Teoría de Galois

Hoja 1. Anillos, polinomios y cuerpos.

A lo largo de todo el curso por anillo entenderemos un anillo unitario y conmutativo. Entenderemos que todo homomorfismo de anillos $\varphi\colon R \to S$ satisface $\varphi(1_R) = 1_S$.

Repaso de Teoría de Anillos

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 R es infinito.

2. Sea R un anillo y $a \in R$, escribimos $(a) = \{ar\ : r \in R\} = aR \subseteq R$. Demuestra que:

a) (a) es un ideal de R.

b) $(a) = R$ si, y solo, si $a \in \mathcal{U}(R)$.

c) R es un cuerpo si, y solo si, sus únicos ideales son $\{0\}$ y R.

3. Sea R un dominio de integridad y $a, b \in R$. Prueba que $(a) = (b)$ si, y solo si, existe un $c \in \mathcal{U}(R)$ tal que $a = bc$.

4. Sean $I \subseteq J$ ideales en un anillo R. Demuestra que:

a) $J/I \subseteq R/I$ es un ideal.

b) (Teorema de Isomorfía) Sea $\varphi\colon R \to S$ un homomorfismo de anillos. Prueba que $\ker(\varphi)$ es un ideal de R, $\varphi(R)$ es un subanillo de S y $R/\ker(\varphi) \cong \varphi(R)$.

c) El anillo cociente $(R/I)/(J/I)$ es isomorfo a R/J. *Sugerencia: usa el teorema de isomorfía.*

d) (Teorema de correspondencia) Existe una correspondencia entre los ideales de R que contienen a I y los ideales del anillo cociente R/I.

5. Sea n un número natural. Prueba que $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ es un cuerpo si, y solo si, n es primo.

6. Dados $I = \{(3x, y) : x, y \in \mathbb{Z}\}$ y $J = \{(a, 0) : a \in \mathbb{Z}\}$, demuestra que I es un ideal maximal y J es un ideal primo no maximal de $\mathbb{Z} \times \mathbb{Z}$.

7. Dado un dominio de integridad R. Se dice que un elemento $0 \neq a \in R$ es irreducible si $a \notin \mathcal{U}(R)$ y siempre que $a = bc$ se tiene que $b \in \mathcal{U}(R)$ o $c \in \mathcal{U}(R)$. Se dice que $0 \neq a \in R$ es primo si $a \notin \mathcal{U}(R)$ e $I = (a)$ es un ideal primo de R, es decir, siempre que $bc \in I$ se tiene que $b \in I$ o $c \in I$.

a) Demuestra que los elementos primos en R son irreducibles.

b) Prueba que si R es un dominio de ideales principales, entonces el recíproco del apartado anterior también es cierto, es decir, todo elemento irreducible en R es primo.

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

9. Sea $d \in \mathbb{Z}$, $1 \neq d \neq e^2$ con $e \in \mathbb{Z}$, consideramos el subanillo

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

Definimos la aplicación $N\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ como $N(a + b\sqrt{d}) = a^2 - db^2$. Demuestra que N cumple:

(i) $N(x) = 0$ si, y solo si, $x = 0$.

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

(iii) $x \in \mathcal{U}(\mathbb{Z}[\sqrt{d}])$ si, y solo si, $N(x) = \pm 1$. *Sugerencia: nota que* $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d})$.

10. Halla las unidades de $\mathbb{Z}[i]$ y $\mathbb{Z}[\sqrt{3}i]$. Decide si todo número primo $p \in \mathbb{Z}$ es primo en $\mathbb{Z}[i]$.
Sugerencia: considera primos de la forma $p = a^2 + b^2$ *para* $a, b \in \mathbb{Z}$.

11. Prueba que $\mathbb{Z}[\sqrt{3}i]$ no es un dominio de ideales principales. Demuestra que $\mathbb{Z}[\sqrt{3}i]$ tampoco es un dominio de factorización única.
Sugerencia: prueba que 2, $1 + \sqrt{3}i$ *y* $1 - \sqrt{3}i$ *son elementos irreducibles en* $\mathbb{Z}[\sqrt{3}i]$. *Nota que*

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

en particular en $\mathbb{Z}[\sqrt{3}i]$ *hay elementos irreducibles que no son primos.*

12. * ¿Cuántos elementos tiene el anillo $\mathbb{Z}[i]/(2i)$? ¿Se trata de un cuerpo?
Sugerencia: nota que $(2i) = (2) = 2\mathbb{Z}[i]$.

13. 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.

