Álgebra III

Práctica 1 – Segundo Cuatrimestre de 2018

Nota: En esta práctica la palabra anillo significará anillo conmutativo con identidad $1 \neq 0$, y todo morfismo de anillos $f : A \to B$ manda el 1_A en el 1_B.

Repaso de anillos, cuerpos y morfismos

Ejercicio 1. Sean A, B anillos y $f : A \to B$ un morfismo de anillos. Probar que:

i) A tiene ideales maximales y todo ideal propio está contenido en un ideal maximal.

ii) $\mathfrak{p}$ es un ideal primo de A si y sólo si $A/\mathfrak{p}$ es un dominio íntegro.

iii) $\mathfrak{m}$ es un ideal maximal de A si y sólo si $A/\mathfrak{m}$ es un cuerpo.

iv) Si $\mathfrak{p}$ es un ideal primo de B entonces $f^{-1}(\mathfrak{p})$ es un ideal primo de A.

v) Si f es sobreyectivo y $\mathfrak{m}$ es un ideal maximal de B entonces $f^{-1}(\mathfrak{m})$ es un ideal maximal de A.

vi) Si $\mathbb{K}$ es un cuerpo y $f : \mathbb{K} \to B$ es un morfismo de anillos, entonces f es inyectivo.

vii) Sea D un dominio íntegro finito. Probar que D es un cuerpo.

Ejercicio 2. Dado $b \in \mathbb{C}$ se define $\mathbb{Q}[b] = \left\{ \sum_{i=0}^{n} a_i\, b^i \,/\, a_i \in \mathbb{Q} \right\}$. Probar que $\mathbb{Q}[\sqrt{2}\,]$, $\mathbb{Q}[\sqrt{3}\,]$, $\mathbb{Q}[i]$ y $\mathbb{Q}[\sqrt[3]{2}\,]$ son cuerpos. ¿Cómo se podría generalizar esto?

Ejercicio 3. Caracterizar los siguientes conjuntos:

i) $\{f : \mathbb{R} \to \mathbb{C} \,:\, f \text{ isomorfismo de cuerpos}\}$.

ii) $\{f : \mathbb{C} \to \mathbb{R} \,:\, f \text{ morfismo de cuerpos}\}$.

iii) $\{f : \mathbb{Q} \to \mathbb{F}_p \,:\, f \text{ morfismo de cuerpos}\}$ (p primo).

iv) $\{f : \mathbb{Q} \to \mathbb{K} \,:\, f \text{ morfismo de cuerpos}\}$, $\mathbb{K}$ cuerpo fijo.

v) $\{f : \mathbb{Q}[\sqrt{2}\,] \to \mathbb{Q}[\sqrt{3}\,] \,:\, f \text{ morfismo de cuerpos}\}$.

vi) $\{f : \mathbb{C} \to \mathbb{C} \,:\, f \text{ morfismo de cuerpos y } f(a) = a \;\forall\, a \in \mathbb{R}\,\}$.

vii) $\{f : \mathbb{Q}[i] \to \mathbb{Q}[i] \,:\, f \text{ morfismo de cuerpos}\}$.

vii) $\{f : \mathbb{Q}[i] \to \mathbb{Q}[i] \,:\, f \text{ isomorfismo de cuerpos}\}$.

ix) $\{f : \mathbb{Q}[i] \to \mathbb{R} \,:\, f \text{ morfismo de cuerpos}\}$.

x) $\{f : \mathbb{R} \to \mathbb{R} \,:\, f \text{ morfismo de cuerpos}\}$.

Ejercicio 4. Sea $\mathbb{K}$ un cuerpo y sea A una $\mathbb{K}$-álgebra de dimensión finita. Probar que si A es un dominio íntegro, entonces es un cuerpo.

Ejercicio 5. Sea A un anillo. Notamos $\mathcal{U}(A)$ al conjunto de los elementos de A que tienen inverso multiplicativo.

i) Probar que $(\mathcal{U}(A)\,,\cdot\,)$ es un grupo, llamado el *grupo de unidades* de A.

ii) Caracterizar el grupo de unidades de los siguientes anillos:
$\mathbb{Z}$, $\mathbb{K}$ ($\mathbb{K}$ cuerpo), $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-5}\,]$, $A[X]$ (A dominio íntegro), $\mathbb{Z}/n\mathbb{Z}$.

Ejercicio 6. Sea A un dominio íntegro. Consideremos en el conjunto $A\times A-\{\,0\,\}$ la relación de equivalencia

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

Definimos en $K=A\times A-\{\,0\,\}\,/\sim$ las siguientes operaciones:

$$\begin{aligned}(a,b)+(c,d) &= (ad+cb,bd)\\ (a,b)\cdot(c,d) &= (ac,bd)\end{aligned}$$

i) Probar que $(K,+\,,\,\cdot\,)$ es un cuerpo, llamado el *cuerpo de fracciones* (o de cocientes) del anillo A.

ii) Probar que $f:A\to K$ definida por $f(a)=(a,1)$ es un monomorfismo de anillos.

iii) Sea D un anillo. Probar que son equivalentes:

   (a) D es un dominio íntegro.

