

# Taller # 2 de Anillos y Campos

Julián Vera (Código: (20212167064)),  
Nicole Vargas (Código: (20212167015)),  
y Wilson Jerez (Código: 201181167034)

Universidad Distrital Francisco José de Caldas  
Facultad de Ciencias Matemáticas y Naturales  
Programa Académico de Matemáticas

## Ejercicios

1. Sea  $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$  y  $g(x) = x^2 + 2x - 3$  en  $\mathbb{Z}_7[x]$ . Encuéntrese  $q(x)$  y  $r(x)$  en  $\mathbb{Z}_7[x]$  tal que

$$f(x) = g(x)q(x) + r(x), \quad \text{con} \quad \deg(r(x)) < 2.$$

**Solución:** Aplicamos la división de polinomios en  $\mathbb{Z}_7[x]$ , cuidando la aritmética módulo 7.

- *División inicial:* Dividimos el término de mayor grado de  $f(x)$  entre el de mayor grado de  $g(x)$ :

$$\frac{x^6}{x^2} = x^4.$$

Multiplicamos  $g(x)$  por  $x^4$  y restamos:

$$\begin{aligned} f(x) - x^4 g(x) &= (x^6 + 3x^5 + 4x^2 - 3x + 2) - (x^6 + 2x^5 - 3x^4) \\ &= (x^6 - x^6) + (3x^5 - 2x^5) + (0 - (-3x^4)) + 4x^2 - 3x + 2 \\ &= x^5 + 3x^4 + 4x^2 - 3x + 2. \end{aligned}$$

Denotamos este nuevo polinomio como

$$r_1(x) = x^5 + 3x^4 + 4x^2 - 3x + 2.$$

- *Segundo paso:* Dividimos el término de mayor grado de  $r_1(x)$  entre  $x^2$ :

$$\frac{x^5}{x^2} = x^3.$$

Multiplicamos  $g(x)$  por  $x^3$  y restamos:

$$\begin{aligned} r_1(x) - x^3 g(x) &= (x^5 + 3x^4 + 4x^2 - 3x + 2) - (x^5 + 2x^4 - 3x^3) \\ &= (x^5 - x^5) + (3x^4 - 2x^4) + (0 - (-3x^3)) + 4x^2 - 3x + 2 \\ &= x^4 + 3x^3 + 4x^2 - 3x + 2. \end{aligned}$$

Sea

$$r_2(x) = x^4 + 3x^3 + 4x^2 - 3x + 2.$$

- *Tercer paso:* Dividimos  $x^4$  entre  $x^2$ :

$$\frac{x^4}{x^2} = x^2.$$

Multiplicamos  $g(x)$  por  $x^2$  y restamos de  $r_2(x)$ :

$$\begin{aligned} r_2(x) - x^2 g(x) &= (x^4 + 3x^3 + 4x^2 - 3x + 2) - (x^4 + 2x^3 - 3x^2) \\ &= (x^4 - x^4) + (3x^3 - 2x^3) + (4x^2 - (-3x^2)) - 3x + 2 \\ &= x^3 + (4x^2 + 3x^2) - 3x + 2 \\ &= x^3 + 7x^2 - 3x + 2 \\ &\equiv x^3 - 3x + 2 \pmod{7}, \end{aligned}$$

porque  $7x^2 \equiv 0$  en  $\mathbb{Z}_7$ . Denotamos

$$r_3(x) = x^3 - 3x + 2.$$

- *Cuarto paso:* Dividimos  $x^3$  entre  $x^2$ :

$$\frac{x^3}{x^2} = x.$$

Multiplicamos  $g(x)$  por  $x$  y restamos:

$$\begin{aligned} r_3(x) - x g(x) &= (x^3 - 3x + 2) - (x^3 + 2x^2 - 3x) \\ &= (x^3 - x^3) + (0x^2 - 2x^2) + ((-3x) - (-3x)) + 2 \\ &= -2x^2 + 2 \equiv 5x^2 + 2 \pmod{7}. \end{aligned}$$

Por tanto, ahora el resto es  $5x^2 + 2$ , que aún tiene grado 2, así que seguimos.

- *Quinto paso:* Dividimos  $5x^2$  entre  $x^2$ :

$$\frac{5x^2}{x^2} = 5.$$

Multiplicamos  $g(x)$  por 5 (en  $\mathbb{Z}_7$ ,  $-2 \equiv 5$ ), y restamos:

$$\begin{aligned} 5 \cdot g(x) &= 5x^2 + 10x - 15 \equiv 5x^2 + 3x + 6 \pmod{7}, \\ (5x^2 + 2) - (5x^2 + 3x + 6) &= (5x^2 - 5x^2) + (0 - 3x) + (2 - 6) \\ &= -3x - 4 \equiv 4x + 3 \pmod{7}. \end{aligned}$$

El resto final es, por tanto,

$$r(x) = 4x + 3,$$

y satisface  $\deg(r(x)) < 2$ .

