Universidad de la República
Facultad de Ciencias
Centro de Matemática

Álgebra I
Segundo semestre de 2021

Repartido 5: Divisibilidad en dominios

1. Este ejercicio ilustra que si D no es un dominio, no es necesariamente cierto que todo polinomio $f \in D[X]$ tenga a lo sumo tantas raíces como su grado.

   a) Probar que el polinomio $X^3 - X$ tiene 6 raíces en $\mathbb{Z}_6$.

   b) Probar que el polinomio $X^2 + 1$ tiene infinitas raíces en el anillo de los cuaterniones $\mathcal{H}$.

2. Probar que en $\mathbb{Z}_5[X]$ vale

   $$3X^3 + 4X^2 + 3 = (X+2)^2(3X+2) = (X+2)(X+4)(3X+1).$$

   Explicar por qué esta última igualdad no contradice el hecho de que $\mathbb{Z}_5[X]$ sea un dominio factorial.

3. Probar que el polinomio $X^4 + X^3 + X + 1$ no es irreducible sobre $\mathbb{k}[X]$, para ningún cuerpo $\mathbb{k}$.

4. Sea $D = \{a + b\sqrt{10} : a, b \in \mathbb{Z}\} \subset \mathbb{R}$. Definimos $* : D \to D$ mediante $\left(a + b\sqrt{10}\right)^* = a - b\sqrt{10}$ y $N : D \to \mathbb{Z}$ mediante $N(u) = u\,u^*$. Probar:

   a) Vale $(uv)^* = u^*v^*$ para todo $u, v \in D$. Vale $u^* = u$ si y solo si $u \in \mathbb{Z}$.

   b) Vale $N(uv) = N(u)N(v)$ para todo $u, v \in D$. Vale $N(u) = 0$ si y solo si $u = 0$.

   c) Un elemento $u \in D$ es invertible si y solo si $N(u) = \pm 1$.

   d) Los elementos 2, 3, $4 + \sqrt{10}$ y $4 - \sqrt{10}$ son irreducibles en D.
   Sugerencia: observar que las ecuaciones $x^2 = 2$ y $x^2 = 3$ no tienen solución en $\mathbb{Z}_5$.

   e) Los elementos 2, 3, $4 + \sqrt{10}$ y $4 - \sqrt{10}$ no son primos en D.
   Sugerencia: calcular $\left(4 + \sqrt{10}\right)\left(4 - \sqrt{10}\right)$.

5. Dos ideales I y J de un anillo A se dicen *primos entre sí* si $I + J = A$. Probar que en un dominio de ideales principales, dos ideales (a) y (b) son primos entre sí si y solo si a y b son primos entre sí.

6. Sea D un dominio de ideales principales.

   a) Sea P un ideal propio de D. Probar que existen ideales maximales $P_1, \ldots, P_r$ de D tales que $P = P_1 \cdots P_r$ y que esta descomposición es única a menos del orden de los factores.

   b) Un ideal P de D se dice *primario* si $P \neq D$ y verifica $ab \in P$ y $a \notin P$, entonces $\exists n \in \mathbb{Z}^+$ tal que $b^n \in P$. Probar que un ideal P es primario si y solo si $P = \{0\}$ o existen $n \in \mathbb{Z}^+$ y $p \in D$ irreducible tales que $P = \langle p^n \rangle$.

   c) Si $P_1, \ldots, P_n$ son ideales primarios con $P_i = \langle p_i^{m_i} \rangle$, $\forall i = 1, \ldots, n$, siendo $p_1, \ldots, p_n$ elementos irreducibles no asociados, entonces $P_1 \cdots P_n = P_1 \cap \cdots \cap P_n$.

   d) Sea P un ideal propio de D. Probar que existen ideales primarios $P_1, \ldots, P_n$ de D tales que $P = P_1 \cap \cdots \cap P_n$ y que esta descomposición es única a menos del orden de los factores.

7. Un dominio D se dice *euclídeo* si existe una función $\delta : D\backslash\{0\} \to \mathbb{N}$ que verifica:

   - Para todo $a, b \in D\backslash\{0\}$ es $\delta(a) \leqslant \delta(ab)$.

