

## PRÁCTICA 7

**Algunas definiciones.**

Para  $A$  anillo arbitrario. Sea  $M$  un  $A$ -módulo y sea  $\mathcal{S}$  un sistema de generadores de  $M$ . Decimos que  $\mathcal{S}$  es un *sistema de generadores minimal* de  $M$  si ningún subconjunto propio de  $\mathcal{S}$  es un sistema de generadores de  $M$ .

Para  $A$  un dominio íntegro.

Un polinomio  $p \in A[X]$  se dice *primitivo* si los únicos elementos que dividen a todos sus coeficientes son las unidades.

Un elemento  $a \in A$  se dice *reducible* si existen  $b, c \in A$  no unidades tales que  $a = bc$ ;  $a$  se dice *irreducible* si no es reducible ni es una unidad. Dos elementos irreducibles  $a, b$  se dicen *asociados* si  $a = ub$  para alguna unidad  $u$ . Un elemento  $a \in A$  se dice *primo* si  $a \neq 0$ ,  $a$  no es una unidad y para todos los elementos  $b, c \in A$  tales que  $a|bc$ , es cierto que  $a|b$  ó  $a|c$ .

Un dominio íntegro  $A$  se dice un *dominio de factorización unica* (DFU) si verifica lo siguiente.

- Todo  $x \in A \setminus \{0\}$  puede escribirse como  $x = up_1 \dots p_n$ , con  $u$  una unidad y  $p_i$  elementos irreducibles (eventualmente ninguno).
- Si  $x = wq_1 \dots q_m$  es otra descomposición con  $w$  una unidad y  $q_i$  irreducibles, entonces  $n = m$  y existe una biyección  $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  tal que  $p_i$  es asociado a  $q_{\sigma(i)}$ .

**Ejercicios**

1. Probar que los  $\mathbb{Z}$ -módulos  $\mathbb{Q}^*$ ,  $\mathbb{R}^*$  y  $\mathbb{C}^*$  no son finitamente generados.
2. Sea  $M$  un módulo no nulo finitamente generado. Probar que si  $\mathcal{S}$  es un sistema de generadores de  $M$  entonces existen  $x_1, \dots, x_n \in \mathcal{S}$  tales que  $M = \langle x_1, \dots, x_n \rangle$ .
3. Probar que todo módulo de tipo finito posee un sistema de generadores minimal.
4. Para todo  $n \in \mathbb{N}$ ,  $\mathbb{Z}$  (considerado como  $\mathbb{Z}$ -módulo) admite un sistema de generadores minimal con  $n$  elementos.
5. Sean  $K$  un cuerpo y  $A = \bigcup_{n=1}^{\infty} K[x_1, \dots, x_n]$ . Probar que el ideal  $I := \langle x_i : i \in \mathbb{N} \rangle$  no es finitamente generado como  $A$ -módulo.
6. Sea  $K$  un cuerpo,  $A = K[X]/\langle X^n \rangle$ , con  $n > 1$ . Probar que  $A$  no es un  $A$ -módulo simple, pero es *indescomponible*, es decir, no existen submódulos propios  $N_1$  y  $N_2$  tales que  $A = N_1 \oplus N_2$ .
7. Decidir cuáles de las siguientes afirmaciones son verdaderas.
  - a) De todo sistema de generadores de un módulo  $M$  puede extraerse una base.