Para hallar el cociente total  $q(x)$ , sumamos todos los términos usados en cada división:

$$q(x) = x^4 + x^3 + x^2 + x + 5 \equiv x^4 + x^3 + x^2 + x - 2, \quad (\text{en } \mathbb{Z}_7).$$

**Conclusión:** Hemos obtenido

$$\boxed{q(x) = x^4 + x^3 + x^2 + x - 2 \quad \text{y} \quad r(x) = 4x + 3.}$$

Verificando la igualdad  $f(x) = g(x)q(x) + r(x)$  en  $\mathbb{Z}_7[x]$ , se confirma la corrección de esta división.

2. Para factorizar el polinomio  $x^4 + 4$  en  $\mathbb{Z}_5[x]$ , seguimos los siguientes pasos:

**Paso 1: Expresión del polinomio en  $\mathbb{Z}_5[x]$**

Dado que estamos en el cuerpo finito  $\mathbb{Z}_5$ , el número 4 es equivalente a  $-1$ , por lo que podemos reescribir:

$$x^4 + 4 \equiv x^4 - 1 \pmod{5}$$

Observamos que esto se asemeja a una diferencia de cuadrados:

$$x^4 - 1 = (x^2 - 1)(x^2 + 1).$$

**Paso 2: Factorización de  $x^2 - 1$  y  $x^2 + 1$  en  $\mathbb{Z}_5[x]$**

En  $\mathbb{Z}_5$ , las raíces de  $x^2 - 1 = 0$  son los valores  $x = \pm 1$ . Esto nos da:

$$x^2 - 1 = (x - 1)(x + 1).$$

Ahora, examinemos  $x^2 + 1$ . En  $\mathbb{Z}_5$ , buscamos raíces de  $x^2 + 1 = 0$ , lo que equivale a encontrar soluciones para  $x^2 \equiv -1 \equiv 4 \pmod{5}$ . Como  $2^2 \equiv 4 \pmod{5}$ , tenemos que  $x^2 + 1$  tiene raíces en  $x = \pm 2$ , lo que nos da la factorización:

$$x^2 + 1 = (x - 2)(x + 2).$$

**Paso 3: Factorización completa en factores lineales**

Uniendo ambas factorizaciones, obtenemos:

$$x^4 + 4 = (x - 1)(x + 1)(x - 2)(x + 2) \quad \text{en } \mathbb{Z}_5[x].$$

Por lo tanto, la factorización completa en factores lineales en  $\mathbb{Z}_5[x]$  es:

$$(x - 1)(x + 1)(x - 2)(x + 2).$$

3. Vamos a revisar detalladamente la factorización del polinomio  $f(x) = x^3 + 2x + 3$  en  $\mathbb{Z}_5[x]$  y verificar si la factorización correcta es  $(x - 2)(x + 1)^2$ .

**Paso 1: Comprobación de raíces en  $\mathbb{Z}_5$**

Buscamos valores en  $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$  que satisfagan  $f(x) = 0$ .

$$f(x) = x^3 + 2x + 3$$

Calculamos:

$$\begin{aligned}
f(0) &= 0^3 + 2(0) + 3 = 3 \neq 0, \\
f(1) &= 1^3 + 2(1) + 3 = 1 + 2 + 3 = 6 \equiv 1 \pmod{5}, \\
f(2) &= 2^3 + 2(2) + 3 = 8 + 4 + 3 = 15 \equiv 0 \pmod{5}, \quad \checkmark \\
f(3) &= 3^3 + 2(3) + 3 = 27 + 6 + 3 = 36 \equiv 1 \pmod{5}, \\
f(4) &= 4^3 + 2(4) + 3 = 64 + 8 + 3 = 75 \equiv 0 \pmod{5}, \quad \checkmark
\end{aligned}$$

Encontramos que  $x = 2$  y  $x = 4 \equiv -1 \pmod{5}$  son raíces.

**Paso 2: División de  $f(x)$  por  $(x - 2)$**

Hacemos la división de  $f(x)$  entre  $(x - 2)$  en  $\mathbb{Z}_5$ .

El cociente es:

$$x^2 + 2x + 1.$$

**Paso 3: Factorización de  $x^2 + 2x + 1$**

$$x^2 + 2x + 1 = (x + 1)(x + 1) = (x + 1)^2.$$

### Conclusión

La factorización completa de  $f(x)$  en  $\mathbb{Z}_5[x]$  es:

$$(x - 2)(x + 1)^2.$$

Esto muestra que  $f(x)$  **no es irreducible** en  $\mathbb{Z}_5[x]$  porque se descompone en factores de grado menor.

4. Pruebe que si  $F$  es un campo, todo ideal primo propio de  $F[x]$  es maximal.

**Paso Previo: Necesidad del Teorema 27.24**

Antes de proceder con la demostración, necesitamos el siguiente resultado fundamental:

**Teorema 27.24 (Fraleigh, 7ª Edición)** Si  $F$  es un campo, entonces todo ideal en  $F[x]$  es principal.

### Demostración del Teorema 27.24

Sea  $N$  un ideal de  $F[x]$ .

