ÁLGEBRA 3
Segundo cuatrimestre — 2019

Práctica 0: Preliminares

A menos que se indique lo contrario, todos los anillos son conmutativos y con unidad 1, distinta de 0. Más aún, los morfismos de anillos mandan 1 en 1.

1. Sea A un anillo.

(a) Existen en A ideales maximales y, de hecho, todo ideal propio de A está contenido en uno maximal.

(b) Un ideal $\mathfrak{p}$ de A es primo sii el cociente $A/\mathfrak{p}$ es un dominio íntegro.

(c) Un ideal $\mathfrak{m}$ de A es maximal sii el cociente $A/\mathfrak{m}$ es un cuerpo.

(d) Un anillo es un cuerpo sii posee exactamente dos ideales.

2. Un anillo A es un cuerpo sii todo morfismo de anillos $f : A \to B$ es inyectivo.

3. Un dominio íntegro finito es un cuerpo [1].

4. (a) Si B es un anillo, $A \subseteq B$ un subanillo y $b \in B$, existe un único menor subanillo de B que contiene tanto a A como a b, y lo escribimos $A[b]$. Se tiene

$$A[b] = \left\{ \sum_{i=0}^{n} a_i b^i : n \geq 0,\ a_0, \ldots, a_n \in A \right\}.$$

(b) Los subanillos $\mathbb{Q}\left[\sqrt{2}\right]$, $\mathbb{Q}\left[\sqrt{3}\right]$, $\mathbb{Q}[i]$ y $\mathbb{Q}\left[\sqrt[3]{2}\right]$ de $\mathbb{C}$ son cuerpos.

5. (a) Sea K un cuerpo y $f \in K[X]$. El anillo $K[X]/(f)$ es un cuerpo sii f es irreducible.

(b) Construya un cuerpo de 9 elementos. Más generalmente, construya un cuerpo de p^2 elementos para cada primo p.

(c) Muestre que $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$.

6. Describa todos los morfismos de cuerpos

(a) $\mathbb{C} \to \mathbb{R}$;

(b) $\mathbb{Q} \to \mathbb{F}_p$;

(c) $\mathbb{Q} \to K$, con K un cuerpo;

(d) $\mathbb{Q}\left[\sqrt{2}\right] \to \mathbb{Q}\left[\sqrt{2}\right]$;

(e) $\mathbb{Q}[\sqrt{2}] \to \mathbb{Q}\left[\sqrt{3}\right]$;

(f) $\mathbb{Q}\left[\sqrt[3]{2}\right] \to \mathbb{Q}\left[\sqrt[3]{2}\right]$;

(g) $\mathbb{R} \to \mathbb{R}$;

(h) $\mathbb{C} \to \mathbb{C}$, que son $\mathbb{R}$-lineales.

7. Sea K un cuerpo. Una K-álgebra de dimensión finita que es un dominio íntegro es un cuerpo.

8. Si A es un anillo, escribimos $U(A)$ al conjunto de elementos inversibles de A.

(a) El conjunto $U(A)$ es un grupo con la multiplicación de A, al que llamamos *grupo de unidades* de A.

[1] Más aún, el resultado es válido sin pedirle al anillo que sea conmutativo, y se conoce como *pequeño teorema de Wedderburn*.

(*b*) Determine los grupos de unidades de $\mathbb{Z}$, de un cuerpo, de $\mathbb{Z}[i]$, de $\mathbb{Z}\left[\sqrt{-5}\right]$, de $\mathbb{Z}/n\mathbb{Z}$ y de $A[X]$, si A es un dominio íntegro.

9. (*a*) Si A es un dominio íntegro, entonces $A[X]$ también lo es.

(*b*) Si A es un dominio íntegro, entonces $A[X_1, \ldots, X_n]$ también lo es.

(*c*) ¿Que puede decir de $A[X_i, i \in I]$ si A es un dominio íntegro y el conjunto I es *arbitrario*?

10. Sea A un dominio íntegro.

(*a*) La relación $\sim$ sobre el conjunto $X = A \times (A \setminus \{0\})$ tal que si $(a, b), (c, d) \in X$ es

$$(a, b) \sim (c, d) \iff ad = cb$$

es una relación de equivalencia.

(*b*) Sea $K(A) = X/\sim$ y escribamos $[a, b]$ a la clase de equivalencia de $(a, b) \in X$ en $K(A)$. Muestre que existen operaciones $+, \cdot : K(A) \times K(A) \to K(A)$ tales que para todo $(a, b), (c, d) \in X$,

$$[a, b] + [c, d] = [ad + bc, bd], \qquad [a, b] \cdot [c, d] = [ac, bd]$$

que $(K(A), +, \cdot)$ es un cuerpo y que la función $\iota : a \in A \mapsto [a, 1] \in K(A)$ es un morfismo de anillos.

