Álgebra III

Práctica 1 – Segundo Cuatrimestre de 2012

Anillos, cuerpos y morfismos

Ejercicio 1. Sea A un anillo. Probar que:

i) A tiene ideales maximales.

ii) Para todo $\mathcal{I}$ ideal propio de A existe un ideal maximal de A que contiene a $\mathcal{I}$.

iii) $\bigcup\limits_{\mathcal{M} \text{ maximal}} \mathcal{M} = \{ x \in A \,/\, x \text{ no es unidad} \}$

iv) Si $\mathcal{M}$ es un ideal maximal de A entonces es un ideal primo. Mostrar que no vale la vuelta.

v) $\mathcal{P}$ es un ideal primo de A si y sólo si $A/\mathcal{P}$ es un dominio íntegro.

vi) A es un cuerpo si y sólo si tiene exactamente dos ideales.

vii) $\mathcal{M}$ es un ideal maximal de A si y sólo si $A/\mathcal{M}$ es un cuerpo.

Ejercicio 2. Sea $f : A \to B$ un morfismo de anillos. Probar que:

i) $\mathrm{Ker}(f)$ es un ideal propio de A.

ii) $\mathrm{Im}(f)$ es un subanillo de B.

iii) Si $\mathcal{I}$ es un ideal de B entonces $f^{-1}(\mathcal{I})$ es un ideal de A que contiene a $\mathrm{Ker}(f)$.

iv) Si $\mathcal{I}$ es un ideal de A y f es un *epimorfismo* entonces $f(\mathcal{I})$ es un ideal de B.

v) Si $\mathcal{I}$ es un ideal primo de B entonces $f^{-1}(\mathcal{I})$ es un ideal primo de A.

vi) Si f es un epimorfismo y $\mathcal{M}$ es un ideal maximal de B entonces $f^{-1}(\mathcal{M})$ es un ideal maximal de A.

Ejercicio 3. Probar que:

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

ii) Si A es un anillo tal que todo morfismo de anillos que tiene como conjunto de partida a A es inyectivo, entonces A es un cuerpo.

Ejercicio 4.

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

ii) Probar que $\mathbb{C}$ no tiene subcuerpos finitos.

Ejercicio 5. Dado $b \in \mathbb{C}$ se define $\mathbb{Q}[b] = \left\{ \sum\limits_{i=0}^{n} a_i\, b^i \,/\, a_i \in \mathbb{Q} \right\}$. Probar que $\mathbb{Q}[\sqrt{2}\,]$, $\mathbb{Q}[\sqrt{3}\,]$, $\mathbb{Q}[i]$ y $\mathbb{Q}[\sqrt[3]{2}\,]$ son cuerpos.

Ejercicio 6. Caracterizar los siguientes conjuntos:

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

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

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

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

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

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

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

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

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

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

Ejercicio 7. 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 8. 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), $\mathbb{Z}_n$.

Ejercicio 9. 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 10. Caracterizar el cuerpo de fracciones de los siguientes dominios íntegros:

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

Ejercicio 11. Sea $\mathbb{K}$ un cuerpo. Se definen en $\mathbb{K}\times\mathbb{K}$ las siguientes operaciones:

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

i) Probar que $(\,\mathbb{K}\times\mathbb{K}\,,\,+\,,\,\cdot\,)$ es un anillo.

ii) Probar que cuando $\mathbb{K}$ es $\mathbb{C}$, $\mathbb{Z}_2$ o $\mathbb{Z}_5$ entonces $(\,\mathbb{K}\times\mathbb{K}\,,\,+\,,\,\cdot\,)$ no es un cuerpo, mientras que si $\mathbb{K}$ es $\mathbb{R}$, $\mathbb{Z}_3$ o $\mathbb{Z}_7$ sí lo es.

iii) Probar que $(a,b)\in\mathbb{K}\times\mathbb{K}$ es inversible si y sólo si $a^2+b^2\neq 0$.

iv) Deducir que $\mathbb{K}\times\mathbb{K}$ es cuerpo si y sólo si $a^2+b^2=0$ en $\mathbb{K} \Leftrightarrow a=b=0$.

v) Probar que si p es primo, $\mathbb{Z}_p\times\mathbb{Z}_p$ es cuerpo si y sólo si p es de la forma $4k+3$, con $k\in\mathbb{Z}$.

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

Ejercicio 12. Probar que si A es un dominio íntegro entonces $A\left[(X_i)_{i\in I}\right]$ es un dominio íntegro.