- Si  $N = \{0\}$ , entonces  $N = \langle 0 \rangle$ , que es principal. - Supongamos que  $N \neq \{0\}$ , y tomemos un polinomio  $g(x)$  no nulo en  $N$  con grado mínimo. - Si  $\deg(g(x)) = 0$ , entonces  $g(x) \in F$  y es una unidad. Por el **Teorema 27.5**, en este caso  $N = F[x] = \langle 1 \rangle$ , lo que muestra que  $N$  es principal. - Si  $\deg(g(x)) \geq 1$ , tomemos cualquier  $f(x) \in N$ . - Por el **Teorema 23.1**, aplicando la **división euclidiana**, existen  $q(x), r(x) \in F[x]$  tales que

$$f(x) = g(x)q(x) + r(x),$$

donde  $r(x) = 0$  o  $\deg(r(x)) < \deg(g(x))$ . - Como  $f(x), g(x) \in N$ , se tiene que  $f(x) - g(x)q(x) = r(x) \in N$ . - Como  $g(x)$  tiene grado mínimo en  $N$ , se deduce que  $r(x) = 0$ . - Así,  $f(x) = g(x)q(x)$ , lo que muestra que  $N = \langle g(x) \rangle$ , probando que  $N$  es principal. ♦

## Demostración del Teorema

**Teorema:** Si  $F$  es un campo, entonces todo ideal primo propio de  $F[x]$  es maximal.

### Paso 1: Identificación de los ideales primos

Por el **Teorema 27.24**, todo ideal en  $F[x]$  es principal. Así, un ideal primo propio en  $F[x]$  es de la forma  $\langle p(x) \rangle$  para algún polinomio  $p(x) \in F[x]$ .

Si  $\langle p(x) \rangle$  es primo, entonces para cualquier  $f(x), g(x) \in F[x]$ , si  $f(x)g(x) \in \langle p(x) \rangle$ , se cumple que al menos uno de  $f(x)$  o  $g(x)$  pertenece a  $\langle p(x) \rangle$ .

Esto implica que  $p(x)$  debe ser **irreducible**, pues si fuera reducible, es decir, si

$$p(x) = f(x)g(x)$$

con  $\deg f(x), \deg g(x) < \deg p(x)$ , ninguno de los factores pertenecería a  $\langle p(x) \rangle$ , lo que contradice la primacidad del ideal.

### Paso 2: Prueba de que es maximal

Supongamos que  $\langle p(x) \rangle$  es un ideal primo propio y que existe un ideal  $N$  tal que

$$\langle p(x) \rangle \subsetneq N \subsetneq F[x].$$

Por el **Teorema 27.24**,  $N$  es principal, es decir,  $N = \langle g(x) \rangle$  para algún  $g(x) \in F[x]$ . Como  $p(x) \in N$ , existe  $q(x) \in F[x]$  tal que

$$p(x) = g(x)q(x).$$

Dado que  $p(x)$  es irreducible,  $g(x)$  debe ser un múltiplo de  $p(x)$  o una unidad en  $F[x]$ .

- Si  $g(x)$  es una unidad en  $F[x]$ , entonces  $N = F[x]$ , lo que contradice que  $N$  es un ideal propio. - Si  $g(x)$  es un múltiplo de  $p(x)$ , entonces  $N = \langle p(x) \rangle$ , lo que significa que  $\langle p(x) \rangle$  es maximal.

## Conclusión

Hemos probado que todo ideal primo propio en  $F[x]$  es maximal.  $\square$

5. Si  $D$  es un dominio de ideales principales (DIP), entonces  $D[x]$  es un DIP.

### Demostración.

Sea  $D$  un dominio de ideales principales, es decir, un dominio integral en el cual todo ideal es principal. Debemos demostrar que todo ideal de  $D[x]$  es principal.

**Paso 1:** *Reducción a ideales no nulos.* Sea  $I$  un ideal de  $D[x]$ . Si  $I = \{0\}$ , entonces  $I$  es principal pues  $I = \langle 0 \rangle$ . Asumamos que  $I \neq \{0\}$ .

**Paso 2:** *Elección de un polinomio de grado mínimo.* Dado que  $I$  es no nulo, existe un polinomio  $f(x) \neq 0$  en  $I$  con grado mínimo, es decir, para todo  $g(x) \in I$  con  $g(x) \neq 0$ , se cumple  $\deg(f) \leq \deg(g)$ .

**Paso 3:** *Generación del ideal con  $f(x)$ .* Sea  $\langle f(x) \rangle = \{f(x)h(x) \mid h(x) \in D[x]\}$ . Queremos probar que  $I = \langle f(x) \rangle$ , es decir, que  $f(x)$  genera  $I$ .

**Paso 4:** *División en  $D[x]$ .* Para cualquier  $g(x) \in I$ , usamos la división euclídea en  $D[x]$ :

$$g(x) = q(x)f(x) + r(x), \quad \text{donde } \deg(r) < \deg(f).$$

Como  $I$  es un ideal, tanto  $g(x)$  como  $q(x)f(x)$  pertenecen a  $I$ , de donde  $r(x) = g(x) - q(x)f(x)$  también está en  $I$ . La elección de  $f(x)$  con grado mínimo implica que no puede existir un  $r(x) \neq 0$  con  $\deg(r) < \deg(f)$  dentro de  $I$ , pues esto contradiría la minimalidad de  $f(x)$ . Por tanto,  $r(x) = 0$ , con lo que  $g(x) = q(x)f(x) \in \langle f(x) \rangle$ . Así,  $I \subseteq \langle f(x) \rangle$ .