- Si $a, b \in D$ con $b \neq 0$, entonces existen $q, r \in D$ tales que $a = bq + r$, con $r = 0$ o $r \neq 0$ y $\delta(r) < \delta(b)$.

a) Probar que $\mathbb{Z}$ es un dominio euclídeo definiendo $\delta(n) = |n|$. ¿Hay unicidad de q y r en $a = bq + r$?

b) Probar que $\Bbbk[X]$ es un dominio euclídeo ($\Bbbk$ cuerpo).

c) Probar que todo dominio euclídeo es un dominio de ideales principales[1].

d) Probar que si D es un dominio euclídeo, entonces:

- $\delta(a) \geqslant \delta(1),\ \forall a \in D\backslash\{0\}$,
- $a \in D\backslash\{0\}$ es invertible si y solo si $\delta(a) = \delta(1)$, y
- $\delta(a) = \delta(au)$ para todo $a \in D\backslash\{0\}, u \in D^\times$

e) Sean $a, b \in D, b \neq 0$. Probar que q, r son únicos si y solo si $\delta(a + b) \leqslant \text{máx}\{\delta(a), \delta(b)\}$

8. *Algoritmo de Euclides*. Sean a_1, a_2 elementos no nulos de un dominio euclídeo D.
Se definen q_1 y a_3 mediante $a_1 = a_2q_1 + a_3$, con $a_3 = 0$ o $a_3 \neq 0$ y $\delta(a_3) < \delta(a_2)$. Si $a_3 \neq 0$, definimos q_2 y a_4 mediante $a_2 = a_3q_2 + a_4$, con $a_4 = 0$ o $a_4 \neq 0$ y $\delta(a_4) < \delta(a_3)$, y así seguimos. De esta manera se obtienen[2] por recurrencia una sucesión de pares $(q_i,\ a_{i+2})$, tales que $a_i = a_{i+1}q_i + a_{i+2}$ y $a_{i+2} = 0$ o $a_{i+2} \neq 0$ y $\delta(a_{i+2}) < \delta(a_{i+1})$, $\forall i = 1, 2, \ldots$.

a) Probar que existe n tal que $a_n \neq 0$ y $a_{n+1} = 0$, y que en este caso es $a_n = \text{mcd}(a_1, a_2)$.

b) Utilizar la construcción de la parte anterior para expresar $\text{mcd}(a_1, a_2)$ en la forma $xa_1 + ya_2$, con $x, y \in D$.

c) Utilizar el algoritmo de Euclides para encontrar el máximo común divisor de $X^3 + X^2 + X - 3$ y $X^4 - X^3 + 3X^2 + X - 4$ en $\mathbb{Q}[X]$.

9. *a*) Sean $m, n \in \mathbb{Z},\ n > 0$. Probar que existen $q, r \in \mathbb{Z}$ tales que $m = qn + r$ y $|r| \leqslant n/2$.

b) Sean $a, b, c \in \mathbb{Z},\ c > 0$. Probar que existen $r, q \in \mathbb{C}$ tales que $a + bi = qc + r$ y $|r|^2 < c^2$. Sugerencia: aplicar la parte anterior con a y b en lugar de m.

c) Probar que los *enteros de Gauss* $\mathbb{Z}[i] = \{a + bi :\ a, b \in \mathbb{Z}\}$ son un dominio euclídeo, definiendo $\delta(z) = z\overline{z} = |z|^2,\ \forall\ z \in \mathbb{Z}[i] \subset \mathbb{C}$.
Sugerencia: dados $y = a + bi$ y $x = c + di \in \mathbb{Z}[i]$, $x \neq 0$, hay que probar que existen $q, r \in \mathbb{Z}[i]$ tales que $y = qx + r$ con $r = 0$ o $\delta(r) < \delta(x)$. Si $x \in \mathbb{Z}^+$, es la parte anterior. En el caso general, probar que existen $q, r_0 \in \mathbb{Z}[i]$ tales que $y\overline{x} = qx\overline{x} + r_0$ y $r_0 = 0$ o $\delta(r_0) < \delta(x\overline{x})$; luego tomar $r = y - qx$.

d) Hallar los elementos invertibles de $\mathbb{Z}[i]$.

