Tarea 2 Estructuras Algebraicas

Pedro Montero

Departamento de Matemática, Universidad Técnica Federico Santa María

En cada sección, debe **escoger solamente un ejercicio** (a, b, c o d) para resolver. A menos que se especifique lo contrario, denotaremos por A un anillo conmutativo con unidad no-nulo y por k un cuerpo.

1. **Anillos, dominios y cuerpo de fracciones (10 pts).**

   (a) Probar que si A es un dominio de integridad, entonces $A[X_1, \ldots, X_n]$ también.
   Indicación: Recuerde que $A[X][Y] \cong A[X, Y]$.

   (b) Supongamos que A es un dominio de integridad y sea $\mathrm{Fr}(A)$ su cuerpo de fracciones[1]. Probar que $\mathrm{Fr}(A)$ es un cuerpo y que la función $\iota_A : A \to \mathrm{Fr}(A),\ a \mapsto \frac{a}{1}$ es un morfismo de anillos inyectivo.

   (c) Sea A un dominio entero. Decimos que A es un **dominio euclideano**[2] si existe una función (*euclideana*) $\varphi : A \setminus \{0\} \to \mathbb{N}$ tal que para todos $a, b \in A$ con $b \neq 0$ existe una escritura (no necesariamente única)

   $$a = bq + r \text{ donde } r = 0, \text{ o bien } r \neq 0 \text{ y } \varphi(r) < \varphi(b).$$

   Probar que un dominio euclideano es un dominio de ideales principales.
   Indicación: Dado $I \subseteq A$ *ideal no-nulo, sea* $x \in I \setminus \{0\}$ *tal que* $\varphi(x)$ *sea minimal. Probar que* $I = \langle x \rangle$.

   (d) Probar que todo dominio de integridad *finito* A (i.e., tal que A es un conjunto finito) es un cuerpo.
   Indicación: Dado $a \neq 0$, *considerar la sucesión* $\{a, a^2, a^3, \ldots\} \subseteq A$.

2. **Ideales y anillos cocientes (10 pts).**

   (a) Probar que $k[X, Y]$ **no** es un dominio de ideales principales.

   (b) Sea k un cuerpo y recordemos que si 1_k es el neutro multiplicativo de k, entonces la **característica** de k, denotada $\mathrm{car}(k)$, es el mínimo entero positivo n tal que

   $$\underbrace{1_k + \cdots + 1_k}_{n \text{ sumandos}} = 0$$

   en caso de dicho n existir, y $\mathrm{car}(k) = 0$ en otro caso. Considerar el morfismo de anillos

   $$\varphi : \mathbb{Z} \longrightarrow k,\ n \mapsto \begin{cases} \underbrace{1_k + \cdots + 1_k}_{n \text{ sumandos}} & \text{si } n > 0. \\ 0 & \text{si } n = 0. \\ \underbrace{(-1_k) + \cdots + (-1_k)}_{(-n) \text{ sumandos}} & \text{si } n < 0. \end{cases}$$

   y deducir, analizando $\ker(\varphi)$, que $\mathrm{car}(k)$ es 0 o un número primo.

   (c) Sea k un cuerpo y $P \in k[X]$ un polinomio irreducible no-nulo de coeficiente principal 1. Probar que el cuerpo cociente $K := k[X]/\langle P \rangle$ es un k-espacio vectorial y que $\dim_k(K) = \deg(P)$.

   (d) Sea $A = \mathbb{R}[\cos(t), \sin(t)]$ el anillo cuyos elementos son funciones reales dadas por polinomios con coeficientes reales en las variables $\cos(t)$ y $\sin(t)$ (e.g. $f(t) = 2\cos(t)^2 - 1 \in A$). Probar que

   $$A \cong \mathbb{R}[X, Y]/\langle X^2 + Y^2 - 1 \rangle.$$

   Indicación: Considerar el morfismo de $\mathbb{R}$*-álgebras* $\varphi : \mathbb{R}[X, Y] \to A$ *dado por* $X \mapsto \cos(t),\ Y \mapsto \sin(t)$.

3. **Anillos reducidos y anillos noetherianos, Teorema de la base de Hilbert (10 pts).**

   (a) Sea $I \subseteq A$ un ideal de A. Probar que el **radical**

   $$\sqrt{I} := \left\{ a \in A \mid \exists\, n \in \mathbb{N}^{\geq 1} \text{ tal que } a^n \in I \right\}$$

   es un ideal de A, y que además $\sqrt{\sqrt{I}} = \sqrt{I}$.