**Paso 5:** *Conclusión.* Por construcción,  $\langle f(x) \rangle \subseteq I$ . De 1) y 4) se concluye  $I = \langle f(x) \rangle$ . Con ello, todo ideal de  $D[x]$  es principal, y por ende  $D[x]$  es un dominio de ideales principales.

6. Indique cuáles de las funciones dadas  $\nu$  son evaluaciones euclidianas para los dominios enteros dados.

(a) La función  $\nu$  para  $\mathbb{Z}$  dada por  $\nu(n) = n^2$  para  $n \in \mathbb{Z}$  distinto de cero.

(b) La función  $\nu$  para  $\mathbb{Q}$  dada por  $\nu(a) = a^2$  para  $a \in \mathbb{Q}$  distinto de cero.

7. Encuéntrese el mcd de los polinomios

$$f(x) = x^{10} - 3x^9 + 3x^8 - 11x^7 + 11x^6 - 11x^5 + 19x^4 - 13x^3 + 8x^2 - 9x + 3,$$

$$g(x) = x^6 - 3x^5 + 4x^4 - 9x^3 + 5x^2 - 5x + 2$$

en  $\mathbb{Q}[x]$ .

**Solución:**

Aplicamos el **algoritmo de Euclides** siguiendo la sucesión típica de divisiones:

$$\begin{aligned} f(x) &= q_1(x)g(x) + r_1(x), \\ g(x) &= q_2(x)r_1(x) + r_2(x), \\ r_1(x) &= q_3(x)r_2(x) + r_3(x), \\ &\vdots \\ r_{n-1}(x) &= q_n(x)r_n(x) + 0, \end{aligned}$$

donde el último residuo no nulo,  $r_n(x)$ , es el **máximo común divisor**.

En nuestro caso concreto, los pasos de división se especifican como sigue:

$$f(x) = (x^4 - 2x) \cdot g(x) + \underbrace{(-2x^7 + 6x^6 - 6x^5 + 6x^4 - 13x^3 + 8x^2 - 9x + 3)}_{r_1(x)},$$

$$g(x) = (x^2 + 6x - 19) \cdot r_1(x) + \underbrace{(19x^4 + 57x^3 + 38x^2 - 23x + 2)}_{r_2(x)},$$

$$r_1(x) = (x - 3) \cdot r_2(x) + \underbrace{(x^3 + 2x - 1)}_{r_3(x)},$$

$$r_2(x) = (19x + 57) \cdot r_3(x) + 0.$$

Tras la última división, el proceso de Euclides concluye porque el residuo es cero y, por tanto, el *último resto distinto de cero* es

$$r_3(x) = x^3 + 2x - 1.$$

En un anillo de polinomios sobre un campo  $\mathbb{Q}[x]$ , los divisores máximos comunes son únicos *salvo* un factor constante no nulo. Así, concluimos:

$$\boxed{\gcd(f(x), g(x)) = x^3 + 2x - 1.}$$

**Observación:** Cada coeficiente se maneja sobre  $\mathbb{Q}$ , por lo que las operaciones de división de polinomios se realizan sin restricciones, y no necesitamos normalizar factores adicionales más allá de un posible factor multiplicativo no cero. Así queda verificado el resultado final.

8. Muéstrese que  $\{a + xf(x) \mid a \in \mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$  es un ideal en  $\mathbb{Z}[x]$ .
9. Sea  $D$  un dominio euclidiano y sea  $\nu$  una evaluación euclidiana en  $D$ . Muéstrese que si  $a$  y  $b$  son asociados en  $D$ , entonces  $\nu(a) = \nu(b)$ .
10. Sea  $D$  un DFU. Un elemento  $c$  en  $D$  es un mínimo común múltiplo de dos elementos  $a$  y  $b$  en  $D$  si  $a \mid c$  y  $b \mid c$  y  $c$  divide a todo elemento de  $D$  que sea divisible entre  $a$  y  $b$ . Muéstrese para cualesquiera dos elementos no nulos de  $D$ , un dominio euclidiano, tienen un mínimo común múltiplo en  $D$ .

## 11. Solución:

### 1. El anillo y la norma

Recordemos que

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\},$$

y que para cada  $z = a + b\sqrt{-5}$  definimos la *norma* como

$$N(z) = z\bar{z} = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2.$$

Esta norma resulta crucial porque *es multiplicativa*, es decir,

$$N(z_1 z_2) = N(z_1) N(z_2),$$

lo que nos ayudará a analizar la irreducibilidad de varios elementos.

### 2. Dos factorizaciones distintas de 6

En  $\mathbb{Z}[\sqrt{-5}]$ , el número entero 6 tiene las siguientes dos factorizaciones:

$$6 = 2 \cdot 3 \quad \text{y} \quad 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Vamos a ver que los factores que aparecen en una y otra expresión son *irreducibles* y no se pueden relacionar por unidades (asociados). De este modo, comprobamos que la factorización de 6 en este anillo *no* es única (hasta unidades).