   (b) Existe $f:D\to K$ monomorfismo de anillos para algún cuerpo K.

Ejercicio 7. Caracterizar el cuerpo de fracciones de los siguientes dominios íntegros:

$$\mathbb{Z}\,;\ \mathbb{Z}[i]\,;\ \mathbb{Z}[\sqrt{2}\,]\,;\ A[X]\ (A \text{ dominio íntegro})\,;\ \mathbb{K}\ (\mathbb{K} \text{ cuerpo}).$$

Dominios de factorización única, álgebras de polinomios e irreducibilidad de polinomios

Ejercicio 8. Probar que si A es un dominio íntegro entonces $A\,[(X_i)_{i\in I}]$ es un dominio íntegro.

Ejercicio 9. Sea A un dominio íntegro y sea $a\in A$. Probar que:

i) Si a es primo, entonces a es irreducible.

ii) Si A es DFU (dominio de factorización única), a irreducible implica a primo.

iii) Verificar que en general no vale que irreducible implica primo.
Sugerencia: $\mathbb{Z}[\sqrt{-5}]$

iv) Si A es DFU entonces $A\,[(X_i)_{i\in I}]$ es DFU.

v) Si A es principal entonces A es DFU, pero no vale la recíproca.

Ejercicio 10. Un dominio íntegro A se dice *euclideano* si está provisto de un algoritmo de división, es decir, si existe $g : A - \{0\} \to \mathbb{N} \cup \{0\}$ que satisface las dos condiciones siguientes:

- $\forall\, a, b \in A - \{0\}$, si $a \mid b$ entonces $g(a) \leq g(b)$.
- $\forall\, a, b \in A - \{0\}$ existen $q,\ r \in A$ tales que $a = b \cdot q + r$ y $r = 0$ o $g(r) < g(b)$.

Probar que:

i) $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{K}$ y $\mathbb{K}[X]$ ($\mathbb{K}$ cuerpo) son anillos euclideanos.

ii) Si A es una anillo euclideano, entonces A es principal.

Ejercicio 11. Sea $p \in \mathbb{Z}$ primo. Probar que:

i) -1 es un cuadrado en $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ si y sólo si $p = 2$ o $p = 4k + 1$.

ii) p es irreducible en $\mathbb{Z}[i]$ si y sólo si p no es suma de dos cuadrados (en $\mathbb{Z}$).

iii) p es suma de dos cuadrados (en $\mathbb{Z}$) si y sólo si $p = 2$ o $p = 4k + 1$.

Ejercicio 12.

i) Sea $\mathbb{K}$ un cuerpo y sea $f \in \mathbb{K}[X]$. Probar que $\mathbb{K}[X]/\langle f \rangle$ es un cuerpo si y sólo si f es irreducible.

ii) Construir un cuerpo de 9 elementos.

iii) Probar que $\mathbb{R}[X]/\langle X^2 + 1 \rangle \simeq \mathbb{C}$.

Ejercicio 13. Sea A un DFU y sea $\mathbb{K}$ su cuerpo de cocientes. Probar que si $f \in A[X]$ es un polinomio irreducible de grado > 0 entonces, visto como polinomio con coeficientes en $\mathbb{K}$, también es irreducible. ¿Vale la recíproca? ¿Y agregando alguna hipótesis razonable?

Ejercicio 14. Sea $p \in \mathbb{N}$ primo, y sea $\Phi_p : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ definida por

$$\Phi_p(a_n X^n + \cdots + a_0) = \overline{a}_n X^n + \cdots + \overline{a}_0$$

donde $\overline{a}_i$ denota el resto de a_i módulo p.

i) Probar que $\Phi_p(f) + \Phi_p(g) \equiv \Phi_p(f + g) \pmod{p}$ y $\Phi_p(f) \cdot \Phi_p(g) \equiv \Phi_p(f \cdot g) \pmod{p}$.

ii) Sea $f \in \mathbb{Z}[X]$ tal que $\Phi_p(f) \neq 0$ y $\mathrm{gr}(\Phi_p(f)) = \mathrm{gr}(f)$. Probar que si $\Phi_p(f)$ es irreducible en $\mathbb{F}_p[X]$, entonces f no se factoriza en $\mathbb{Z}[X]$ en la forma $f = g\,h$ con g, h de grado mayor o igual que 1.

iii) Probar que $X^4 + 1$ es irreducible en $\mathbb{Z}[X]$ pero reducible en $\mathbb{F}_p[X]$ para todo primo p.

Ejercicio 15. *Criterio de irreducibilidad de Eisenstein.* Sea A un DFU y sea $\mathbb{K}$ su cuerpo de cocientes. Sea $f = \sum\limits_{i=0}^{n} a_i\, X^i \in A[X]$, con $n > 0$. Probar que si existe un primo $p \in A$ que verifica: $p \nmid a_n$, $p \mid a_i\ \forall\, 0 \leq i \leq n-1$ y $p^2 \nmid a_0$, entonces f es irreducible en $K[X]$.