   (b) Sea A un anillo noetheriano y sea $I \subseteq A$ un ideal. Probar que A/I es un anillo noetheriano.

---

[1] Definido como el cociente de $A \times (A \setminus \{0\})$ por la relación de equivalencia $(a, b) \sim (c, d) \overset{\text{def.}}{\iff} ad = bc$ en A.

[2] Por ejemplo, $\mathbb{Z}$ es euclideano para la función $\varphi(n) = |n|$ y $k[X]$ es euclideano para la función $\varphi(P) = \deg(P)$.

(c) Sea A un anillo noetheriano y sea $I \subseteq A$ un ideal. Probar que si $x \in \bigcap_{n=1}^{\infty} I^n$ entonces x pertenece al ideal $xI := \{ax,\ a \in I\}$.
Indicación: Por definición, si $I = \langle a_1, \ldots, a_r \rangle$, entonces I^n está generado por[3]

$$\{P(a_1, \ldots, a_r),\ P \in A[X_1, \ldots, X_r] \text{ polinomio homogéneo de grado } n\}.$$

Notar que si $x \in I^n$ entonces existe $P_n \in A[X_1, \ldots, X_r]$ homogéneo de grado n tal que $x = P_n(a_1, \ldots, a_r)$. Considerar $J_n := \langle P_1, \ldots, P_n \rangle$ y deducir que para cierto $N \in \mathbb{N}^{\geq 1}$ existen $Q_i \in A[X_1, \ldots, X_r]$ tales que $x = Q_1(a_1, \ldots, a_r)x + \ldots + Q_N(a_1, \ldots, a_r)x$.

(d) Sea A un anillo tal que todo ideal *primo* $\mathfrak{p} \subseteq A$ es finitamente generado. Probar que A es noetheriano.
Indicación: Asumir lo contrario. Utilizar el lema de Zorn para probar que existe un elemento maximal I en la familia de todos los ideales que no son finitamente generados. Probar por contradicción que I es un ideal primo considerando $x, y \in A \setminus I$ tales que $xy \in I$: sean $x_1, \ldots, x_r, y$ generadores del ideal $I + \langle y \rangle$, con $x_1, \ldots, x_r \in I$, y sean $a_1, \ldots, a_s$ generadores del ideal $J := \{a \in A \mid ay \in I\}$. Probar que los elementos $x_1, \ldots, x_r, a_1 y, \ldots, a_s y$ generan I.

4. **Hilbert Nullstellensatz y Topología de Zariski (10 pts).**

(a) Demostrar, utilizando el Hilbert Nullstellensatz, que si $I, J \subseteq \mathbb{C}[X_1, \ldots, X_n]$ son ideales. Entonces

$$\sqrt{IJ} = \sqrt{I} \cap \sqrt{J} \quad \text{y} \quad \sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}.$$

Para esto, puede considerar $X := V(I) = V(\sqrt{I}) \subseteq \mathbb{A}^n$ e $Y := V(J) = V(\sqrt{J}) \subseteq \mathbb{A}^n$.

(b) Dado $f \in \mathbb{C}[X_1, \ldots, X_n] \stackrel{\text{def}}{=} \mathscr{O}(\mathbb{A}^n)$, definimos el **abierto principal** asociado a f mediante

$$U_f := \{a \in \mathbb{A}^n \mid f(a) \neq 0\}.$$

Probar que $\mathscr{B} = \{U_f\}_{f \in \mathscr{O}(\mathbb{A}^n)}$ forma una base para la topología de Zariski de $\mathbb{A}^n$.

(c) Sea $I = \langle X^2, XY \rangle \subseteq \mathbb{C}[X, Y]$ y sea $X = V(I) \subseteq \mathbb{A}^2$. Determinar $\mathfrak{I}(X)$.

(d) Sea $I := \langle X^3 - X^2, X^2Y - X^2, XY - Y, Y^2 - Y \rangle \subseteq \mathbb{C}[X, Y]$. Probar que $I = \langle X^2, Y \rangle \cap \langle X - 1, Y - 1 \rangle$. ¿Es I un ideal radical? Describir $V(I) \subseteq \mathbb{A}^2$.

