Práctica 6

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 $a|c$.

Sistemas de generadores

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 $x_1, \ldots, x_n \in \mathcal{S}$ tales que $M =< x_1, \ldots, x_n >$.

3. Probar que todo módulo de tipo finito posee un sistema de generadores minimal.

4. Un A-módulo M se dice *localmente cíclico* si todo submódulo de M de tipo finito es cíclico. Probar lo siguiente.

   (a) Todo submódulo de un módulo localmente cíclico es localmente cíclico.

   (b) Si M es localmente cíclico y $f : M \longrightarrow N$ es un epimorfismo de módulos, entonces N es localmente cíclico.

   (c) $\mathbb{Q}$ y $\mathbb{Q}/\mathbb{Z}$ son $\mathbb{Z}$-módulos localmente cíclicos pero no son de tipo finito.

5. Sean K un cuerpo y $A = \bigcup_{n=1}^{\infty} K[x_1, \ldots, x_n]$. Probar que el ideal $I := \langle x_i : i \in \mathbb{N} \rangle$ no es finitamente generado como A-módulo.

Dominios

6. Sea K un cuerpo. Probar que el anillo de polinomios de Laurent $K[X, X^{-1}]$ es un dominio euclídeo.

7. 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 $< a >$ es primo.

   (d) Si A es DFU y $a \in A$ es irreducible, entonces a es primo.

8. Sea $d \in \mathbb{Z}$ libre de cuadrados y sea $\sqrt{d} \in \mathbb{C}$ una raíz cuadrada de d. Consideramos el subanillo de $\mathbb{C}$,

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\},$$

y definimos la aplicación φ de un elemento de $\mathbb{Z}[\sqrt{d}]$ por $\varphi(a + b\sqrt{d}) := a^2 - db^2$.

Probar lo siguiente.

(a) $\varphi(zw) = \varphi(z)\varphi(w)$, para todo $z, w \in \mathbb{Z}[\sqrt{d}]$.

(b) $z \in \mathbb{Z}[\sqrt{d}]$ es una unidad si y sólo si $\varphi(z) = \pm 1$.

(c) $z \in \mathbb{Z}[\sqrt{d}]$ es tal que $\varphi(z)$ es un número primo, entonces z es irreducible.

(d) El anillo $\mathbb{Z}[\sqrt{d}]$ es *prefactorial*. Es decir, probar que todo elemento no nulo de $\mathbb{Z}[\sqrt{d}]$ que no es una unidad puede escribirse como producto de elementos irreducibles.

9. Sea $A = \mathbb{Z}[\sqrt{-5}]$. Mostrar que los elementos $3, 7, 4 + \sqrt{-5}, 1 + 2\sqrt{-5}, 1 - 2\sqrt{-5}$ son irreducibles y no primos. ¿Es $\mathbb{Z}[\sqrt{-5}]$ un DFU?

10. Dar un ejemplo de tres dominios íntegros $A \subseteq B \subseteq C$ tales que A y C sean DFU, pero B no.

11. Sea A un dominio íntegro, I ideal propio de A; $\pi : A \longrightarrow A/I$ 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 $\mathbb{Q}[X]$.

Módulos libres

17. 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 $A = N_1 \oplus N_2$.

18. 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.

19. *a*) Sea $(M_i)_{i \in I}$ una familia infinita de módulos no nulos y S un sistema de generadores de $\bigoplus_{i \in I} M_i$. Probar que $\sharp S \geq \sharp I$.

    b) Existen módulos libres que admiten bases finitas de distinto cardinal.
    Ejemplo: Sea $B = \mathrm{End}_A(A^{(\mathbb{N})})$. Definimos $u, v \in B$ por:

$$u(e_{2i+1}) = 0 \quad u(e_{2i}) = e_i$$
$$v(e_{2i+1}) = e_i \quad u(e_{2i}) = 0$$

    Probar que $\{u, v\}$ es una base de B como B-módulo.