### 3. Verificación de irreducibilidad de los factores

#### 3.1. Irreducibilidad de 2

- *Norma de 2:*  $N(2) = 4$ .
- Si 2 fuera reducible, existiría una factorización

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}),$$

con ninguno de los dos factores igual a  $\pm 1$  (los únicos posibles valores de las unidades en este anillo).

- Tomando la norma,

$$4 = N(2) = N(a + b\sqrt{-5}) N(c + d\sqrt{-5}).$$

Eso implica que el par de normas debe multiplicarse para dar 4. En particular, podría pensarse en factorizar 4 como  $1 \times 4$ ,  $2 \times 2$  o  $4 \times 1$ .

- *Norma 2 imposible:* No hay solución en enteros para  $a^2 + 5b^2 = 2$ , pues revisando casos sencillos  $(a, b)$  no aparece ninguna pareja que cumpla esa ecuación.
- De modo que, si uno de los factores tuviera norma 4, el otro forzosamente tendría norma 1 (es decir, sería unidad). Esto demuestra que no podemos factorizarlos ambos como no unidades. Por lo tanto, 2 es irreducible.

### 3.2. Irreducibilidad de 3

- *Norma de 3:*  $N(3) = 9$ .
- Si 3 fuera reducible, al tomar la norma veríamos que la única forma de factorizar 9 con factores mayores que 1 es  $3 \times 3$ . Sin embargo, no existe elemento en  $\mathbb{Z}[\sqrt{-5}]$  con norma 3, porque la ecuación  $a^2 + 5b^2 = 3$  tampoco tiene soluciones en enteros.
- Luego, si uno de los factores de la factorización hipotética de 3 no fuera unidad, su norma tendría que ser 3, lo cual no es posible. Así, no hay factorización no trivial. De ahí se concluye que 3 es irreducible.

### 3.3. Irreducibilidad de $1 + \sqrt{-5}$ y $1 - \sqrt{-5}$

- *Normas:*

$$N(1 + \sqrt{-5}) = 1^2 + 5 \cdot 1^2 = 6, \quad N(1 - \sqrt{-5}) = 1^2 + 5 \cdot 1^2 = 6.$$

- Para factorizar, por ejemplo,  $1 + \sqrt{-5}$  en un producto no trivial  $(x)(y)$ , las normas de  $x$  e  $y$  tendrían que multiplicarse para dar 6. Por tanto, una de las normas debería ser 2 o 3 (porque  $6 = 2 \times 3$ ), o bien 1 y 6. Pero ya hemos visto que no puede haber un factor con norma 2 ni con norma 3, y si uno de los factores tuviera norma 1, sería una unidad.
- Por lo tanto,  $1 + \sqrt{-5}$  no admite factorizaciones no triviales (análogamente para  $1 - \sqrt{-5}$ ). Esto prueba su irreducibilidad.

## 4. Diferencia esencial entre las dos factorizaciones de 6



Hemos verificado que 2, 3,  $1 + \sqrt{-5}$  y  $1 - \sqrt{-5}$  son irreducibles. Ahora, para ver que las dos factorizaciones

$$6 = 2 \cdot 3 \quad \text{y} \quad 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

no son “la misma” (ni difieren sólo por una unidad), basta notar que no podemos convertir, por ejemplo, 2 en  $1 + \sqrt{-5}$  multiplicándola por  $\pm 1$ . Si existiera  $u \in \{\pm 1\}$  tal que

$$2 = u(1 + \sqrt{-5}),$$

se obtendría una contradicción al comparar partes reales e imaginarias. Por tanto, estas factorizaciones no se relacionan por asociados, lo que confirma que  $\mathbb{Z}[\sqrt{-5}]$  no tiene factorización única.

## 5. Conclusión

Así, el elemento 6 en  $\mathbb{Z}[\sqrt{-5}]$  admite dos descomposiciones distintas en irreducibles:

$$6 = 2 \cdot 3 \quad \text{y} \quad 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

sin que los factores aparecidos en una factorización sean meramente asociados a los de la otra. Con esto finalizamos la demostración de que  $\mathbb{Z}[\sqrt{-5}]$  *no* es un dominio de factorización única.