- b) Todo conjunto linealmente independiente de un módulo  $M$  puede extenderse a una base.
- c) Todo submódulo de un módulo libre es libre.
- d) Si  $x \in M$  es no nulo entonces  $\{x\}$  es linealmente independiente.
- e) Existen módulos libres con elementos no nulos  $x$  tales que  $\{x\}$  es linealmente dependiente.
- f) Existen módulos no libres tales que para todo elemento no nulo  $x$ , el conjunto  $\{x\}$  es linealmente independiente.
- g) Si  $A$  es un anillo íntegro y  $M$  es un  $A$ -módulo libre entonces todo elemento no nulo de  $M$  es linealmente independiente.
- h) Si  $M$  es un  $A$ -módulo libre y  $N$  es un submódulo de  $M$  que es libre como  $A$ -módulo, entonces  $N$  es un sumando directo de  $M$ .
8. Sea  $K$  un cuerpo. Probar que el anillo de polinomios de Laurent  $K[X, X^{-1}]$  es un dominio euclídeo.
9. Sean  $A$  dominio íntegro y  $a \in A$ . Probar lo siguiente.
- (a) Si  $a \in A$  es primo, entonces  $a$  es irreducible.
- (b)  $a \in A \setminus \{0\}$  no unidad. Entonces  $a$  es primo si y sólo si  $\langle a \rangle$  es primo.
- (d) Si  $A$  es DFU y  $a \in A$  es irreducible, entonces  $a$  es primo.
10. **Cuerpo de fracciones.** Sea  $A$  un dominio íntegro. En  $A \times (A \setminus \{0\})$  consideramos la siguiente relación:  $(a, b) \sim (c, d)$  sii  $ad = bc$ .
- (a) Probar que  $\sim$  es una relación de equivalencia.
- (b) Sea  $K := (A \times (A \setminus \{0\})) / \sim$  el conjunto de clases de equivalencia. Notamos con  $\frac{a}{b}$  a la clase de un elemento  $(a, b)$ . Probar que las operaciones,
- $$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$
- están bien definidas.
- (c) Probar que  $K$  es un cuerpo y que  $i : A \rightarrow K$ , dado por  $i(a) := \frac{a}{1}$ , es un monomorfismo de anillos.
- (d) Probar que dado un cuerpo  $K'$  y un monomorfismo de anillos  $j : A \rightarrow K'$ , existe un único morfismo de anillos  $\bar{j} : K \rightarrow K'$  tal que  $\bar{j} \circ i = j$ .
11. Sea  $A$  un dominio íntegro,  $I$  ideal propio de  $A$ ;  $\pi : A \rightarrow A/I$  la proyección canónica. Sean  $f = \sum_{i=0}^n a_i X^i \in A[X]$  mónico y  $\bar{f} = \sum_{i=0}^n \pi(a_i) X^i \in (A/I)[X]$ . Probar que si  $f$  es reducible en  $A[X]$ , entonces  $\bar{f}$  es reducible en  $(A/I)[X]$ .
12. **Criterio de irreducibilidad de Eisenstein.** Sean  $A$  un DFU y  $K$  su cuerpo de fracciones. Sea  $f = \sum_{i=0}^n a_i X^i \in A[X]$ . Supongamos que existe un primo  $p \in A$  tal que:

- $p$  no divide a  $a_n$ ,
- $p$  divide a  $a_i$ ,  $0 \leq i \leq n-1$ ,
- $p^2$  no divide a  $a_0$ .

Probar que  $f$  es irreducible en  $K[X]$

13. **Lema de Gauss.** Sean  $A$  un DFU y  $K$  su cuerpo de fracciones.

Sea  $f = \sum_{i=0}^n a_i X^i \in A[X]$  con  $a_0 \neq 0$ . Si  $p$  y  $q$  son elementos de  $A$  no nulos, coprimos entre sí tales que  $\frac{p}{q} \in K$  es raíz de  $f$ , demostrar que  $p/a_0$  y  $q/a_n$  en  $A$ .

14. Mostrar que  $X^2 + Y^2 - 1$  y  $XT - YZ$  son irreducibles en  $\mathbb{Q}[X, Y]$  y  $\mathbb{Q}[X, Y, Z, T]$  respectivamente.

15. Sea  $I = \langle Y + X^2 - 1, XY - 2Y^2 + 2Y \rangle \subset \mathbb{R}[X, Y]$ . Decidir si  $\mathbb{R}[X, Y]/I$  es un cuerpo.

16. Sea  $I \subseteq \mathbb{Z}[X]$  un ideal propio no nulo. Probar que  $I$  es primo si y sólo si es de alguna de las siguientes formas.

- $I = \langle p \rangle$ , con  $p \in \mathbb{Z}$  primo.
- $I = \langle p, f \rangle$ , con  $p \in \mathbb{Z}$  primo  $f \in \mathbb{Z}[X]$  tal que  $\bar{f} \in \mathbb{Z}_p[X]$  es irreducible en  $\mathbb{Z}_p[X]$ .
- $I = \langle f \rangle$ , con  $f \in \mathbb{Z}[X]$  primitivo e irreducible en  $\mathbb{Q}[X]$ .