Ejercicio 13. 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) En $A=\mathbb{Z}[\sqrt{-5}\,]$ los elementos 3, 7, $4+\sqrt{-5}$, $4-\sqrt{-5}$, $1+2\sqrt{-5}$ y $1-2\sqrt{-5}$ son irreducibles pero no primos. ¿Conclusiones?

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

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

vi) Si $f:A\to B$ es un isomorfismo de anillos, a es irreducible en A si y sólo si $f(a)$ es irreducible en B.

Ejercicio 14. Sean $A\subseteq B\subseteq C$ dominios íntegros. Dar un ejemplo en que A y C sean DFU y B no.

Ejercicio 15. 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 $g(a)\le g(b)$.
- $\forall\, a,b\in A-\{0\}$ existen $q,\ r\in A$ tales que $a=b\cdot q+r$ y $r=0$ o $g(r)<g(b)$.

Probar que:

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

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

Ejercicio 16. Sea $p \in \mathbb{Z}$ primo. Probar que:

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

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

iii) p es primo en $\mathbb{Z}[i]$ si y sólo si p es de la forma $4k + 3$.

Ejercicio 17. Sea A un dominio íntegro y sea $P \in A[X]$. Definimos $e_P : A[X] \to A[X]$ en la forma $e_P(Q) = Q(P(X))$. Probar que:

i) e_P es un morfismo de anillos, llamado *especialización en P*.

ii) Todo morfismo de anillos de $A[X]$ en $A[X]$ que vale la identidad sobre A es una especialización en algún P.

iii) Si una especialización e_P es un automorfismo de $A[X]$ entonces su inversa también es una especialización.

iv) e_{cX+b} es un automorfismo de anillos si y sólo si $c \in \mathcal{U}(A)$.

v) Si f es un automorfismo de $A[X]$ tal que $f(a) = a \ \forall\, a \in A$, entonces f es de la forma e_{cX+b} para algún $c \in \mathcal{U}(A)$.

Ejercicio 18.

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 19. 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?

Ejercicio 20. Sea $p \in \mathbb{N}$ primo, y sea $\Phi_p : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$ 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 $\mathbb{Z}_p[X]$, 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.

Ejercicio 21. *Criterio de irreducibilidad de Eisenstein.* Sea A un DFU y sea $\mathbb{K}$ su cuerpo de cocientes. Sea $f = \sum_{i=0}^{n} a_i X^i \in A[X]$, con $n > 0$. Probar que si existe un primo $p \in A$ que verifica: $p \nmid a_n$, $p \mid a_i \; \forall\, 0 \le i \le n-1$ y $p^2 \nmid a_0$, entonces f es irreducible en $K[X]$.

Ejercicio 22. *Teorema de Gauss.* Sea A un DFU y sea $\mathbb{K}$ su cuerpo de cocientes. Sea $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ 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 23. 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 $\mathbb{Q}[X]$ $\forall\, n \in \mathbb{N}$.

iv) Si $a \in \mathbb{Z}$ es tal que $p \mid a$ pero $p^2 \nmid a$, entonces $X^n - a$ es irreducible en $\mathbb{Q}[X]$.

Ejercicio 24. 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.

Ejercicio 25. Probar que si $f \in \mathbb{Q}[X]$ es irreducible, entonces f no tiene raíces múltiples en $\mathbb{C}$.

Ejercicio 26. Determinar todos los polinomios de grado 2, 3, 4 y 5 irreducibles en $\mathbb{Z}_2[X]$.

Ejercicio 27. 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) Determinar condiciones necesarias y suficientes para que $X^3 + aX^2 + bX - 1$ sea reducible en $\mathbb{Z}[X]$. Lo mismo para $X^3 + b$.

Ejercicio 28. 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 $c \in \mathbb{K}$.

Ejercicio 29. Analizar la reducibilidad de:

i) $2X^5 + 18X^3 + 30X^2 - 24$; $X^4 + 4X^2 + 10$; $X^3 - X^2 + 7X + 2$ en $\mathbb{Q}[X]$ y en $\mathbb{Z}[X]$

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

iii) $(X + a)^4 + 1$ en $\mathbb{Q}[X]$ $(a \in \mathbb{Q})$

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

Ejercicio 30. Sea $\mathbb{K}$ un cuerpo finito de q elementos. Probar que en $\mathbb{K}[X]$ hay $\dfrac{q^2 - q}{2}$ polinomios mónicos irreducibles de grado 2.