5. **Geometría de ideales y operaciones entre ideales (10 pts).**

(a) Consideremos la variedad algebraica afín

$$X = \{(x, y, z) \in \mathbb{A}^3 \mid y = x^2,\ z = x^3\}.$$

Determinar el ideal $\mathfrak{I}(X)$, ¿es X irreducible?.

(b) Sea $A = \mathbb{Z}$ y sea $I_n = n\mathbb{Z}$ para todo $n \in \mathbb{N}$. Probar que para todos $n, m \in \mathbb{N}^{\geq 1}$ se cumple que

$$I_n I_m = I_{mn}, \quad I_n \cap I_m = I_{\text{mcm}(n,m)}, \quad I_n + I_m = I_{\text{mcd}(n,m)}.$$

(c) Sea X un espacio topológico irreducible, Y un espacio topológico arbitrario no-vacío, y sea $f : X \to Y$ una función continua. Probar que $f(X)$ es un espacio topológico irreducible (con la topología inducida).

(d) Sean $I_1, \ldots, I_n$ ideales de A tales que $I_i + I_j = A$ para todo $i \neq j$, y sea $J = I_1 \cap \cdots \cap I_n$. Probar que el morfismo inyectivo

$$\varphi : A/J \hookrightarrow (A/I_1) \times \cdots \times (A/I_n),\ (a \mod J) \mapsto (a \mod I_1, \ldots, a \mod I_n)$$

es un isomorfismo.

6. **Módulos, submódulos y cocientes (10 pts).**

(a) Sea $\varphi : M \to M'$ un morfismo de A-módulos y sea N un A-módulo arbitrario. Definimos el **pullback** φ^* y el **pushforward** φ_* de φ mediante:

$$\begin{aligned} \varphi^* : \text{Hom}_A(M', N) &\longrightarrow \text{Hom}_A(M, N) \\ f &\longmapsto f \circ \varphi \end{aligned} \qquad \begin{aligned} \varphi_* : \text{Hom}_A(N, M) &\longrightarrow \text{Hom}_A(N, M') \\ g &\longmapsto \varphi \circ g \end{aligned}$$

Probar que φ^* y φ_* son morfismos de A-módulos.

[3] e.g. si $I = \langle a, b \rangle$ entonces $I^3 = \langle a^3, a^2b, ab^2, b^3 \rangle$

(b) Sea B una A-álgebra. Probar que si B es un A-módulo finitamente generado, entonces B es una A-álgebra finitamente generada.

(c) Sea $A = \mathbb{Z}$ y sea $I_n = n\mathbb{Z}$ para todo $n \in \mathbb{N}$. Sean $n, m \in \mathbb{N}^{\geq 1}$ con $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ y $m = p_1^{\beta_1} \cdots p_r^{\beta_r}$, donde $p_1, \ldots, p_r$ son números primos distintos y $\alpha_i, \beta_i \in \mathbb{N}$ para todo $i \in \{1, \ldots, r\}$. Probar que

$$(I_n : I_m) = \langle p_1^{\gamma_1} \cdots p_r^{\gamma_r} \rangle \subseteq \mathbb{Z},$$

donde $\gamma_i = \text{máx}\{\alpha_i - \beta_i, 0\}$ para todo $i \in \{1, \ldots, r\}$.

(d) Sean $n, m \in \mathbb{N}^{\geq 1}$. Probar que $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$, donde $d = \text{mcd}(n, m)$.
Indicación: Probar que para todo grupo abeliano G se tiene que $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, G) \cong G[n]$, *donde por definición* $G[n] := \{g \in G \mid ng = 0\}$ *es el subgrupo de elementos de* n-torsion. *Luego, construir un isomorfismo explícito* $(\mathbb{Z}/m\mathbb{Z})[n] \cong \mathbb{Z}/\text{mcd}(n, m)\mathbb{Z}$.

7. **Módulos finitamente generados, Teorema de Cayley–Hamilton y Lema de Nakayama (10 pts).**

(a) Sea $A = \mathbb{Z}$ y $M = \mathbb{Z}$ visto como A-módulo libre de rango 1. Probar que $\{1\}$ y $\{-1\}$ son las **únicas** bases de M como A-módulo.