14. Demuestra que si $\varphi\colon R \to S$ es un homomorfismo de anillos y $a \in \mathcal{U}(R)$, entonces $\varphi(a) \in \mathcal{U}(S)$. ¿Es cierto el recíproco?

15. Sea $\varphi\colon R \to S$ un homomorfismo de anillos biyectivo. Prueba que si $a \in R$ es irreducible, entonces $\varphi(a) \in S$ es irreducible. ¿Qué ocurre si solo asumes que φ es sobreyectivo?
Sugerencia: considera el epimorfismo evaluación $e_1\colon \mathbb{Q}[x] \to \mathbb{Q}$ *para responder a la segunda pregunta.*

16. Demuestra que:

a) No existe ningún homomorfismo de anillos (cuerpos) $\varphi\colon \mathbb{Q} \to \mathbb{Z}_p$ para ningún primo $p \in \mathbb{Z}$.

b) No existe ningún homomorfismo de anillos (cuerpos) $\varphi\colon \mathbb{R} \to \mathbb{Q}$.

Anillos de polinomios

17. Prueba que $I = (2, x) \subseteq \mathbb{Z}[x]$ no es un ideal principal. En particular, $\mathbb{Z}[x]$ no es un dominio de ideales principales.

18. 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. ¿Qué ocurre si R no es un dominio de integridad? Concluye que el anillo de polinomios $R[x]$ es un dominio de integridad si, y solo, si R es un dominio de integridad.

19. 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 de integridad?
Sugerencia: para la segunda parte considera $\mathbb{Z}_4[x]$.

20. (Homomorfismo evaluación) Sea R un anillo y $a \in R$, prueba que la aplicación $e_a\colon R[x] \to R$ definida por $p \mapsto p(a)$ es un homomorfismo de anillos sobreyectivo. Si R es un cuerpo, concluye que $\ker(e_a)$ es un ideal maximal de $R[x]$.

21. Fijado un entero $n \in \mathbb{Z}$ con $n \geq 2$, 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 solo si, n es un número primo.

22. ** Demuestra que en $\mathbb{Z}[x]$ el ideal $(5, x+2)$ es maximal y que el anillo cociente $\mathbb{Z}[x]/(5, x+2)$ es isomorfo al cuerpo $\mathbb{Z}_5$.
Sugerencia: prueba que $\mathbb{Z}[x]/(5, x+2) \cong \mathbb{Z}_5[x]/(x+2)$ y que $(x+2) = \ker(e_{-2})$.

23. ¿Cuántos elementos tiene el anillo $\mathbb{Z}_3[x]/(x^2+x+1)$? ¿Se trata de un cuerpo?
Sugerencia: usa el algoritmo de la división.

24. Sea $p \in \mathbb{Q}[x]$ dado por $p(x) = (x^2+1)(x^4+2x+2)$. Escribimos $R = \mathbb{Q}[x]/(p)$ y $\bar{f} = f + (p)$.

a) Describe los ideales en R. ¿Es R un cuerpo?

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.
Sugerencia: el teorema del máximo común divisor y el algoritmo de la división son relevantes.

25. Halla un generador de $I = (x^3+1, x^2+1)$ en $\mathbb{Z}_2[x]$.

26. Sea K un cuerpo. Demuestra que si $p \in K[x]$ es un polinomio no nulo de grado n entonces p tiene, a lo sumo, n raíces.
Sugerencia: usa inducción sobre el grado y el algoritmo de división en $K[x]$.

27. Demuestra que si K es un cuerpo infinito y $f, g \in K[x]$ son tales que $f(a) = g(a)$ para todo $a \in K$, entonces $f = g$. ¿Qué ocurre si K es finito?
Sugerencia: para la segunda parte, considera $f(x) = x^p - x$ en $\mathbb{Z}_p[x]$.

28. Si $f \in \mathbb{Z}[x]$ y $r/s \in \mathbb{Q}$ es una raíz de f con $(r,s) = 1$, entonces s divide al coeficiente director de f y r divide al término independiente de f. En particular, las raíces racionales de polinomios enteros mónicos son números enteros.

Criterios de irreducibilidad

29. 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 solo si, $p(x) = (x-a)q(x)$ con $q \in K[x]$.

b) Todo polinomio de grado uno en $K[x]$ es irreducible.

c) Todo polinomio de grado dos o tres en $K[x]$ es irreducible si, y solo si, no tiene raíces en K.

30. Enumera todos los polinomios irreducibles de grado 1, 2, 3 y 4 de $\mathbb{Z}_2[x]$ y $\mathbb{Z}_3[x]$.

31. ¿Cuántos elementos tiene el anillo $\mathbb{Z}_3[x]/(x^2+1)$? ¿Se trata de un cuerpo?

