Estructuras Algebraicas

Hoja 6. Divisibilidad y factorización en dominios.

Por anillo siempre entenderemos dominio de integridad.

---

1. 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 $ev_1\colon \mathbb{Q}[x] \to \mathbb{Q}$ para responder a la segunda pregunta.

2. Demuestra que en el anillo $\mathbb{Z}[\sqrt{-5}]$ los elementos 2, 3, $1 \pm \sqrt{-5}$ son irreducibles pero no son primos.

3. Prueba que $\mathbb{Z}[\sqrt{-3}]$ no es un dominio de factorización única mostrando dos factorizaciones distintas de 4. ¿Es $\mathbb{Z}[\sqrt{-3}]$ un dominio de ideales principales?

4. Sea $\varphi\colon A \to B$ un homomorfismo de anillos. Prueba que si A es un cuerpo entonces φ es necesariamente inyectivo.

5. Demuestra que:

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

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

6. Prueba que el grupo de automorfismos del cuerpo $\mathbb{Q}$ es trivial.

7. Prueba que el grupo de automorfismos del cuerpo $\mathbb{R}$ es trivial. (*Sugerencia: usa el ejercicio anterior junto con el hecho de que, por ser un cuadrado, todo elemento estrictamente positivo ha de tener imagen estrictamente positiva, lo cual, a su vez, implica que cualquier automorfismo debe preservar el orden*).

8. Prueba que el grupo de los automorfismos del cuerpo $\mathbb{Q}[i]$ es isomorfo a C_2.

9. Deduce del ejercicio anterior que el grupo de los automorfismos contínuos del cuerpo $\mathbb{C}$ es isomorfo a C_2.

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

11. Factoriza los siguientes polinomios en su correspondiente anillo:

a) $X^5 + 2X + 2 \in \mathbb{Q}[X]$;

b) $X^4 - 1$ en $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{F}_2[X]$ y $\mathbb{F}_3[X]$;

c) $X^4 + X^3 - X^2 \in \mathbb{F}_2[X]$.

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

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

14. 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 $\mathbb{F}_p[x]$.

15. Sea p un número primo.

a) Demuestra que todos los elementos del grupo multiplicativo $\mathbb{F}_p{}^*$ son raíces del polinomio $X^{p-1} - 1$.

b) Deduce que el polinomio $X^{p-1} - 1 \in \mathbb{F}_p[X]$ factoriza como producto de $p-1$ polinomios mónicos de grado uno.

16. Sea K un cuerpo finito de característica p.

a) Demuestra que $(x+y)^p = x^p + y^p$ para todo $x, y \in K$.

b) Concluye que la aplicación $\phi\colon K \to K$ definida como $\phi(x) = x^p$ es un automorfismo de K. El automorfismo ϕ se denomina *automorfismo de Frobenius* de K.

17. Encuentra un generador del ideal de $\mathbb{Q}[X]$ generado por los polinomios X^4+3X^3+2X+4 y X^2-X-1 y exprésalo en términos de estos polinomios.

18. Construye cuerpos con 8, 25 y 125 elementos como cocientes de anillos de polinomios adecuados.

Ejercicios Adicionales

19. Demuestra que todo cuerpo finito K tiene p^n elementos para algún $n \in \mathbb{N}$.
Sugerencia: Si $\mathrm{char}(K) = p$ *entonces* K *contiene al cuerpo* $\mathbb{F}_p$ *y es, por tanto, un espacio vectorial sobre él.*

20. Sea G un grupo abeliano $G = G(q_1) \times \cdots \times G(q_d)$ su descomposición como producto directo de sus q_j-subgrupos de Sylow.

a) Prueba que G es cíclico si, y solo si, cada $G(q_j)$ lo es.

b) Sea K un cuerpo finito y consideremos el grupo $G = K^*$. Demuestra que cada q-subgrupo de Sylow Q de G es cíclico. (*Sugerencia: Basta probar que* Q *solo puede tener un subgrupo de orden* q*, lo cual es consecuencia de que el polinomio* $x^q - 1$ *no puede tener más de* q *raíces*).

c) Concluye que el grupo multiplicativo de un cuerpo finito es cíclico.

21. Sea $p \in \mathbb{Z}$ un número primo. Se considera el conjunto

$$\mathbb{Z}_{(p)} := \left\{ x \in \mathbb{Q} : x = \frac{r}{s} \text{ donde } r, s \in \mathbb{Z} \text{ y } \ p \text{ no divide a } s \right\}.$$

a) Demuestra que $\mathbb{Z}_{(p)}$ es un subanillo de $\mathbb{Q}$ y halla el conjunto de las unidades $U(\mathbb{Z}_{(p)})$. El anillo $\mathbb{Z}_{(p)}$ es el *localizado* de $\mathbb{Z}$ en (p).

b) Identifica el cuerpo de fracciones de $\mathbb{Z}_{(p)}$.

c) Prueba que $\mathbb{Z}_{(p)}$ es un anillo de ideales principal (y, por tanto, dominio de factorización única), demostrando que todos sus ideales son de la forma $(p^k) := p^k\mathbb{Z}_{(p)}$. Muestra la factorización en elementos irreducibles de $75/8$ en $\mathbb{Z}_{(p)}$ para $p = 3, 5$ y 7. (¿Por qué no se pregunta para $p = 2$?)

d) Deduce que $(p) := p\mathbb{Z}_{(p)}$ es el único ideal maximal de $\mathbb{Z}_{(p)}$.

e) Calcula el núcleo del (único) homomorfismo $\mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$.

f) Demuestra que el homomorfismo $\mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ anterior es suprayectivo.
(Sugerencia: Dado $r/s \in \mathbb{Z}_{(p)}$ *escribe una identidad de Bezout para los números enteros* sr *y* pr*).*

g) Utiliza el teorema de isomorfía relativo al homomorfismo anterior para identificar qué cuerpo es el anillo cociente de $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$.

22. Fijado un primo $p \in \mathbb{Z}$, considera $G = \mathrm{GL}_2(\mathbb{F}_p)$ el conjunto de matrices (2×2) invertibles con entradas en el cuerpo $\mathbb{F}_p$.

a) Demuestra que G es un grupo con el producto habitual de matrices.

b) Justifica que $|G| = (p^2-1)(p^2-p) = p(p-1)^2(p+1)$.

c) Demuestra que el conjunto P de matrices unitriangulares superiores es un p-subgrupo de Sylow de G isomorfo al grupo aditivo de $\mathbb{F}_p$.

d) Demuestra que $\mathbf{N}_G(P)$ es el subgrupo de G formado por las matrices triangulares superiores. Deduce que el número de subgrupos de G conjugados a P es $p+1$.

e) Demuestra que $\mathbf{N}_G(P)/\mathbf{C}_G(P)$ es cíclico.
Sugerencia: Usa que el grupo multiplicativo de un cuerpo finito es cíclico, por el Ejercicio 20.c).