# TEORÍA DE GALOIS

Hoja 1.2. Factorización.

**1. Elementos irreducibles y elementos primos.** *Se dice que un elemento $a \neq 0$ en un dominio $D$ es irreducible cuando $a \notin U(D)$ y sólo es divisible por las unidades y por los asociados. Se dice que $a$ es primo en $D$ cuando $a \notin U(D)$ y genera un ideal primo.*

**a)** Demuestra que si $a$ es primo en $D$ entonces es irreducible.

**b)** Prueba que si $D$ es un dominio de ideales principales entonces el recíproco del apartado anterior también es cierto, es decir, que todo irreducible es primo. *Sugerencia: demuestra que en un DIP todo irreducible genera un ideal maximal.*

**c)** Demuestra que en un dominio de ideales principales todo elemento no nulo es una unidad o se puede expresar como un producto finito de primos.

**d)** Demuestra que un dominio de ideales principales es un dominio de factorización única.

**2. Una fuente de ejemplos y contraejemplos.** Vamos a estudiar los dominios de la forma

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : \ a, b \in \mathbb{Z}\}$$

donde $d \in \mathbb{Z}$, $d \neq 1$ y no es divisible por el cuadrado de un primo. Definimos $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}_{\geq 0}$, $N(a+b\sqrt{d}) = |a^2 - db^2|$.

**a)** Demuestra que la función $N$ tiene las siguientes propiedades:

(i) $N(x) = 0$ si y sólo si $x = 0$.

(ii) $N(xy) = N(x)N(y)$.

(iii) $x \in U(\mathbb{Z}[\sqrt{d}])$ si y sólo si $N(x) = 1$.

**b)** Encuentra elementos no triviales en los grupos $U(\mathbb{Z}[\sqrt{-1}])$, $U(\mathbb{Z}[\sqrt{-3}])$ y $U(\mathbb{Z}[\sqrt{3}])$.

**c)** Demuestra que en $\mathbb{Z}[\sqrt{-3}]$ hay elementos irreducibles que no son primos. Sugerencia: estudia la factorización

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4 = 2 \cdot 2.$$

**Dominios euclídeos (DE).** *Diremos que un dominio $D$ es euclídeo si existe una función*

$$d : D \to \mathbb{Z} \geq 0$$

*que verifica:*

*1) Si $a$ y $b$ no nulos, entonces $d(a) \leq d(ab)$.*

*2) Si $b$ es no nulo, entonces existen elementos $q$ y $r$ en $D$ tal que $a = bq + r$, donde $r = 0$ o $d(r) < d(b)$.*

**3.** Demuestra que tanto $\mathbb{Z}$ como $k[x]$ (donde $k$ es un cuerpo) son dominios euclídeos.

**4.** Demuestra que $\mathbb{Z}[\sqrt{-1}]$ es un dominio euclídeo.

**Dominios de ideales principales (DIP)** *Diremos que un dominio $D$ es de ideales principales si todo ideal se puede general con un solo elemento.*

**5.** Demuestra que si $D$ es un dominio euclídeo, entonces es un dominio de ideales principales.

**6.** Demuestra que $\mathbb{Z}[\sqrt{-3}]$ no es un dominio de ideales principales.

**7.** Demuestra que en un dominio de ideales principales un ideal es maximal si y sólo si está generado por un elemento irreducible.

**8. Ideales en $\mathbb{Z}$**

**a)** Demuestra que todo ideal en $\mathbb{Z}$ es principal. *Sugerencia: utiliza el algoritmo de la división y demuestra que si un ideal $I$ es no nulo, entonces $I = n\mathbb{Z}$ donde $n$ es el menor entero positivo en $I$.*

**b)** Halla todos los ideales primos de $\mathbb{Z}$, e indica cuáles son maximales.

**9.** Sea $K$ un cuerpo. Demuestra que todo ideal en $K[x]$ es principal. Halla un generador del ideal $I = (x^3 + 1\ ,\ x^2 + 1)$ en $\mathbb{F}_2[x]$.

