

TEORÍA DE GALOIS

Hoja 1. Anillos de polinomios. Factorización. Cocientes.

Suponemos que todos los anillos son conmutativos y con unidad. Si $f : R \rightarrow T$ es un homomorfismo entonces suponemos siempre que $f(1_R) = 1_T$.

1. Demuestra que el anillo de polinomios $R[x]$ es un dominio de integridad si y sólo si R es un dominio de integridad.
2. Demuestra que si R es un dominio de integridad y $f(x), g(x) \in R[x]$ son polinomios no nulos entonces el grado del producto es la suma de los grados. ¿Vale lo mismo si R no es un dominio?
3. Sea R un dominio de integridad. Demuestra que los únicos elementos invertibles de $R[x]$ son los elementos de R que son invertibles. ¿Sucede lo mismo si R no es un dominio?
4. Demuestra que $\text{char } R = \text{char } R[x]$.
5. Sea K un cuerpo.
 - a) Demuestra que todo ideal en $K[x]$ es principal.
 - b) Demuestra que un ideal $I \subset K[x]$ es maximal si y sólo si está generado por un elemento irreducible.
 - c) Concluye, usando el apartado anterior, que en $K[x]$ todo elemento irreducible es primo.
 - d) Usando inducción en el grado y los dos apartados anteriores, demuestra que $K[x]$ es un dominio de factorización única.

Teorema. Sea K un cuerpo. Todo polinomio en $K[x]$ se puede escribir como producto de un número finito de irreducibles, siendo la expresión única salvo orden de los factores y/o producto por unidades.

6. Calcula un generador para cada uno de los siguientes ideales en los anillos indicados:
 - a) $I = \langle x^3 + 1, x^2 + 1 \rangle$ en $\mathbb{F}_2[x]$.
 - b) $I = \langle x^2, x^3 - x, x^2 - 1 \rangle$ en $\mathbb{Q}[x]$.
 - c) $I = \langle x^3 - 1, x^3 - x, x^2 - 1 \rangle$ en $\mathbb{R}[x]$.
7. Considera un cuerpo K . Demuestra los siguientes enunciados:
 - a) Demuestra que todo polinomio de grado uno en $K[x]$ es irreducible y además tiene una raíz en K .

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Cartagena99

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

Criterio de irreducibilidad módulo p . Sean $f(x) \in \mathbb{Z}[x]$, $p \in \mathbb{Z}$ un primo, y sea $\bar{f}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ su imagen via el homomorfismo de anillos $\mathbb{Z}[x] \rightarrow \mathbb{Z}/p\mathbb{Z}[x]$. Si $\text{gr}(f(x)) = \text{gr}(\bar{f}(x))$, y si $\bar{f}(x)$ es irreducible en $\mathbb{Z}/p\mathbb{Z}[x]$, entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.

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

b) El recíproco del criterio anterior no es cierto. Demuestra que el polinomio $x^4 - 10x^2 + 1$ es irreducible en $\mathbb{Q}[x]$ y sin embargo es reducible en $\mathbb{F}_p[x]$ para todo primo p . *Sugerencia: Usa que el grupo multiplicativo \mathbb{F}_p^* es cíclico (esto lo probaremos más adelante). Observa que en tal caso, ó bien 2 ó 3 son cuadrados en \mathbb{F}_p , ó bien 6 es un cuadrado en \mathbb{F}_p .*

Criterio de Eisenstein. Sea $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ con $n \geq 1$, y $a_n \neq 0$. Supongamos que existe un primo $p \in \mathbb{Z}$ tal que

$$p \nmid a_n, \quad p \mid a_{n-1}, \dots, a_0, \quad \text{y} \quad p^2 \nmid a_0.$$

Entonces $f(x)$ es irreducible sobre $\mathbb{Q}[x]$.

c) Demuestra que para cada $n \geq 1$ hay infinitos polinomios en $\mathbb{Q}[x]$ irreducibles de grado n .

d) Para cada primo p , el polinomio

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

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 (e) del problema anterior y el Criterio de Eisenstein.*

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

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

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

10. 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 $\mathbb{C}[x]$.

11. 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 $\mathbb{F}_2[x]$.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

- - -

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70

Cartagena99

Más sobre cocientes

12. Encuentra todos los ideales de los siguientes anillos:

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

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

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

14. ¿Cuántos elementos tiene el anillo $\mathbb{F}_3[x]/\langle x^2 + x + 1 \rangle$? ¿Se trata de un cuerpo?