12. Use el algoritmo euclideo en  $\mathbb{Z}[i]$  para encontrar el máximo común divisor de  $8 + 6i$  y  $5 - 15i$ .
13. Sea  $\langle \alpha \rangle$  un ideal principal distinto de cero en  $\mathbb{Z}[i]$ .
  - a) Muéstrese que  $\mathbb{Z}[i]/\langle \alpha \rangle$  es un anillo finito. [**Sugerencia: úsese el algoritmo de división.**]
  - b) Muéstrese que si  $\pi$  es un irreducible de  $\mathbb{Z}[i]$ , entonces  $\mathbb{Z}[i]/\langle \pi \rangle$  es un campo.
  - c) Con respecto a b), encuéntrese el orden  $n$  y característica de cada uno de los siguientes campos:
    - 1)  $\mathbb{Z}[i]/\langle 3 \rangle$
    - 2)  $\mathbb{Z}[i]/\langle 1 + i \rangle$
    - 3)  $\mathbb{Z}[i]/\langle 2 + i \rangle$
14. Sea  $n \in \mathbb{Z}^+$  libre de cuadrado, esto es, no es divisible por el cuadrado de ningún primo. Sea  $\mathbb{Z}[\sqrt{-n}] = \{a + b\sqrt{-n} \mid a, b \in \mathbb{Z}\}$ .
  - a) Defínase la norma  $N$  dada por  $N(a + b\sqrt{-n}) = a^2 + nb^2$ , identificándola como una norma multiplicativa en  $\mathbb{Z}[\sqrt{-n}]$ .
  - b) Muéstrese que  $N(\alpha) = 1$  para  $\alpha \in \mathbb{Z}[\sqrt{-n}]$  si y solo si  $\alpha$  es una unidad en  $\mathbb{Z}[\sqrt{-n}]$ .
  - c) Muéstrese que todo  $\alpha \in \mathbb{Z}[\sqrt{-n}]$  que sea distinto de cero y no sea unidad tiene factorización en irreducibles en  $\mathbb{Z}[\sqrt{-n}]$ . [**Sugerencia: úsese (b).**]

## Solución

### (a) Definición de la norma y multiplicatividad

Sea  $\alpha = a + b\sqrt{-n}$  en  $\mathbb{Z}[\sqrt{-n}]$ . Definimos la norma

$$N(\alpha) = a^2 + nb^2.$$

Queremos ver que, dadas  $\alpha = a + b\sqrt{-n}$  y  $\beta = c + d\sqrt{-n}$ , se cumple

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

En efecto, si multiplicamos

$$\alpha\beta = (a + b\sqrt{-n})(c + d\sqrt{-n}) = (ac - bdn) + (ad + bc)\sqrt{-n},$$

entonces, al calcular

$$N(\alpha\beta) = (ac - bdn)^2 + n(ad + bc)^2,$$

y tras expandir con cuidado, podemos comprobar que

$$(a^2 + nb^2)(c^2 + nd^2) = (ac - bdn)^2 + n(ad + bc)^2.$$

Así,  $N(\alpha\beta) = N(\alpha)N(\beta)$ , confirmando que  $N$  es un morfismo multiplicativo.

—

### (b) Caracterización de las unidades mediante la norma

Queremos mostrar que  $N(\alpha) = 1$  si y sólo si  $\alpha$  es una unidad en  $\mathbb{Z}[\sqrt{-n}]$ .

$\Rightarrow$  Si  $N(\alpha) = 1$ , consideramos la inversa de  $\alpha = a + b\sqrt{-n}$  en el campo de fracciones  $\mathbb{Q}(\sqrt{-n})$ . Se sabe que

$$\alpha^{-1} = \frac{a - b\sqrt{-n}}{a^2 + nb^2}.$$

Dado que  $a^2 + nb^2 = 1$ , la inversa se simplifica a  $a - b\sqrt{-n}$ , que está de nuevo en  $\mathbb{Z}[\sqrt{-n}]$ . Esto prueba directamente que  $\alpha$  es invertible (es decir, es una unidad) en el anillo.

$\Leftarrow$  Si  $\alpha$  es unidad, existe alguna  $\beta \in \mathbb{Z}[\sqrt{-n}]$  tal que  $\alpha\beta = 1$ . Aplicando la norma y usando su multiplicatividad,

$$N(\alpha\beta) = N(\alpha)N(\beta) = N(1) = 1.$$

Dado que  $N(\alpha)$  y  $N(\beta)$  son números enteros positivos (excepto si fueran cero, en cuyo caso no tendríamos una unidad), la única forma de que su producto sea 1 es que ambos valgan 1. Así,  $N(\alpha) = 1$ .

En resumen, las unidades son exactamente aquellos elementos con norma igual a 1.

—

### (c) Factorización de elementos no nulos ni unidades en irreducibles

Para demostrar la factorización en irreducibles en  $\mathbb{Z}[\sqrt{-n}]$ , usamos el **principio de buena ordenación** en la norma.

- Si  $\alpha$  no es una unidad, entonces  $N(\alpha) > 1$ . Si  $\alpha$  no es irreducible, se puede escribir como  $\alpha = \beta\gamma$  con  $\beta, \gamma$  no unidades.
- Como la norma es multiplicativa, tenemos que  $N(\alpha) = N(\beta)N(\gamma)$ , y por ser enteros positivos, se tiene  $N(\beta), N(\gamma) < N(\alpha)$ .
- Procedemos por inducción en la norma. Si todo elemento de norma menor que  $N(\alpha)$  tiene factorización en irreducibles, entonces también lo tiene  $\alpha$ , pues sus factores  $\beta$  y  $\gamma$  se pueden descomponer en irreducibles.
- Aplicando el principio de buena ordenación, concluimos que todo elemento distinto de cero y no unidad en  $\mathbb{Z}[\sqrt{-n}]$  se puede descomponer en irreducibles.

Con esto, queda demostrada la factorización en irreducibles.