(*c*) Si $h : A \to L$ es un monomorfismo de anillos con codominio en un cuerpo L, entonces existe exactamente un morfismo de anillos $\bar{h} : K(A) \to L$ tal que $\bar{h} \circ \iota = h$.

Llamamos al par ordenado $(K(A), \iota)$ el *cuerpo de fracciones* de A, aunque generalmente dejamos al morfismo ι implícito, y decimos que $K(A)$ mismo es el cuerpo de fracciones de A.

(*d*) Un anillo B es un dominio íntegro sii existe un morfismo inyectivo de anillos $B \to Q$ con codominio en un cuerpo.

(*e*) Describa explícitamente el cuerpo de fracciones de los anillos $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}\left[\sqrt{2}\right]$ y, si A es un dominio íntegro, $A[X]$.

11. Sea A un anillo.

(*a*) Sea $f : A \to B$ un morfismo de anillos. Para cada $b \in B$ existe exactamente un morfimo de anillos $e_b : A[X] \to B$ que extiende a f y tal que $e_b(X) = b$. Llamamos a e_b la *especialización* en b.

Recíprocamemente, todo morfimo de anillos $A[X] \to B$ que extiende a f es la especialización en algún elemento de b.

(*b*) Si A es un dominio íntegro, determine el grupo de automorfismos $A[X] \to A[X]$ que extienden a la inclusión $A \hookrightarrow A[X]$.

12. (*a*) Todo elemento primo de un dominio íntegro es irreducible, pero la implicación recíproca no es necesariamente cierta.

(*b*) En un dominio de factorización única todo elemento irreducible es primo.

(*c*) En $\mathbb{Z}\left[\sqrt{-5}\right]$ los números 3, 7, $4 + \sqrt{-5}$, $4 - \sqrt{-5}$, $1 + 2\sqrt{-5}$ y $1 - 2\sqrt{-5}$ son irreducibles pero no primos, de manera que ese anillo no es un dominio de factorización única.

(*d*) Un dominio de ideales principales es un dominio de factorización única, pero la recíproca no es cierta.

13. Un *dominio euclideano* es un dominio A dotado de una función $N : A \setminus \{0\} \to \mathbb{N}$ tal que

(i) si $a, b \in A \setminus \{0\}$, existe $q, r \in A$ tales que $a = qb + r$, con o bien $r = 0$ o bien $N(r) < N(b)$;

(ii) si $a, b \in A \setminus \{0\}$, entonces $N(a) \leq N(ab)$.

(a) Muestre que si $N : A \setminus \{0\} \to \mathbb{N}$ es una función que satisface la primera de estas dos condiciones, entonces la función $N' : A \setminus \{0\} \to \mathbb{N}$ dada por

$$N'(a) = \min_{b \in A \setminus \{0\}} N(ab)$$

satisface las dos.

(b) Los anillos $\mathbb{Z}$, $\mathbb{Z}[i]$ y, si K es un cuerpo, $K[X]$ son euclideanos.

(c) Un anillo euclideano es un dominio de ideales principales.

14. Si p un primo racional, las siguientes afirmaciones son equivalentes:

(i) $X^2 + 1$ es irreducible en $\mathbb{F}_p[X]$;

(ii) -1 no es un cuadrado en $\mathbb{F}_p$;

(iii) $p \equiv 3 \mod 4$.

(iv) p no es suma de dos cuadrados en $\mathbb{Z}$;

(v) p es irreducible en $\mathbb{Z}[i]$.

Irreducibilidad

15. *Lema de Gauss.* Sea A un dominio de factorización única, sea K su cuerpo de cocientes y sea $f \in A[X]$. Si f es irreducible en $A[X]$, entonces f es irreducible en $K[X]$. Probar que la recíproca vale si f es primitivo.

16. Sea p un primo racional y sea $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ el único morfismo de anillos tal que $\pi(X) = X$. Sea $f \in \mathbb{Z}[X]$ tal que $\pi(f)$ es un polinomio no nulo cuyo grado coincide con el grado de f. Si $\pi(f)$ es irreducible en $\mathbb{F}_p[X]$, entonces f no se factoriza en $\mathbb{Z}[X]$ como producto de factores de grado positivo.

17. Si A es un dominio de factorización única, entonces $A[X]$ también. ¿Qué sucede con $A[X_1, \ldots, X_n]$ y con $A[X_i, i \in I]$ con I un conjunto arbitrario?

18. *Criterio de Eisenstein.* Sea A un dominio de factorización única y sea K su cuerpo de cocientes. Sea $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ con $n > 0$ y a_n.