**10.** Demuestra que $Z[x]$ no es un dominio de ideales principales.

**Dominios de factorización única (DFU).** *Se dice que un dominio es de factorización única si todo elemento no nulo que no es una unidad se puede escribir como un producto de un número finito de irreducibles de manera única (salvo producto por unidades y salvo el orden de los factores).*

**11.** Demuestra que todo dominio de ideales principales es un dominio de factorización única. En particular $\mathbb{Z}$, y $k[x]$ son DFU-s (cuando $k$ es un cuerpo).

**12.** Demuestra que $\mathbb{Z}[i]$ es dominio de factorización única.

**13.** Demuestra que $\mathbb{Z}[\sqrt{-3}]$ no es dominio de factorización única.

**14.** Demuestra que $Z[x]$ es un dominio de factorización única.

**15.** Considera un cuerpo $K$. Demuestra los siguientes enunciados:

**a)** (Teorema de Ruffini) Sean $P \in K[x]$ y $a \in K$. Entonces $P(a) = 0$ si y sólo si $P \in \langle x - a \rangle$.

**b)** Todo polinomio de grado dos o tres es irreducible en $K[x]$ si y sólo si no tiene raíces en $K$. ¿Qué se puede decir si el grado del polinomio es mayor que tres?

**c)** Sea $a \in K$. Un polinomio $p(x) \in K[x]$ es irreducible si y sólo si $q(x) = p(x + a)$ lo es.

**d)** Sea $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ en $K[x]$ con $a_0 \cdot a_n \neq 0$. Entonces, $f$ es irreducible si y sólo si $a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$ es irreducible.

**e)** Demuestra que todo polinomio de grado uno en $K[x]$ es irreducible.

**16. Algunos criterios de irreducibilidad en $\mathbb{Q}[x]$**

**a)** (Lema de Gauss) Decimos que un polinomio $f(X) \in \mathbb{Z}[x]$ es primitivo cuando el máximo común divisor de sus coeficientes es 1. Demuestra que en $\mathbb{Z}[X]$ el producto de dos polinomios primitivos es primitivo. *Sugerencia: utiliza el homomorfismo de anillos $\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$ donde $p$ es un número primo.*

**b)** Sea $f(x) \in \mathbb{Z}[x]$ un polinomio de grado $n \geq 2$. Prueba que si $f(x)$ es reducible como polinomio en $\mathbb{Q}[x]$, entonces se puede expresar como producto de dos polinomios en $\mathbb{Z}[x]$ de grado menor que $n$.

**c)** Sea $f(x) \in \mathbb{Z}[x]$ un polinomio de grado $n \geq 2$. A la vista del apartado anterior, decide de manera razonada si la siguiente afirmación es verdadera o falsa: *Si $a \in \mathbb{Q}$ es una raíz de $f(x)$ entonces $a \in \mathbb{Z}$.*

**d)** Sea $f(x) \in \mathbb{Z}[x]$, $p \in \mathbb{Z}$ un primo, y sea $\overline{f}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ su imagen via el homomorfismo de anillos

$\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$. Demuestra que si $\mathrm{gr}(f(x)) = \mathrm{gr}(\overline{f}(x))$, y si $\overline{f}(x)$ es irreducible en $\mathbb{Z}/p\mathbb{Z}[x]$, entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.

**e)** Aplica el criterio anterior para deducir que $x^3 + x + 1$ es irreducible en $\mathbb{Q}[x]$.

**f)** (*) El recíproco del enunciado en (d) no es cierto. Demuestra que el polinomio $x^4 + 1$ es irreducible en $\mathbb{Q}[x]$ y sin embargo es reducible en $\mathbb{F}_p[x]$ para todo primo $p$.