(b) Sea M un A-modulo libre finitamente generado de rango $r \geq 1$, y sea $\mathfrak{m} \subseteq A$ un ideal maximal. Probar que

$$M/\mathfrak{m}M \cong (A/\mathfrak{m})^r$$

como $(A/\mathfrak{m})$-módulos.

(c) Sea A un anillo y sea I un ideal finitamente generado de A tal que $I^2 = I$. Probar que $I = \langle e \rangle$ es un ideal principal generado por cierto elemento $e \in A$ que cumple $e^2 = e$.

(d) Sea $A = \mathscr{C}^0([0,1], \mathbb{R})$ el anillo conmutativo de funciones continuas $f : [0,1] \to \mathbb{R}$. Dado un elemento $x \in [0,1]$, definimos el ideal maximal de A asociado a x mediante

$$\mathfrak{m}_x := \{f \in A \mid f(x) = 0\}.$$

Probar que **todo** ideal maximal de A es de la forma $\mathfrak{m}_x$ para algún $x \in [0,1]$.
Indicación: Sea $\mathfrak{m} \subseteq \mathscr{C}$ *ideal maximal. Suponer por contradicción que para todo* $p \in [0,1]$ *existe* $f_p \in \mathfrak{m}$ *tal que* $f_p(p) \neq 0$, *y sea* $U_p \subseteq [0,1]$ *una vecindad abierta de* p *tal que* $f_p(x) \neq 0$ *para todo* $x \in U_p$. *Construir, usando la compacidad*[4] *de* $[0,1]$, *una función* $g \in \mathfrak{m}$ *de la forma* $g = f_{p_1}^2 + \cdots + f_{p_N}^2$, *y deducir que* $\mathfrak{m} = \mathscr{C}$.

Finalmente, debe **escoger sólamente un problema** (A, B o C) para resolver.

Problema A (30 pts).

El objetivo de este problema es estudiar más en detalle propiedades del anillo $\mathscr{O} := \mathbb{C}[X,Y]/\langle X^2 + Y^2 - 1 \rangle$. Para esto, podrá utilizar (sin demostración) los hechos siguientes:

(a) El ideal $\langle X^2 + Y^2 - 1 \rangle \subseteq \mathbb{C}[X,Y]$ es primo. En particular, el polinomio $P = X^2 + Y^2 - 1$ es irreducible.

(b) El ideal $\langle UV - 1 \rangle \subseteq \mathbb{C}[U,V]$ es primo. En particular, el polinomio $Q = UV - 1$ es irreducible.

(c) El **lema de Bézout** es válido para cualquier dominio de ideales principales. Más precisamente, si A es un dominio de ideales principales y $a, b \in A$ entonces un *máximo común divisor* de a y b es un generador $d \in A$ (no necesariamente único) del ideal $\langle a \rangle + \langle b \rangle = \langle a, b \rangle \subseteq A$. Así, existen $x, y \in A$ tales que

$$ax + by = d.$$

En particular, decimos que a y b son *relativamente primos* si $d = 1$ es un máximo común divisor de a y b (i.e. $\langle a \rangle + \langle b \rangle = A$). Más aún, si $f = \frac{p}{q} \in \text{Fr}(A)$ con $p, q \in A \setminus \{0\}$ entonces siempre podemos suponer que p y q son relativamente primos en A.

Utilizando lo anterior, responda justificadamente las siguientes preguntas:

1. Sean A y B dominios de integridad tales que $B \subseteq A \subseteq \text{Fr}(B)$. Probar que si B es un dominio de ideales principales, entonces A también.
Indicación: Sea $I \subseteq A$ *un ideal. Considerar* $I \cap B = \langle a \rangle$ *ideal principal. Probar que* $I = \langle a \rangle$.

[4] Recordar que el hecho que $[0,1]$ es compacto implica que para todo cubrimiento abierto $[0,1] = \bigcup_{\lambda \in \Lambda} U_\lambda$, existe un sub-cubrimiento finito $[0,1] = U_{\lambda_1} \cup \cdots \cup U_{\lambda_N}$, con $\lambda_1, \ldots, \lambda_N \in \Lambda$.

2. Probar que $\mathscr{O} \cong \mathbb{C}[U,V]/\langle UV-1\rangle$ como $\mathbb{C}$-álgebras.
Indicación: El polinomio X^2+Y^2 puede ser factorizado sobre $\mathbb{C}$.