Si existe un primo $p \in A$ tal que $p \nmid a_n$, $p \mid a_i$ para cada $i \in \{0, \ldots, n-1\}$ y $p^2 \nmid a_0$, entonces f no se factoriza en $A[X]$ como producto de factores de grado positivo.

19. *Teorema de Gauss.* Sea A un dominio de factorización única y sea K su cuerpo de cocientes. Sea $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ con $n > 0$ y $a_0 a_n \neq 0$. Si p y q son elementos no nulos de A coprimos entre sí y tales que $f(p/q) = 0$, entonces $p \mid a_0$ y $q \mid a_n$.

20. Si p es un primo racional, entonces

(a) $(X+1)^p - 1$ se factoriza en $\mathbb{Q}[X]$ como producto de X y de un único otro factor irreducible;

(b) el polinomio $1 + X + X^2 + \cdots + X^{p-1}$ es irreducible en $\mathbb{Q}[X]$;

(c) el polinimio $X^n - p$ es irreducible en $\mathbb{Q}[X]$ para todo $n \in \mathbb{N}$.

¿Cuáles de estas propiedades son equivalentes a la primalidad de p?

21. Sea K un cuerpo.

(a) Existe exactamente una función K-lineal $\partial : K[X] \to K[X]$ tal que $\partial(X) = 1$ y

$$\partial(f \cdot g) = \partial(f) \cdot g + f \cdot \partial(g)$$

para cada f, $g \in K[X]$.

(b) Sea $f \in K[X]$ y $a \in K$ una raíz de f. Entonces a es una raíz múltiple de f sii es raíz de $\partial(f)$.

22. Todas las raíces de un polinomio con coeficientes racionales que es irreducible son simples.

23. Los polinomios $\sum_{i=0}^{n} X^i$ y $\sum_{i=0}^{n} X^i/i!$ tienen a todas sus raíces complejas simples, cualquiera sea $n \in \mathbb{N}$.

24. Sean a, $b \in \mathbb{Z}$.

(a) El polinomio $X^3 + aX^2 + bX + 1$ es reducible en $\mathbb{Z}[X]$ sii $a = b$ o $a + b = -2$.

(b) Encuentre condiciones necesarias y suficientes sobre a y b para que el polinomio $X^3 + aX^2 + bX - 1$ sea reducible.

25. ¿Para qué valores de $b \in \mathbb{Z}$ es reducible el polinomio $X^3 + b$?

26. Factorice el polinomio $X^5 + X^4 + X^2 + X + 2$ en $\mathbb{Q}[X]$.

27. Estudie la reducibilidad de los siguientes polinomios:

(a) $2X^5 + 18X^3 + 30X^2 - 24$, $X^4 + 4X^2 + 10$, $X^3 - X^2 + 7X + 2$, tanto en $\mathbb{Q}[X]$ como en $\mathbb{Z}[X]$;

(b) $X^4 - 4$, $X^3 + X^2 + X + 1$, $X^4 + X^3 + 1$, $X^5 + 6X^4 + 5X^2 - 2X + 9$ en $\mathbb{Z}[X]$;

(c) $(X + a)^4 + 1$ en $\mathbb{Q}[X]$, para cada $a \in \mathbb{Q}$;

(d) $X^2 + Y^2 + 1$ en $\mathbb{Q}[X, Y]$.

28. Si K es un cuerpo y $a \in K$, entonces el polinomio $X^4 - a$ es reducible en $K[X]$ sii existe $b \in K$ tal que $a = b^2$ o $a = -4b^4$.

29. (a) Encuentre todos los polinomios irreducibles de grados 2, 3, 4 y 5 en $\mathbb{F}_2[X]$.

(b) Si K tiene q elementos, ¿cuántos polinomios irreducibles hay en $K[X]$ de grado 2? ¿Y de grado 3?

Heinrich Martin Weber
1842–1913, Alemania

En 1893 Weber dio la primera definición precisa de lo que hoy entendemos por un cuerpo. Trabajó en álgebra y en teoría de números. Particularmente importante es su contribución a la pueba del llamado teorema de Kronecker-Weber que describe a todas las extensiones abelianas de $\mathbb{Q}$, aunque su demostración —como la de Kronecker— contenía agujeros y errores; la primera demostración completa de ese teorema fue dada por David Hibert en 1896.

La palabra *cuerpo* fue introducida por Richard Dedekind en sus clases alrededor de 1859; en alemán, la palabra usada por Dedekind es *Zahlkörper*, y de ahí viene el uso tradicional de la letra k para denotar a los cuerpos. El primero en usar la palabra *field* en inglés fue Eliakim Hastings Moore, en un artículo publicado en 1893 a propósito de los cuerpos finitos; ese es el origen del uso de la letra F para los cuerpos.