**Universidad de la República**
**Facultad de Ciencias**
**Centro de Matemática**

**Anillos y módulos**
**Primer semestre de 2025**

## Repartido 3: Dominios

1. Probar que el polinomio $X^3 - X$ tiene 6 raíces en $\mathbb{Z}_6$. Probar que el polinomio $X^2 + 1$ tiene infinitas raíces en el anillo de los cuaterniones $\mathcal{H}$.

2. Sea $A$ un anillo y $a \in A[[X]]$. Probar que $a$ es invertible en $A[[X]]$ si y solo si $a_0$ es invertible en $A$. Hallar explícitamente el inverso de $1 - X$ en $\mathbb{Z}[[X]]$.

3. Sea $\Bbbk$ un cuerpo. Probar que todo ideal no nulo de $\Bbbk[[X]]$ es de la forma $\langle X^n \rangle$, para algún $n \in \mathbb{N}$. Probar que $\Bbbk[[X]]$ tiene un solo ideal maximal[1].

4. Sea $\Bbbk$ un cuerpo y $A \subset \Bbbk$ un subanillo (luego $A$ es un dominio).

   *a*) Probar que $F = \left\{ab^{-1} : a, b \in A,\ b \neq 0\right\}$ coincide con la intersección de todos los subcuerpos de $\Bbbk$ que contienen a $A$.

   *b*) Probar que el cuerpo de fracciones de $A$ es isomorfo a $F$.

5. Sea $\mathbb{Z}\left(\sqrt{-5}\right) = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\}$. Probar que $A$ es un subanillo de $\mathbb{C}$ y que su cuerpo de fracciones es isomorfo a $\mathbb{Q}\left(\sqrt{-5}\right) = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Q}\right\}$.

6. Probar las Proposiciones 3.1.8 y 3.1.12 de las notas del curso.

7. 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 $\left(4 + \sqrt{10}\right)\left(4 - \sqrt{10}\right)$.

8. Sea $D = \mathbb{Z}\left[X^2, X^3\right]$ el subanillo de $\mathbb{Z}[X]$ generado por $X^2$ y $X^3$. Probar que $X^6$ admite más de una factorización en $D$. Deducir que $D$ es un dominio que no es factorial.

9. Probar lo que quedó pendiente en la demostración de la Proposición 3.1.22 de las notas del curso.

10. 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 $P = \langle p^n \rangle$.

[1] Un anillo conmutativo que tiene un solo ideal maximal se llama un *un anillo local*.

*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.

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

- Para todo $a, b \in D \setminus \{0\}$ es $\delta(a) \leq \delta(ab)$.
- Si $a, b \in D$ con $b \neq 0$, entonces existen $q, r \in D$ tales que $a = bq + r$, con $r = 0$ o $\delta(r) < \delta(b)$.

*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[2].

*d*) Probar que si $D$ es un dominio euclídeo, entonces $\delta(a) \geq \delta(1)$, $\forall a \in D \setminus \{0\}$ y $a \in D \setminus \{0\}$ es invertible si y solo si $\delta(a) = \delta(1)$.

12. *Algoritmo de Euclides.* Sean $a_1, a_2$ elementos no nulos de un dominio euclídeo $D$.
Se definen $q_1$ y $a_3$ mediante $a_1 = a_2 q_1 + a_3$, 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 $a_2 = a_3 q_2 + a_4$, con $a_4 = 0$ o $a_4 \neq 0$ y $\delta(a_4) < \delta(a_3)$, y así seguimos. De esta manera se obtienen[3] 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 $a_n = \mathrm{mcd}(a_1, a_2)$.

*b*) Utilizar la construcción de la parte anterior para expresar $\mathrm{mcd}(a_1, a_2)$ 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 $\mathbb{Q}[X]$.

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

*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 $\mathbb{Z}[i]$.

---

[2] Se puede probar que $D = \{m + n(1 + i\sqrt{19})/2 :\ m, n \in \mathbb{Z}\} \subset \mathbb{C}$ es un dominio de ideales principales que no es euclídeo.
[3] Los elementos $(q_i,\ a_{i+2})$ no tienen porqué ser únicos, en ese caso se hace una elección.