3. Sea $\mathbb{C}[U,U^{-1}]$ la sub-álgebra del cuerpo de funciones racionales $\mathbb{C}(U)$ generada por U y $U^{-1}=\frac{1}{U}$. Probar que $\mathscr{O} \cong \mathbb{C}[U,U^{-1}]$ como $\mathbb{C}$-álgebra y deducir, usando (1), que $\mathscr{O}$ es un dominio de ideales principales.
Indicación: Considerar el morfismo de $\mathbb{C}$-álgebras $\varphi : \mathbb{C}[U,V] \to \mathbb{C}[U,U^{-1}]$ que envía $\varphi(U)=U$ y $\varphi(V)=U^{-1}$. Para determinar los posibles $P \in \ker(\varphi)$, utilizar division de polinomios en $K[V]$ donde $K=\mathbb{C}(U)$.

Problema B (30 pts).

El objetivo de este problema es estudiar ciertas curvas algebraicas afines de la forma $y^s = x^r$ en el plano $\mathbb{A}^2$. Para esto, comenzemos por considerar

$$C := \{(x,y) \in \mathbb{A}^2 \mid x^2 = y^3\}$$

curva plana.

1. Probar que $\mathfrak{I}(C) = \langle X^2 - Y^3\rangle \subseteq \mathbb{C}[X,Y]$ y deducir que C es irreducible.
Indicación: Considerar la parametrización $\varphi : \mathbb{A}^1 \to C$, $t \mapsto (t^3,t^2)$ para probar que $\mathscr{O}(C)$ puede verse como el subanillo $\mathbb{C}[T^2,T^3]$ de $\mathbb{C}[T] = \mathscr{O}(\mathbb{A}^1)$.

2. Probar que $\mathscr{O}(C)$ **no** es un dominio de ideales principales, y deducir que C **no** es isomorfa a $\mathbb{A}^1$.
Indicación: Considerar el ideal $I = \langle T^2, T^3\rangle \subseteq \mathbb{C}[T^2,T^3]$.

3. Sean $r,s \in \mathbb{N}^{\geq 1}$ relativamente primos, y sea

$$C_{r,s} := \{(x,y) \in \mathbb{A}^2 \mid x^r = y^s\}.$$

Probar que $\mathfrak{I}(C_{r,s}) = \langle X^r - Y^s\rangle \subseteq \mathbb{C}[X,Y]$ y que $\mathscr{O}(C_{r,s}) \cong \mathbb{C}[T^s,T^r]$.
Indicación: Dado $P \in \mathfrak{I}(C_{r,s}) \subseteq \mathbb{C}[X,Y]$, escribir

$$P(X,Y) = P_0(Y) + XP_1(Y) + \cdots + X^{r-1}P_{r-1}(Y) \mod I,$$

donde $I := \langle X^r - Y^s\rangle$. Notar que $P(T^s,T^r) = 0$ y que las potencias de T que aparecen en el término $T^{si}P_i(T^r)$ son congruentes a si módulo r. Deducir que $P_i = 0$ para todo $i \in \{0,\ldots,r-1\}$ y por ende $P \in I$.

Problema C (30 pts).

El objetivo de este problema es estudiar el **largo** de un módulo y algunas de sus propiedades. Sea M un A-módulo. Una **serie de composición** de M es una cadena finita

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

de submódulos que *no pueden ser refinados*[5] (i.e., tales que no existe un submódulo N de M tal que $M_{i-1} \subsetneq N \subsetneq M_i$ para todo $i \in \{1,\ldots,n\}$), y en este caso decimos que n es el **largo** de la serie de composición.

Si M posee al menos una serie de composición, decimos que M es un A-módulo **de largo finito** y definimos el **largo de** M como el mínimo largo posible entre todas las series de composición de M, y lo denotaremos $\ell(M) \in \mathbb{N}$. En caso de que M no posea una serie de composición, escribiomos $\ell(M) := +\infty$.

1. Sea M un A-módulo de largo finito. Probar que si $N \subsetneq M$ es un submódulo propio entonces $\ell(N) < \ell(M)$, y deducir que **toda** serie de composición de M tiene largo $\ell(M)$.
Indicación: Para la primera parte, considerar $N_i := N \cap M_i$. Para la segunda parte, usar inducción en $\ell(M)$.