32. Sea R un anillo y sea $a \in R$. Si $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$, definimos $f(x+a) = a_0 + a_1(x+a) + \cdots + a_n(x+a)^n \in R[x]$.

a) Demuestra que $f(x)$ es irreducible si, y solo si, $q(x) = f(x+a)$ es irreducibles.

b) Usa este resultado para probar que los polinomios $\Phi_p(x) = x^{p-1} + \cdots x + 1$ son irreducibles para todo p primo.
Sugerencia: prueba que $\Phi_p(x)(x-1) = x^p - 1$ y, a continuación, demuestra que $\Phi_p(x+1)$ es irreducible usando el criterio de Einsestein.

El polinomio Φ_p es el p-ésimo polinomio ciclotómico.

33. Sea $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ en $K[x]$ con $a_0 \cdot a_n \neq 0$. Prueba que f es irreducible si, y solo si, $\tilde{f}(x) = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$ es irreducible.

34. Decimos que un polinomio $f(x) \in \mathbb{Z}[x]$ es primitivo si el máximo común divisor de sus coeficientes es 1.

a) Prueba que un homomorfismo de anillos $f\colon R \to S$ se extiende de manera natural a un homomorfismo de anillos $R[x] \to S[x]$. En particular, si p es un primo, la reducción de coeficientes módulo p define un homomorfismo de anillos $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$.

b) Demuestra que en $\mathbb{Z}[x]$ el producto de dos polinomios primitivos es primitivo.
Sugerencia: usa el apartado anterior.

c) (Lema de Gauss) 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 es reducible como polinomio en $\mathbb{Z}[x]$.

d) Sea $f(x) \in \mathbb{Z}[x]$ mónico y se $p \in \mathbb{Z}$ un primo. Consideramos $\bar{f}(x) \in \mathbb{Z}_p[x]$ la imagen de f via el homomorfismo de anillos $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Demuestra que si $\bar{f}(x)$ 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 $\mathbb{Q}[x]$.

35. Discute la irreducibilidad del polinomio $x^5 + 11x^2 + 15$ en $\mathbb{Q}[x]$.
Sugerencia: usar reducción de coeficientes módulo $p = 2$ y probar que el polinomio resultante es irreducible en $\mathbb{Z}_2[x]$.

36. ** Prueba que el polinomio $x^4 + 1$ es irreducible en $\mathbb{Q}[x]$ pero reducible en $\mathbb{Z}_p[x]$ para todo primo p.
Sugerencia: deja los casos en que p es impar para más adelante.

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

$$f_1(x) = x^4 + 3x + 6, \quad f_2(x) = x^3 + 11^{11}x + 13^{13}, \quad f_3(x) = x^5 - 9x^2 + 1.$$

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

39. Demuestra que todo polinomio irreducible en $\mathbb{R}[x]$ tiene grado 1 o 2. Factoriza $x^4 - 1$ como producto de polinomios mónicos irreducibles en $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_2[x]$ y $\mathbb{Z}_3[x]$.

Cuerpos

Cuando p es un número primo, el anillo $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ tiene estructura de cuerpo. Cuando pensamos en $\mathbb{Z}_p$ como cuerpo, es común usar la notación $\mathbb{F}_p$.

40. Sea K un cuerpo de característica p. Demuestra que no existe ningún homomorfismo de anillos (cuerpos) $\varphi\colon K \to \mathbb{Q}$ para ningún primo $p \in \mathbb{Z}$.

41. (Frobenius) Sea K un cuerpo de característica p, probar que

$$(a+b)^p = a^p + b^p\,,$$

para todo $a, b \in K$. En particular, la aplicación $\mathrm{Frob}\colon K \to K$ dada por $a \mapsto a^p$ es un homomorfismo de anillos inyectivo. Además, Frob fija el cuerpo primo de K.

42. Si $n > 0$ no es un cuadrado. Demuestra que:

a) $\mathbb{F}_3[\xi] = \{a + b\xi \mid a, b \in \mathbb{F}_3,\ \xi^2 = -1\}$ es un cuerpo. ¿Ha aparecido antes en esta hoja de problemas?

b) $\mathbb{Q}[\sqrt{n}] := \{a + b\sqrt{n} : a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{R}$.

c) $\mathbb{Q}[\sqrt{-n}] := \{a + b\sqrt{-n} : a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{C}$.

d) No existe ningún homomorfismo de anillos (cuerpos) $\varphi\colon \mathbb{Q}[i] \to \mathbb{Q}[\sqrt{2}]$.

e) Existen infinitos homomorfismos de anillos (cuerpos) $\varphi\colon \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$.