Ejercicio 16. *Teorema de Gauss.* Sea A un DFU y sea $\mathbb{K}$ su cuerpo de cocientes. Sea $f = \sum\limits_{i=0}^{n} a_i\, X^i \in A[X]$ con $a_0 \neq 0$. Demostrar que si p y q son elementos no nulos de A, coprimos entre sí tales que $\frac{p}{q} \in \mathbb{K}$ es raíz de f, entonces $p \mid a_0$ y $q \mid a_n$ en A.

Ejercicio 17. Sea $p \in \mathbb{Z}$ primo. Probar que:

i) $(X+1)^p - 1$ es divisible por X y $\dfrac{(X+1)^p - 1}{X}$ es irreducible en $\mathbb{Q}[X]$.

ii) $1 + X + X^2 + \cdots + X^{p-1}$ es irreducible en $\mathbb{Q}[X]$.

iii) $X^n - p$ es irreducible en $\mathbb{Q}[X]\ \forall\, n \in \mathbb{N}$.

Ejercicio 18. Sea $n > 1$ un entero. Probar que $X^n + 5X^{n-1} + 3$ es irreducible en $\mathbb{Z}[X]$.

Ejercicio 19.

i) Sea $\mathbb{K}$ un cuerpo. Sea $f \in \mathbb{K}[X]$ y sea $a \in \mathbb{K}$ una raíz de f. Probar que a es raíz múltiple de f si y sólo si es raíz de su derivado.

ii) Probar que si $f \in \mathbb{Q}[X]$ es irreducible, entonces f no tiene raíces múltiples en $\mathbb{C}$.

iii) Probar que $\sum_{i=0}^{n} X^i$ no tiene raíces múltiples en $\mathbb{C}$.

iv) Probar que $\sum_{i=0}^{n} \frac{X^i}{i!}$ no tiene raíces múltiples en $\mathbb{C}$.

Ejercicio 20. Sean $a, b \in \mathbb{Z}$.

i) Probar que $X^3 + aX^2 + bX + 1$ es reducible en $\mathbb{Z}[X]$ si y sólo si $a = b$ o $a + b = -2$.

ii) Sea $\mathbb{K}$ un cuerpo y sea $a \in \mathbb{K}$. Probar que $X^4 - a$ es reducible en $\mathbb{K}[X]$ si y sólo si $a = b^2$ para algún $b \in \mathbb{K}$ o $a = -4c^4$ para algún $c \in \mathbb{K}$.

iii) Hallar a, b, c enteros no nulos distintos dos a dos tales que

$$X(X-a)(X-b)(X-c) + 1$$

sea reducible en $\mathbb{Z}[X]$.

iv) Factorizar $X^5 + X^4 + X^2 + X + 2$ en $\mathbb{Q}[X]$.

Ejercicio 21. Sean $a_1, a_2 \cdots, a_n$ enteros distintos dos a dos.

i) Probar que $(X - a_1)(X - a_2)\cdots(X - a_n) - 1$ es irreducible en $\mathbb{Z}[X]$.

ii) Probar que $(X - a_1)^2(X - a_2)^2 \cdots (X - a_n)^2 + 1$ es irreducible en $\mathbb{Z}[X]$.

Ejercicio 22. Analizar la reducibilidad de:

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

ii) $X^6 + tX^5 - t^2(t-1)X + t(t-1)$ en $\mathbb{Q}(t)[X]$.

iii) $X^7 + 15X^3 + 5$ en $\mathbb{Z}[i][X]$.

iv) $X^m - Y^n$ en $\mathbb{C}[X, Y]$ con $(m, n) = 1$.

Ejercicio 23. Sea $p \in \mathbb{Z}$ primo:

i) Probar que $P(X) = X^p - X - a \in \mathbb{F}_p[X]$ es irreducible si y sólo si $a \neq 0$.
Sugerencia: probar que si $Q(X)$ divide a $P(X)$, entonces $Q(X+1)$ también.

ii) Probar que $X^p - a \in \mathbb{Q}[X]$ es irreducible si y sólo si tiene alguna raíz racional.

Ejercicio 24. Sea $\mathbb{K}$ un cuerpo finito de q elementos. ¿ Cuántos polinomios mónicos irreducibles de grado 2 hay? ¿ Y de grado 3?

Ejercicio 25. Probar que $X^n + 4 \in \mathbb{Z}[X]$ es reducible si y sólo si n es múltiplo de 4.

Ejercicio 26. Probar que el polinomio $(X^2+X)^{2^n}+1$ es irreducible en $\mathbb{Z}[X]$ para todo n entero no negativo.
Sugerencia: $X^2 + X + 1$ es irreducible en $\mathbb{F}_2[X]$.

Continuará ...