproco de la proposición del enunciado. Suponemos $m = q^2$ donde $q = a/b \in \mathbb{Q}$, $a, b \in \mathbb{Z}$ y $\text{mcd}(a, b) = 1$. En consecuencia, deducimos que

$$m = \frac{a^2}{b^2},$$

y al despejar $a^2 = b^2 m$ notamos que

$$a^2 = b(bm) \implies b \mid a^2,$$

donde invocamos el Lema de Euclides para obtener $b \mid a$. No obstante, como a y b eran coprimos, la única causa justificada es que $b = 1$, por lo que concluimos finalmente que $m = a^2$. Q.E.D.

1.3.2 Decimos que un entero d es libre de cuadrados si p^2 no divide a d para ningún número primo p (en particular, 1 es libre de cuadrados). Demostrar que para todo $m \in \mathbb{Z}$ existe un $d \in \mathbb{Z}$ libre de cuadrados tal que $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{d}]$.

DEMOSTRACIÓN: Iniciamos la demostración factorizando $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ y definiendo, a continuación, los números

$$n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}, \quad d = p_1^{a_1 - 2b_1} p_2^{a_2 - 2b_2} \cdots p_k^{a_k - 2b_k}, \quad \text{con } b_i = \left\lfloor \frac{a_i}{2} \right\rfloor.$$

Por una parte, es inmediato notar que $m = n^2 d$ y, por otra parte, el método de construcción nos asegura que $0 \leq a_i - 2b_i \leq 1$, para cada $1 \leq i \leq k$, con lo que deducimos que d es libre de cuadrados.

Habiendo definido estos números auxiliares, notamos que para cada $a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ se cumple

$$a + b\sqrt{m} = a + b\sqrt{n^2 d} = a + bn\sqrt{d} \in \mathbb{Q}[\sqrt{d}],$$

con lo que inferimos que $\mathbb{Q}[\sqrt{m}] \subseteq \mathbb{Q}[\sqrt{d}]$. Recíprocamente, si $a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, entonces

$$a + b\sqrt{d} = a + \frac{b}{n} n\sqrt{d} = a + \frac{b}{n} \sqrt{m} \in \mathbb{Q}[\sqrt{m}],$$

deduciendo finalmente que $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{d}]$.

Q.E.D.

¿Ocurre lo mismo si cambiamos \mathbb{Q} por \mathbb{Z} ?

SOLUCIÓN: Tomando $m = 12$ se puede comprobar que $\mathbb{Z}[\sqrt{d}] \not\subseteq \mathbb{Z}[\sqrt{12}]$, para todo d libre de cuadrados. \square

1.7.3 Sea $a \in \mathbb{R}$. ¿Qué se deduce al aplicar el Primer Teorema de Isomorfía al homomorfismo $\mathbb{R}[X] \rightarrow \mathbb{R}$, dado por $P(X) \mapsto P(a)$? ¿Y qué se deduce al aplicarlo al homomorfismo $\mathbb{R}[X] \rightarrow \mathbb{C}$, dado por $P(X) \mapsto P(i)$?

SOLUCIÓN: La respuesta a la primera pregunta se resume en una aplicación directa que no requiere ninguna ingeniosidad. En cambio, el segundo interrogante encierra un gran enigma. Por ello, como resolver misterios es lo único que aviva nuestro alma, vamos a darle unas reflexiones.

En primer lugar, vamos a verificar que dicho homomorfismo es suryectivo. Con tal fin, dotémosle de un nombre más manejable; pudiera ser f . Este paso es bastante elemental, pues para cualquier $z = a + ib \in \mathbb{C}$, $a, b \in \mathbb{R}$ es evidente que

$$f(a + bX) = z,$$

donde $a + bX \in \mathbb{R}[X]$ sin ninguna clase de dubitación.

El siguiente y último paso se basa en comprobar que $\text{Ker } f = \langle X^2 + 1 \rangle$. Para ello notamos que, dado $P(X) \in \mathbb{R}[X]$, se tiene¹

$$f(P(X)) = 0 \iff P(i) = 0 \iff (X - i) \mid P(X),$$

y por ser todos los coeficientes reales

$$(X - i) \mid P(X) \iff (X + i) \mid P(X).$$

Esta secuencia de equivalencias se puede sintetizar como $f(P(X)) = 0$ si y solo si² $P(X) \in \langle X - i \rangle \cap \langle X + i \rangle$ y $P(X) \in \mathbb{R}[X]$, considerando tanto $\langle X - i \rangle$ como $\langle X + i \rangle$ ideales de $\mathbb{C}[X]$. Es más, el estudiante aventurero puede convencerse de que $\langle X - i \rangle + \langle X + i \rangle = \langle 1 \rangle$, por lo que, invocando el Teorema Chino de los Restos, extraemos que $\langle X - i \rangle \cap \langle X + i \rangle = \langle X - i \rangle \langle X + i \rangle = \langle X^2 + 1 \rangle$.

Concluimos de esta manera que $\text{Ker } f = \mathbb{R}[X] \cap \langle X^2 + 1 \rangle$ ideal de $\mathbb{R}[X]$, por lo que abusaremos un poco de la notación y diremos que $\text{Ker } f = \langle X^2 + 1 \rangle$. Para terminar, aplicamos ahora sí el Primer Teorema de Isomorfía y concluimos que

$$\frac{\mathbb{R}[X]}{\langle X^2 + 1 \rangle} \simeq \mathbb{C}.$$

□

1.7.2 Demostrar el recíproco del Teorema Chino de los Restos para anillos; es decir, probar que si I_1, \dots, I_n son ideales de un anillo A tales que la aplicación $f : A \rightarrow \prod_{i=1}^n A/I_i$, dada por $f(a) = (a + I_1, \dots, a + I_n)$ es suprayectiva, entonces $I_i + I_j = (1)$, para todo $i \neq j$.

DEMOSTRACIÓN: Es suficiente con probar que, dados $i < j$, se cumple $1 \in I_i + I_j$. En efecto, sean $1 \leq i < j \leq n$ arbitrarios. En consecuencia, por ser f suprayectiva, existe $a \in A$ satisfaciendo

$$f(a) = (I_1, \dots, I_i, \dots, 1 + I_j, \dots, I_n),$$

deduciendo, en particular, que $a + I_i = I_i$ y $a + I_j = 1 + I_j$ o, dicho de otra manera, $a \in I_i$ y $1 - a \in I_j$. Para dar término a la demostración, inferimos que

$$1 = a + (1 - a) \in I_i + I_j.$$

Q.E.D.

¹El lector debe hacerse a la idea que se trata de divisibilidad de polinomios en el contexto de \mathbb{C} .

²O, más llanamente, $f(P(X)) = 0 \iff P(X) \in \mathbb{R}[X] \cap \langle X - i \rangle \cap \langle X + i \rangle$.