## Ejercicios de la clase

1. Sea  $D$  un dominio entero y  $F$  su campo de fracciones. Entonces, para cualquier polinomio  $f(X) \in F[X]$ , existe un polinomio  $f_0(X) \in D[X]$  y un elemento  $a \in D$  tal que:

$$f(X) = \frac{f_0(X)}{a}.$$

- Dado que  $D$  es un dominio entero, su campo de fracciones  $F$  consiste en todas las fracciones de la forma  $\frac{a}{b}$ , donde  $a, b \in D$  y  $b \neq 0$ . Consideremos el anillo de polinomios  $F[X]$ , cuyos elementos son expresiones de la forma:

$$f(X) = \sum_{i=0}^n c_i X^i, \quad \text{con } c_i \in F.$$

Queremos demostrar que cualquier polinomio en  $F[X]$  puede escribirse como  $f(X) = \frac{f_0(X)}{a}$ , donde  $f_0(X) \in D[X]$  y  $a \in D$ .

- Construcción de  $f_0(X)$ : Dado un polinomio  $f(X) \in F[X]$ , podemos escribir cada coeficiente  $c_i$  en términos de elementos de  $D$ :

$$c_i = \frac{a_i}{b_i}, \quad \text{con } a_i, b_i \in D, \quad b_i \neq 0.$$

Sea  $a$  el **mínimo común múltiplo** de los denominadores  $b_0, b_1, \dots, b_n$ , es decir,

$$a = \text{mcm}(b_0, b_1, \dots, b_n) \in D.$$

Por la propiedad del mínimo común múltiplo, sabemos que  $a$  es un múltiplo de cada  $b_i$ , lo que significa que existe  $k_i \in D$  tal que:

$$a = k_i b_i.$$

Multiplicamos ambos lados por  $a_i$ , obteniendo:

$$aa_i = k_i b_i a_i.$$

Ahora, dividiendo por  $b_i$  (que es distinto de cero en  $D$ ):

$$\frac{aa_i}{b_i} = k_i a_i.$$

Dado que  $k_i, a_i \in D$  y  $D$  es un anillo, el producto  $k_i a_i$  también pertenece a  $D$ . Definiendo  $d_i = k_i a_i$ , obtenemos:

$$d_i = \frac{aa_i}{b_i} \in D.$$

Definimos entonces el polinomio  $f_0(X)$  en  $D[X]$  como:

$$f_0(X) = \sum_{i=0}^n d_i X^i.$$

Por construcción, tenemos:

$$f(X) = \sum_{i=0}^n c_i X^i = \sum_{i=0}^n \frac{a_i}{b_i} X^i = \sum_{i=0}^n \frac{d_i}{a} X^i = \frac{1}{a} \sum_{i=0}^n d_i X^i = \frac{f_0(X)}{a}.$$

- **Conclusión:** Hemos demostrado que cualquier polinomio en  $F[X]$  puede escribirse como  $f(X) = \frac{f_0(X)}{a}$  con  $f_0(X) \in D[X]$  y  $a \in D$ . Esto implica que  $D[X]$  es un subanillo de  $F[X]$ , ya que cada polinomio en  $F[X]$  se obtiene como un polinomio en  $D[X]$  dividido por un elemento de  $D$ .

□

2. Muestre que el polinomio  $p(x) = x^2 + x + 3$  es irreducible en  $\mathbb{Q}[x]$ .

**Solución:**

Para demostrar la irreducibilidad del polinomio  $p(x) = x^2 + x + 3$  en  $\mathbb{Q}[x]$ , utilizamos el siguiente resultado:

**Teorema 23.10 (Fraleigh, 7ma edición)**

*Sea  $f(x) \in F[x]$  y supongamos que  $f(x)$  tiene grado 2 o 3. Entonces  $f(x)$  es reducible sobre  $F$  si y solo si tiene una raíz en  $F$ .*

**Demostración:**

Supongamos que  $f(x)$  es reducible sobre  $F$ . Entonces puede escribirse como el producto de dos polinomios no constantes en  $F[x]$ , es decir,

$$f(x) = g(x)h(x),$$

donde  $\deg g(x) < \deg f(x)$  y  $\deg h(x) < \deg f(x)$ . Dado que  $f(x)$  tiene grado 2 o 3, uno de los factores (por ejemplo,  $g(x)$ ) debe ser de grado 1. Por lo tanto,

$$g(x) = x - a, \quad \text{para algún } a \in F.$$

Como  $g(a) = 0$ , concluimos que  $a$  es una raíz de  $f(x)$ . De esta manera, si  $f(x)$  es reducible sobre  $F[x]$ , necesariamente tiene una raíz en  $F$ .

Recíprocamente, si existe  $a \in F$  tal que  $f(a) = 0$ , entonces  $x - a$  es un factor de  $f(x)$ , lo que muestra que  $f(x)$  es reducible.

### Aplicación al ejercicio:

Para comprobar que  $p(x) = x^2 + x + 3$  es irreducible en  $\mathbb{Q}[x]$ , basta con verificar que no tiene raíces racionales. Resolviendo la ecuación cuadrática asociada,

$$x = \frac{-1 \pm \sqrt{1 - 12}}{2} = \frac{-1 \pm \sqrt{-11}}{2},$$

se observa que  $\sqrt{-11} \notin \mathbb{Q}$ . Por lo tanto,  $p(x)$  no posee raíces en  $\mathbb{Q}$  y, de acuerdo con el Teorema 23.10, es irreducible sobre  $\mathbb{Q}$ .