2. Sea M un A-módulo de largo finito. Usando (1), probar que toda cadena

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

de submódulos de M puede ser refinada en una serie de composición de M. Deducir que si $N \subseteq M$ es un submódulo, entonces

$$\ell(N) + \ell(M/N) = \ell(M).$$

3. Probar que si $A = k$ es un cuerpo y $M = V$ es un k-espacio vectorial, entonces $\ell(M) = \dim_k(V)$. Por otro lado, probar que si $A = \mathbb{Z}$ y $M = \mathbb{Z}$, entonces $\ell(M) = +\infty$.

[5] Equivalentemente, el A-módulo cociente M_i/M_{i-1} no posee submodulos no-triviales (i.e., diferentes de 0 y M_i/M_{i-1}).

Bonus (21 puntos): El objetivo de este problema es estudiar el **resultante** y **discriminante** de polinomios en una variable con coeficientes en un cuerpo. Para simplificar la exposición, supondremos que $k = \mathbb{C}$ es el cuerpo de los números complejos.

En particular, si $f, g \in \mathbb{C}[X]$ son polinomios no-nulos de grados $\deg(f) = d \geq 1$ y $\deg(g) = e \geq 1$, entonces el Teorema Fundamental del Álgebra nos permite escribir

$$f(X) = a_0X^d + a_1X^{d-1} + \cdots + a_d = a_0 \prod_{j=1}^{d}(X - \lambda_j) \quad \text{y} \quad g(X) = b_0X^e + b_1X^{d-1} + \cdots + b_e = b_0 \prod_{j=1}^{e}(X - \mu_j),$$

donde $\lambda_1, \cdots, \lambda_d \in \mathbb{C}$ (resp. $\mu_1, \ldots, \mu_e \in \mathbb{C}$) son las raíces de f (resp. g), y donde $a_0b_0 \neq 0$. Definimos el **resultante** de f y g como

$$R(f,g) := a_0^e b_0^d \prod_{\substack{1\leq i\leq d\\ 1\leq j\leq e}} (\lambda_i - \mu_j) \overset{\text{def}}{=} a_0^e \prod_{i=1}^{d} g(\lambda_i) = (-1)^{de} b_0^d \prod_{j=1}^{e} f(\mu_j) \in \mathbb{C}.$$

En particular, $R(f,g) = 0$ si y sólo si los polinomios f y g tienen al menos una raíz común. Por conveniencia, definimos $R(f,g) := a_0^e$ (resp. $R(f,g) := b_0^d$) si $d = 0$ (resp. $e = 0$).

(i) Probar que $R(X + a_1, X + b_1) = b_1 - a_1$, que $R(g,f) = (-1)^{de}R(f,g)$ y que $R(fg,h) = R(f,h)R(g,h)$ para todos $f, g, h \in \mathbb{C}[X]$.

(ii) Probar que $f, g \in \mathbb{C}[X]$ poseen un factor común no-constante $h \in \mathbb{C}[X]$ si y sólo si existen polinomios $u, v \in \mathbb{C}[X]$ no-nulos, con $\deg(u) < \deg(f)$ y $\deg(v) < \deg(g)$, tales que

$$vf + ug = 0 \text{ en } \mathbb{C}[X].$$

Indicación: Si $vf = -ug$ y escribimos $f = p_1^{r_1} \cdots p_s^{r_s}$ como producto de polinomios irreducibles, probar que cada p_i debe dividir g.

(iii) Para cada $n \in \mathbb{N}^{\geq 1}$, denotemos por $M_n := \mathbb{C}[X]_{\deg<n}$ al $\mathbb{C}$-espacio vectorial de polinomios de grado $\leq n-1$. Considerar la aplicación $\mathbb{C}$-lineal dada por

$$\rho_{f,g} : M_e \oplus M_d \longrightarrow M_{d+e},\ (u,v) \longmapsto vf + ug,$$

y probar que f y g poseen un factor común no-constante si y sólo si $\det(\rho_{f,g}) = 0$. Verificar que $\det(\rho_{f,g})$ está dado por el determinante $(d+e) \times (d+e)$ siguiente[6]

$$\widetilde{R}(f,g) := \begin{vmatrix} a_0 & a_1 & \cdots & \cdots & a_d & & & \\ & a_0 & a_1 & \cdots & \cdots & a_d & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & a_0 & a_1 & \cdots & \cdots & a_d \\ b_0 & b_1 & \cdots & \cdots & b_e & & & \\ & b_0 & b_1 & \cdots & \cdots & b_e & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & b_0 & b_1 & \cdots & \cdots & b_e \end{vmatrix}.$$

Indicación: Considerar la base $\{1, X, X^2, \ldots, X^{n-1}\}$ de M_n.

