TEORÍA DE GALOIS

Hoja 1.1. Anillos, ideales, cocientes, homomorfismos de anillos.

Suponemos que todos los anillos son conmutativos y con unidad. Suponemos que si $f : R \to T$ es un homomorfismo de anillos entonces $f(1_R) = 1_T$.

---

1. Sea R un anillo finito. Demuestra que todo elemento no nulo de R es o bien un elemento invertible, o bien un divisor de cero. Decide de manera razonada si la afirmación sigue siendo cierta si no suponemos que R sea finito.

2. Demuestra que el conjunto $S = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$ con las operaciones suma y producto módulo 10 es un anillo conmutativo con unidad. ¿Es un cuerpo?

3. Demuestra que el anillo de polinomios $R[x]$ es un dominio de integridad si y sólo si R es un dominio de integridad.

4. 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?

5. 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?

6. Demuestra que char R = char $R[x]$.

7. Decide de manera razonada si los siguientes anillos son cuerpos:

a) $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

b) $\mathbb{Z}_3[\xi] := \{a + b\xi : a, b \in \mathbb{Z}_3,\ \xi^2 = -1\}$.

c) $\mathbb{Z}_5[\mu] := \{a + b\mu : a, b \in \mathbb{Z}_5,\ \mu^2 = 2\}$.

8. Sea $\{J_i\}_{i\in I}$ una familia de ideales en un anillo R. Demuestra que $\cap_{i\in I} J_i$ es también un ideal. ¿Qué puedes decir de $\cup_{i\in I} J_i$?

9. Fijado $a \in R$,

a) Demuestra que $\langle a\rangle = R$ si y sólo si $a \in U(R)$.

b) Demuestra que R es un cuerpo si y sólo si el único ideal propio es (0).

10. Se dice que un elemento $a \in R$ es *nilpotente* si $a^n = 0$ para algún entero positivo n. Demuestra que el conjunto de los elementos nilpotentes de un anillo es un ideal.

11. Demuestra que el ideal $\langle 2, x\rangle \subset \mathbb{Z}[x]$ no es principal.

12. ¿Cuántos elementos tiene el anillo $\mathbb{Z}[i]/\langle 2i\rangle$?

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

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

15. Sea $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Considera el anillo $S = R/2R$.

(a) Calcula cuántos elementos tiene S.

(b) Encuentra todos los subanillos de S.

(c) Encuentra todos los ideales de S.

16. Sea $f : R \to T$ es un homomorfismo de anillos.

a) Demuestra que si $a \in R$ es una unidad, entonces $f(a)$ es una unidad.

b) ¿Es cierto el recíproco del enunciado anterior?

c) Demuestra que si R es un cuerpo entonces f es necesariamente inyectivo.

17. Definimos los números complejos a partir del conjunto $\mathbb{C} := \{z = a + bi : a, b \in \mathbb{R}\}$. Dado que $\mathbb{C}$ es un cuerpo, observa que $U(\mathbb{C})$ es el grupo $(\mathbb{C} \setminus \{0\}, \cdot)$. Fijado $z = a + bi$ definimos el conjugado como $C(z) = \overline{z} = a - bi$. Demuestra que la conjugación induce un homorfismo de grupos multiplicativos

$$U(\mathbb{C}) \to U(\mathbb{C}).$$

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

a) Sea A un anillo. Demuestra que existe un único homorfismo de anillos $\mathbb{Z} \to A$. Concluye que A contiene un subanillo isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}/n\mathbb{Z}$ para algún n entero positivo.

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

d) Demuestra que cualquier cuerpo finito tiene p^n elementos para algún primo p.

e) Demuestra que si un cuerpo K contiene un subanillo isomorfo a $\mathbb{Z}$ entonces contiene un subcuerpo isomorfo a $\mathbb{Q}$.

19. Frobenius. Prueba que si A es un anillo de característica p, entonces la función $F : A \to A$, $F(a) = a^p$ es un homomorfismo de anillos, y que $F(a) = a$ para todo elemento de $\mathbb{Z}/p\mathbb{Z}$ ($\subset A$).

20. Demuestra que:

a) No existe ningún homomorfismo de anillos $f : \mathbb{Q} \to \mathbb{F}_p$ para ningún primo $p \in \mathbb{Z}$.

b) No existe ningún homomorfismo de anillos $f : \mathbb{F}_p \to \mathbb{Q}$ para ningún primo $p \in \mathbb{Z}$.

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

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

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

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

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

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) $R = \mathbb{R}$, $T = \mathbb{C}$, $b = i$.

22. Ecuaciones

a) Sea R un anillo y sea $a \in R$ un elemento tal que $a^2 = a$ (un elemento con esta propiedad recibe el nombre de *elemento idempotente*). Decide de manera razonada si necesariamente $a = 0$ ó $a = 1$. *Sugerencia: Analiza el caso* $a = \overline{5} \in R = Z_{20}$.

b) ¿Cuántas soluciones tiene la ecuación $2x = 4$ en $\mathbb{Z}_{12}$?

c) Demuestra que si R es un dominio de integridad, entonces la ecuación $ax = b$ con $a, b \in R$ o bien no tiene solución, o bien tiene solución única.

d) Encuentra todas las soluciones de la ecuación $x^2 - 5x + 6 = 0$ en $\mathbb{Z}_{12}$, en $\mathbb{Z}_7$, y en $\mathbb{Z}_2$.

e) Sea k un cuerpo. Demuestra que si $p(x) \in k[x]$ es un polinomio no nulo de grado n entonces la ecuación $p(x) = 0$ tiene, a lo sumo, n soluciones (no necesariamente distintas). *Sugerencia: usa inducción en el grado y el algoritmo de división.*

23. Demuestra que $\{(3x, y) : x, y \in \mathbb{Z}\}$ es un ideal maximal de $\mathbb{Z} \times \mathbb{Z}$.

24. Demuestra que $\{(a, 0) : a \in \mathbb{Z}\}$ es un ideal primo pero no maximal en $\mathbb{Z} \times \mathbb{Z}$.

25. Encuentra todos los ideales maximales en $\mathbb{Z}_8$, $\mathbb{Z}_{10}$, $\mathbb{Z}_n$.

26. Sean $I \subset J$ ideales en un anillo A.

a) Demuestra que $J/I \subset A/I$ es un ideal;

b) Demuestra que el anillo cociente $(A/I)/(J/I)$ es isomorfo a A/J.

27. Fijado un entero positivo $n \in \mathbb{Z} \geq 2$, demuestra que el anillo cociente $\mathbb{Z}[x]/n\mathbb{Z}[x]$ es isomorfo a $\mathbb{Z}_n[x]$. Concluye que el ideal $n\mathbb{Z}[x]$ es primo si y sólo si n es un número primo.