3. Determine los elementos de  $\mathbb{Q}[x]/\langle p(x) \rangle$ .

- Los elementos de  $\mathbb{Q}[x]/\langle p(x) \rangle$  están dados por las clases de equivalencia de los polinomios en  $\mathbb{Q}[x]$  módulo  $p(x)$ . Formalmente, podemos describir estos elementos como sigue:

El conjunto de clases de equivalencia es

$$\mathbb{Q}[x]/\langle p(x) \rangle = \{f(x) + \langle p(x) \rangle \mid f(x) \in \mathbb{Q}[x]\}.$$

Es decir, dos polinomios  $f(x)$  y  $g(x)$  representan el mismo elemento si su diferencia es un múltiplo de  $p(x)$ , es decir, si  $f(x) \equiv g(x) \pmod{p(x)}$ .

Como  $p(x)$  tiene grado  $n$ , cada clase de equivalencia tiene un representante único de la forma:

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1},$$

donde  $a_i \in \mathbb{Q}$ . Esto se debe a que cualquier polinomio  $f(x)$  en  $\mathbb{Q}[x]$  puede reducirse módulo  $p(x)$  mediante la división euclidiana, dejando un residuo de grado menor que  $n$ .

- Si  $p(x)$  es irreducible sobre  $\mathbb{Q}$ , entonces  $\mathbb{Q}[x]/\langle p(x) \rangle$  es un **cuerpo** y se puede interpretar como una extensión de  $\mathbb{Q}$  de grado  $n$ .
- Si  $p(x)$  es reducible, el cociente es un **anillo con divisores de cero**, no necesariamente un cuerpo.

Para  $p(x) = x^2 + 1$ , los elementos del cociente son de la forma:

$$a + bx, \quad a, b \in \mathbb{Q}.$$

En este caso,  $\mathbb{Q}[x]/\langle x^2+1 \rangle$  es isomorfo a  $\mathbb{Q}(i)$ , donde  $i^2 = -1$ , representando la extensión  $\mathbb{Q}$  con la unidad imaginaria.

4. Encontrar el inverso multiplicativo de  $a + bt$  en  $\mathbb{Q}[x]/\langle p(x) \rangle$ , donde  $p(x)$  es irreducible en  $\mathbb{Q}[x]$  y  $t$  es la clase de  $x$  en el cociente.

**Solución:** Como  $\mathbb{Q}[x]/\langle p(x) \rangle$  es un cuerpo, todo elemento no nulo tiene inverso. Se busca  $q(t)$  tal que:

$$(a + bt)q(t) \equiv 1 \pmod{p(t)}.$$

Dado que  $p(x)$  es irreducible y de grado  $n$ , se cumple  $\gcd(a + bx, p(x)) = 1$ . Aplicando el algoritmo de Euclides extendido, existen  $q(x), k(x) \in \mathbb{Q}[x]$  tales que:

$$(a + bx)q(x) + k(x)p(x) = 1.$$

Reduciendo módulo  $p(x)$ :

$$(a + bx)q(x) \equiv 1 \pmod{p(x)}.$$

Por lo tanto,  $q(t)$  es el inverso de  $a + bt$ .

**Cálculo explícito para  $\deg(p) = 2$ :** Sea  $p(x) = x^2 + cx + d$ , busquemos  $q(t) = u + vt$  tal que:

$$(a + bt)(u + vt) \equiv 1 \pmod{p(t)}.$$

Multiplicando:

$$(a + bt)(u + vt) = au + (av + bu)t + bvt^2.$$

Sustituyendo  $t^2 = -ct - d$ :

$$bvt^2 = -bvct - bvd.$$

$$(au - bvd) + (av + bu - bvc)t \equiv 1.$$

Sistema de ecuaciones:

$$\begin{cases} au - bvd = 1, \\ av + bu - bvc = 0. \end{cases}$$

Resolviendo:

$$v = \frac{b}{abc - a^2 - b^2d}, \quad u = \frac{bc - a}{abc - a^2 - b^2d}.$$

Inverso:

$$q(t) = u + vt = \frac{bc - a}{abc - a^2 - b^2d} + \frac{b}{abc - a^2 - b^2d}t.$$

**Caso general  $\deg(p) = n$ :** El inverso  $q(t) = c_0 + c_1t + \dots + c_{n-1}t^{n-1}$  se obtiene resolviendo el sistema de  $n$  ecuaciones que surge al imponer  $(a + bt)q(t) \equiv 1 \pmod{p(t)}$ , expresando  $t^k$  en términos de  $1, t, \dots, t^{n-1}$  usando  $p(t) = 0$ . Esto se resuelve mediante eliminación gaussiana o el algoritmo de Euclides extendido.

**Conclusión:** El inverso de  $a + bt$  en  $\mathbb{Q}[x]/\langle p(x) \rangle$  existe y es único, dado que el cociente es un cuerpo. Se obtiene aplicando el algoritmo de Euclides extendido o resolviendo un sistema de ecuaciones.