Estructuras Algebraicas II

Práctica 1 – Segundo Cuatrimestre de 2017

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 un epimorfismo 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.

Ejercicio 3. 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 4. 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 5. 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* 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.

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

Ejercicio 6. Sea A un dominio íntegro y sea $a \in A$. Probar que:

1. Si a es primo, entonces a es irreducible.
2. Si A es DFU (dominio de factorización única), a irreducible implica a primo.
3. Verificar que en general no vale que irreducible implica primo.
   Sugerencia: $\mathbb{Z}[\sqrt{-5}]$
4. Si A es principal entonces A es DFU, pero no vale la recíproca.

Ejercicio 7. 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 8. Sea $p \in \mathbb{Z}$ primo. Probar que:

i) -1 es un cuadrado en $\mathbb{Z}/p$ 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 9.

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 10. 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) ¿Será verdad que si un polinomio mónico f con coeficientes enteros es irreducible en $\mathbb{Z}$ podemos encontrar un primo p tal f sea irreducible en $\mathbb{F}_p[X]$?

Ejercicio 11. *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: $p \nmid a_n$, $p \mid a_i\ \forall\, 0 \leq i \leq n-1$ y $p^2 \nmid a_0$, entonces f es irreducible en $\mathbb{K}[X]$.

Ejercicio 12. *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 13. 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 14. [Lema de Gauss] Si $f \in \mathbb{Z}[x]$ es primitivo, entonces f es irreducible si y sólo si lo es en $\mathbb{Q}[x]$.

Ejercicio 15. Sea A un DFU y sea $\mathbb{K}$ su cuerpo de fracciones. 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.

Ejercicio 16. Si $K \subset L$ son cuerpos, y $p(x), q(x) \in K[x]$ polinomios. Probar que $p(x) \mid q(x)$ si y sólo si lo divide como polinomios en $L[x]$.