**g)** Demuestra que para cada $n \geq 1$ hay infinitos polinomios en $\mathbb{Q}[x]$ irreducibles de grado $n$. *Sugerencia: usa el Criterio de Eisenstein.*

**h)** Para cada primo $p$, el polinomio

$$\phi_p(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + \ldots + 1$$

recibe el nombre de $p$-ésimo polinomio ciclotómico. Demuestra que $\phi_p(x)$ es irreducible para todo primo $p \in \mathbb{Z}$. *Sugerencia: Utiliza el apartado (c) del problema anterior y el Criterio de Eisenstein.*

**17.** Decide razonadamente si los siguientes polinomios son reducibles en $\mathbb{Q}[x]$:

$$f_1(x) = x^4 + 3x + 6, \quad f_2(x) = x^4 + x^2 + 1, \quad f_3(x) = x^3 + 11^{11}x + 13^{13},$$

$$f_4(x) = x^4 - x^3 - x - 1, \quad f_5(x) = \frac{1}{3}x^5 + \frac{5}{2}x^4 + \frac{3}{2}x^3 + \frac{1}{2}, \quad f_6(x) = x^5 - 9x^2 + 1.$$

**18.** Encuentra todos los ideales de los siguientes anillos:

$$R_1 = \mathbb{Q}[x]/(x^3 - 1), \quad R_2 = \mathbb{R}[x]/(x^3 - 1), \quad R_3 = \mathbb{C}[x]/(x^3 - 1),$$

$$R_4 = \mathbb{F}_3[x]/(x^3 - 1), \quad R_5 = \mathbb{F}_5[x]/(x^3 - 1).$$

**19.** En $\mathbb{Q}[x]$ considera el elemento $p(x) = (x^2 + 1)(x^4 + 2x + 2)$. Pongamos $R = \mathbb{Q}[x]/\langle p(x)\rangle$.

(a) Describe los ideales en $R$.

(b) Decide justificadamente si $\overline{x}$ y $\overline{x+1}$ son divisores de cero en $R$.

(c) Decide si $\overline{x}$ y $\overline{x+1}$ son elementos invertibles en $R$ y, en caso afirmativo, encuentra sus inversos.

**20. Factorización sobre $\mathbb{R}$ y sobre $\mathbb{C}$**

**a)** Demuestra que todo polinomio irreducible $p(x) \in \mathbb{R}[x]$ tiene grado 1 ó 2.

**b)** Factoriza a $x^4 - 1$ como producto de polinomios mónicos irreducibles en $\mathbb{R}[X]$.

**c)** Factoriza a $x^4 - 1$ como producto de polinomios mónicos irreducibles en $\mathbb{C}[x]$.

**21. Factorización sobre cuerpos finitos**

**a)** Expresa a $x^4 - 1$ como producto de polinomios mónicos irreducibles en $\mathbb{F}_3[x]$.

**b)** Expresa a $x^4 - 1$ como producto de polinomios mónicos irreducibles en $\mathbb{F}_2[x]$.

**c)** Expresa a $x^4 + x^3 - x^2$ como producto de polinomios mónicos irreducibles en $\mathbb{F}_2[x]$.

**d)** Factoriza al polinomio $x^6 + x^2 + 1$ como producto de irreducibles en $\mathbb{F}_2[x]$.

**e)** Demuestra que $x^3 - x + 1$ es irreducible en $\mathbb{F}_3[x]$.

**f)** Demuestra que $x^5 - x^2 + 1$ es irreducible en $\mathbb{F}_2[x]$.

**g)** Demuestra que $x^{p-1} - 1$ factoriza como producto de $p - 1$ polinomios mónicos de grado uno en $\mathbb{F}_p[x]$.

**22.** Resuelve las siguientes cuestiones usando los problemas 26 y 27 de la Hoja 1.1.

**a)** Demuestra que en $\mathbb{Z}[x]$ el ideal $\langle 5, x+2\rangle$ es maximal y que el anillo cociente es el cuerpo $\mathbb{F}_5$.

**b)** Demuestra que en $\mathbb{Z}[x]$ el ideal $\langle 2, x^2+x+1\rangle$ es maximal, y que el anillo cociente es un cuerpo que contiene estrictamente a $\mathbb{F}_2$.

**c)** Demuestra que en $\mathbb{Z}[x]$ el ideal $\langle 5, x^2-3\rangle$ es maximal, y que el anillo cociente es un cuerpo con 25 elementos.