(iv) Verificar que $R(f,g) = \widetilde{R}(f,g)$ cuando $d = 2$ y $e = 1$.

Hecho (sin demostración[7]): $R(f,g) = \widetilde{R}(f,g)$ para todos $f, g \in \mathbb{C}[X]$.

Dado un polinomio $f \in \mathbb{C}[X]$ de grado $d \geq 1$, donde

$$f(X) = a_0X^d + a_1X^{d-1} + \cdots + a_d = a_0 \prod_{j=1}^{d}(X - \lambda_j),$$

definimos $R(f) := R(f, f')$ de f como el resultante de f y su derivada

$$f'(X) \overset{\text{def}}{=} da_0X^{d-1} + a_1(d-1)X^{d-2} + \ldots + 2a_{d-2}X + a_{d-1},$$

En particular, $R(f) = 0$ si y sólo si f posee al menos una raíz repetida (i.e., de multiplicidad ≥ 2).

[6] Los coeficientes en los espacios vacíos son 0. Además, no necesariamente se tiene que $d = e$ (como se ilustra visualmente), esto sólo se adoptó para simplificar la escritura.

[7] La demostración es rutinaria, pero involucra cálculos con polinomios en varias variables que omitiremos. En palabras simples, la idea es que tanto R como $\widetilde{R}$ son polinomios homogéneos del mismo grado en las variables $\lambda_1, \ldots, \lambda_d, \mu_1, \ldots, \mu_e$, por lo que basta verificar que $\widetilde{R}$ puede factorizarse tal como R.

(v) Probar que $R(f) = a_0^{2d-1} \prod_{1 \leq i \neq j \leq d} (\lambda_i - \lambda_j) = (-1)^{d(d-1)/2} a_0^{2d-1} \prod_{1 \leq i < j \leq d} (\lambda_i - \lambda_j)^2$.

Indicación: Notar que $R(f, f') = a_0^{d-1} \prod_{i=1}^{d} f'(\lambda_i)$. *Usando la regla para la derivada del producto, probar que* $f'(\lambda_i) = a_0(\lambda_i - \lambda_1) \cdots (\lambda_i - \lambda_{i-1})(\lambda_i - \lambda_{i+1}) \cdots (\lambda_i - \lambda_d)$.

Debido a que los términos no-nulos en la primera columna de $\widetilde{R}(f, f')$ son a_0 y da_0, tenemos que $R(f)$ es un múltiplo de a_0. Por lo anterior, y el signo que aparece en (v), es que se define el **discriminante** del polinomio f como

$$\Delta(f) := \frac{(-1)^{d(d-1)/2}}{a_0} R(f) \stackrel{\text{def}}{=} a_0^{2d-2} \prod_{1 \leq i < j \leq d} (\lambda_i - \lambda_j)^2 = (-1)^{d(d-1)/2} a_0^{2d-2} \prod_{1 \leq i \neq j \leq d} (\lambda_i - \lambda_j)$$

(vi) Utilizando el determinante $\widetilde{R}(f, f')$, calcular $\Delta(f)$ para $d = 2$ y $d = 3$.

(vii) Para $n \in \mathbb{N}^{\geq 1}$, identifiquemos el espacio afín $\mathbb{A}^{n^2}$ con el $\mathbb{C}$-espacio vectorial $M_n(\mathbb{C})$ de matrices $n \times n$ con coeficientes complejos. Mediante la identificación anterior, probar que el conjunto de matrices invertibles con valores propios distintos forman un abierto de Zariski no-vacío[8] de $M_n(\mathbb{C})$.

[8] En particular, el conjunto $U \subseteq M_n(\mathbb{C})$ de matrices invertibles cuyos valores propios son todos distintos (y en particular, son diagonalizables) forman un abierto denso de $M_n(\mathbb{C})$.