10. Probar que si $\Bbbk$ es un cuerpo y $f \in \Bbbk[X]$ tiene grado 2 o 3, entonces f es irreducible si y solo si f no tiene ninguna raíz en $\Bbbk$. Mostrar con un ejemplo que la afirmación es falsa si $f \in \mathbb{Z}[X]$.

11. Sean D un dominio factorial, K su cuerpo de fracciones y $f = a_nX^n + \cdots + a_1X + a_0 \in D[X]$. Sea $\frac{p}{q} \in K$ una raíz de f, con $p, q \in D$ coprimos.Probar que $q|a_n$ y $p|a_0$. Deducir que si $f \in D[X]$ es un polinomio mónico y $\alpha \in K$ es una raíz de p, entonces $\alpha \in D$.

---

[1] Se puede probar que $D = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}] = \{m + n(1 + i\sqrt{19})/2 :\ m, n \in \mathbb{Z}\} \subset C$ es un dominio de ideales principales que no es euclídeo.

[2] Los elementos $(q_i,\ a_{i+2})$ no tienen por qué ser únicos, en ese caso se hace una elección.

12. Sea $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ un polinomio primitivo. Probar que si existe un número primo p que no divide a a_n y que verifica que $\overline{a_n} X^n + \overline{a_{n-1}} X^{n-1} + \cdots + \overline{a_1} X + \overline{a_0}$ es irreducible en $\mathbb{Z}_p[X]$, entonces f es irreducible en $\mathbb{Z}[X]$. Mostrar con un ejemplo que la afirmación es falsa si $p|a_n$. Aplicar este criterio para probar que

$$3X^3 - 5X^2 + 4X + 21 \quad \text{y} \quad 4X^3 + 3X^2 + 2X + 4$$

son irreducibles en $\mathbb{Q}[X]$.

13. En cada caso determinar si el polinomio f es irreducible en $D[X]$, para $D = \mathbb{Z}$ y para $D = \mathbb{Q}$.

$$f = 2X^5 - 6X^3 + 9X^2 - 15, \quad f = 2X^3 + 3X^2 + 2X + 3, \quad f = X^4 + X + 4,$$
$$f = 3X^4 + 6X^2 + 6, \quad f = X^3 - 7X + 3, \quad f = X^4 - X^3 + 2X^2 - X + 1.$$

14. Sea p un número primo. Probar que el *polinomio ciclotómico* $f = X^{p-1} + X^{p-2} + \cdots + X + 1$ es irreducible en $\mathbb{Q}[X]$. *Sugerencia*: observar que $f = \frac{X^p - 1}{X - 1}$, luego $f(X + 1) = \frac{(X+1)^p - 1}{X}$ y aplicar el criterio de Eisenstein.

15. Sea $f = X^3 - X + 1 \in \mathbb{Z}[X]$.

    a) Probar que no existe ningún $a \in \mathbb{Z}$ tal que al polinomio $f(X + a)$ se le pueda aplicar el criterio de Eisenstein.

    b) Probar que f es irreducible en $\mathbb{Z}[X]$.

16. Investigar si los siguientes polinomios on irreducibles en $\mathbb{Z}[X, Y]$:

$$Y^4 + 2X^2Y^3 + X^3Y^2 - XY + X, \qquad Y^4 + XY^2 - 2X^2 + 3Y^2 + 2.$$

17. *a*) (*Criterio de Eisenstein generalizado.*) Sea D un dominio, $f = a_0 + a_1 X + \cdots + a_n X^n \in D[X]$. Si existe un ideal primo $P \subset D$ tal que:

    - $a_i \in P$ para todo $i \neq n$,
    - $a_n \notin P$,
    - $a_0 \notin P^2$ (donde $P^2 = PP$),

    entonces f no puede ser escrito como producto de dos polinomios no constantes en $D[X]$. Si además f es *primitivo* (en el sentido que no tiene divisores constantes no invertibles) entonces es irreducible en $D[X]$.

    b) Sea D un dominio. Sean $A = D[y]$, $f = X^n - y \in A[X]$. Probar que f es irreducible en $A[X]$.