TEORÍA DE GALOIS

Hoja 0. Repaso: Anillos, ideales, cocientes, homomorfismos de anillos.

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

Anillos

1. 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?

2. Sea R un anillo finito.

a) Demuestra que todo elemento no nulo de R es o bien un elemento invertible, o bien un divisor de cero. Comprueba que esto es así en $\mathbb{Z}_{12}$.

b) Decide de manera razonada si la afirmación sigue siendo cierta si no suponemos que R sea finito.

c) Demuestra que todo dominio de integridad finito es necesariamente un cuerpo.

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

Ideales

4. 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 $\cup_{i\in I} J_i$?

5. Se dice que un elemento $a \in R$ es *nilpotente* si $a^n = 0$ para algún entero positivo n.

a) Encuentra todos los elementos nilpotentes en $\mathbb{Z}_{18}$.

b) Demuestra que el conjunto de los elementos nilpotentes de un anillo es un ideal.

6. Sea $a \in R$.

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).

> **Proposición.** *Sea R un anillo conmutativo con unidad. Entonces R es un cuerpo si y sólo si sus únicos ideales son (0) y R.*

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

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

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

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

Cocientes

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

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

13. 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.

14. 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.

15. 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.

16. Sobre el número de soluciones de las ecuaciones polinómicas

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 de* $\mathbb{Z}_{20}$.

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 $a, b \in R$ ó bien no tiene solución, ó 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.*

Homomorfismos de anillos

17. 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.

> **Proposición.** *Si K es un cuerpo, entonces todo bomomorfismo de anillos, $f : K \to T$, donde T es un anillo cualquiera, es* **inyectivo**.

18. 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

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

19. Homomorfismo de Frobenius. Sea R un anillo de característica prima p.

a) Demuestra que la función $F : R \to R$, $F(r) = r^p$ es un homomorfismo de anillos.

b) Demuestra que $F(r) = r$ para todo elemento de $\mathbb{Z}/p\mathbb{Z}$ ($\subset R$).

c) Comprueba que Frobenius no es la identidad en $R = \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$

d) ¿Es válido el enunciado del apartado (a) si la característica es positiva pero no prima?

Proposición. *Sea R un anillo de característica $p > 0$, donde p es primo. Entonces la función:*

$$\begin{array}{rccc} F: & R & \longrightarrow & R \\ & r & \mapsto & r^p \end{array}$$

es un homomorfismo de anillos y recibe el nombre de **homomorfismo de Frobenius**.