15. ¿Cuántos elementos tiene el anillo $\mathbb{F}_3[x]/\langle x^2 + 1 \rangle$? ¿Se trata de un cuerpo?

16. Resuelve las siguientes cuestiones:

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.

Más sobre homomorfismos de anillos

17. Resuelve las siguientes cuestiones para un anillo A .

a) Demuestra que existe un único homomorfismo de anillos $\mathbb{Z} \rightarrow A$. Concluye que A contiene un subanillo isomorfo a \mathbb{Z} o a $\mathbb{Z}/n\mathbb{Z}$ para algún n entero positivo. *Abusando del lenguaje diremos que $\mathbb{Z} \subset A$ en el primer caso y que $\mathbb{Z}_n \subset \mathbb{Z}$ en el segundo. El primer caso sucede cuando la característica de A es cero; el segundo, cuando la característica de A es positiva.*

Proposición. Todo anillo contiene, un subanillo isomorfo a \mathbb{Z} , o un subanillo isomorfo a $\mathbb{Z}/n\mathbb{Z}$ para algún entero positivo n .

b) Demuestra que si D es un dominio, entonces ó bien tiene característica cero, ó bien tiene característica p (primo). En particular ó bien $\mathbb{Z} \subset D$ ó bien $\mathbb{Z}/p\mathbb{Z} \subset D$.

c) Prueba que un dominio finito D tiene característica p (primo), y además $\mathbb{Z}/p\mathbb{Z} \subset D$ es una extensión de cuerpos. Concluye que cualquier cuerpo finito tiene p^n elementos para algún primo p .

d) Demuestra que si un cuerpo K contiene un subanillo isomorfo a \mathbb{Z} entonces contiene un subcuerpo

**CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70**

**ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70**

The logo for Cartagena99 features the text 'Cartagena99' in a stylized, blue, serif font. The '99' is significantly larger and more prominent than the word 'Cartagena'. The text is set against a light blue background with a subtle gradient and a soft shadow effect.

18. Sea K un cuerpo. El subcuerpo más pequeño de K recibe el nombre de *subcuerpo primo de K* (por lo visto en el ejercicio anterior éste debe ser isomorfo, o bien a \mathbb{Q} , o bien a \mathbb{F}_p para algún primo p). Resuelve las siguientes cuestiones.

a) Sean K y L dos cuerpos. Si $f : K \rightarrow L$ es un homomorfismo entonces f induce un isomorfismo entre los subcuerpos primos de K y L .

Consecuencia. Si K y L son dos cuerpos con diferente característica **no** puede haber un homomorfismo entre ellos. En particular **no** existe ningún homomorfismo de anillos $f : \mathbb{Q} \rightarrow \mathbb{F}_p$ para ningún primo $p \in \mathbb{Z}$; **ni tampoco** existe ningún homomorfismo de anillos $f : \mathbb{F}_p \rightarrow \mathbb{Q}$ para ningún primo $p \in \mathbb{Z}$.

b) Demuestra que el único homomorfismo de anillos $f : \mathbb{Q} \rightarrow \mathbb{Q}$ es la identidad. Y lo mismo para $f : \mathbb{F}_p \rightarrow \mathbb{F}_p$.

19. Demuestra que:

a) No existe ningún homomorfismo de anillos $f : \mathbb{Q}[i] \rightarrow \mathbb{Q}[\sqrt{2}]$.

b) Existen infinitos homomorfismos de anillos $f : \mathbb{Q}[x] \rightarrow \mathbb{Q}[\sqrt{2}]$.

c) No existe ningún homomorfismo de anillos $f : \mathbb{R} \rightarrow \mathbb{Q}$.

20. Sea $R \subset T$ una inclusión de anillos y sea $b \in T$. Consideramos la función:

$$\begin{aligned} f : R[x] &\rightarrow T \\ p(x) &\mapsto p(b). \end{aligned}$$

a) Demuestra que f es un homomorfismo de anillos. Nos referiremos a este homomorfismo como *homomorfismo de evaluación*.

b) Describe $\ker(f)$ en los casos siguientes:

(i) $R = \mathbb{Q}, T = \mathbb{R}, b = 5$; (ii) $R = \mathbb{Q}, T = \mathbb{R}, b = \sqrt[3]{2}$; (iii) $R = \mathbb{R}, T = \mathbb{C}, b = i$.



CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS
CALL OR WHATSAPP:689 45 44 70