Polinomios
(lista de problemas para examen)

En esta lista de problemas el conjunto de los polinomios de una variable con coeficientes complejos se denota por $\mathcal{P}(\mathbb{C})$. También se usa la notación $\mathbb{C}[x]$, si la variable se denota por x.

Notemos que un polinomio se determina por la lista de sus coeficientes, y la igualdad de dos polinomios se entiende como la igualdad de sus coeficientes correspondientes.

1. Propiedades de la adición y multiplicación de polinomios. Enunciar bien las siguientes propiedades de la adición y multiplicación en $\mathcal{P}(\mathbb{C})$:

1. Propiedad asociativa de la adición.
2. Propiedad conmutativa de la adición.
3. Propiedad neutra del polinomio cero bajo la adición.
4. Existencia de inversos aditivos.
5. Propiedad asociativa de la multiplicación.
6. Propiedad conmutativa de la multiplicación.
7. Propiedad distributiva de la multiplicación con respecto a la adición.
8. Propiedad neutra del polinomio uno.

Estas propiedades significan que el conjunto $\mathcal{P}(\mathbb{C})$ es un anillo asociativo conmutativo con identidad.

2. Grado de polinomios y sus propiedades. Aceptamos el convenio que $\deg(\mathbf{0}_{\mathcal{P}}) = -\infty$. Explicar las siguientes propiedades:

1. Para cualesquier $f, g \in \mathcal{P}(\mathbb{C})$, $\deg(fg) = \deg(f) + \deg(g)$.
2. Para cualesquier $f, g \in \mathcal{P}(\mathbb{C})$, $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.

3. Polinomios de grado cero. ¿Qué polinomios tienen grado cero?

4. Definición de invertibilidad en el anillo de polinomios $\mathcal{P}(\mathbb{C})$. Sea $f \in \mathcal{P}(\mathbb{C})$. ¿Cuándo se dice que f es invertible en $\mathcal{P}(\mathbb{C})$? Escriba bien la definición.

5. Criterio de invertibilidad en el anillo de polinomios $\mathcal{P}(\mathbb{C})$. Sea $f \in \mathcal{P}(\mathbb{C})$. Demuestre que f es invertible en $\mathcal{P}(\mathbb{C})$ si, y sólo si, $\deg(f) = 0$.

6. ¿Cuándo el producto de dos polinomios es cero?. Sean $f, g \in \mathcal{P}(\mathbb{C})$ tales que $fg = \mathbf{0}_{\mathcal{P}}$. Demuestre que $f = \mathbf{0}_{\mathcal{P}}$ o $g = \mathbf{0}_{\mathcal{P}}$.

7. La ley de cancelación en el anillo de polinomios $\boldsymbol{\mathcal{P}}(\mathbb{C})$. Sean $f, g, h \in \mathcal{P}(\mathbb{C})$ tales que $fg = fh$ y $f \neq \mathbf{0}_{\mathcal{P}}$. Demuestre que $g = h$.

8. Definición de la divisibilidad de polinomios. Sean $f, g \in \mathcal{P}(\mathbb{C})$. Se dice que g *divide* a f y se escribe $g \mid f$ si existe un polinomio $q \in \mathcal{P}(\mathbb{C})$ tal que $f = gq$.

9. Ejemplos de divisibilidad. Muestre que:

- $(x - 1) \mid (x^4 - 1)$.
- $(x - 1) \mid (x^5 - 1)$.
- $(x - 1) \mid (x^n - 1)$.
- $(x - a) \mid (x^n - a^n)$, donde a es un número.

10. Divisibilidad y polinomios de grado cero. Sean $f, g \in \mathcal{P}(\mathbb{C})$ y sea $c \in \mathbb{C} \setminus \{0\}$. Muestre que las siguientes condiciones son equivalentes:

(a) $f \mid g$.

(b) $f \mid (c_{\mathcal{P}} g)$.

(c) $(c_{\mathcal{P}} f) \mid g$.

11. Divisibilidad de polinomios que tienen el mismo grado. Sean $f, g \in \mathcal{P}(\mathbb{C}) \setminus \{\mathbf{0}_{\mathcal{P}}\}$ tales que $\deg(f) = \deg(g)$ y $f \mid g$. Muestre que existe un $c \in \mathbb{C} \setminus \{0\}$ tal que $g = cf$.

12. Criterio de divisibilidad mutua de dos polinomios. Sean $f, g \in \mathcal{P}(\mathbb{C})$. Demuestre que las siguientes dos condiciones son equivalentes:

(a) $f \mid g$ y $g \mid f$.

(b) existe un $c \in \mathbb{C} \setminus \{0\}$ tal que $f = c_{\mathcal{P}} g$.

13. Definición del divisores comunes de dos polinomios. Sean $f, g \in \mathcal{P}(\mathbb{C})$. Un polinomio $h \in \mathcal{P}(\mathbb{C})$ llama *divisor común* de f y g si $h \mid f$ y $h \mid g$. Denotamos el conjunto de los divisores comunes de f y g por $\mathcal{D}(f, g)$:

$$\mathcal{D}(f, g) \coloneqq \{h \in \mathcal{P}(\mathbb{C}) : \quad h \mid f \quad \wedge \quad h \mid g\}.$$

14. Definición de máximos comunes divisores de dos polinomios. Sean $f, g \in \mathcal{P}(\mathbb{C})$ no ambos cero. Un polinomio $d \in \mathcal{P}(\mathbb{C})$ se llama un *máximo común divisor* de f y g si d es un divisor común de f y g, y cualquier divisor común de f y g divide a d. Denotamos el conjunto de los máximos comunes divisores de f y g por $\operatorname{MCD}(f, g)$:

$$\operatorname{MCD}(f, g)$$

15. Teorema de división de polinomios. Sean $f, g \in \mathcal{P}(\mathbb{C})$, $g \neq \mathbf{0}_{\mathcal{P}}$. Demostrar que existe un único par de polinomios (q, r) tal que $q, r \in \mathcal{P}(\mathbb{C})$, $f = gq + r$ y $\deg(r) < \deg(g)$.

16. Algoritmo de Euclides para polinomios. Explique el algoritmo de Euclides para polinomios. Tarea adicional: realice el algoritmo de Euclides para polinomios en algún lenguaje de programación.

17. Algoritmo de Euclides extendido. Escriba las fórmulas del algoritmo de Euclides extendido. Dado un par de polinomios $f, g \in \mathcal{P}(\mathbb{C})$ no ambos cero, este algoritmo regresa tres polinomios $u, v, d \in \mathcal{P}(\mathbb{C})$ tales que $fu + gv = d$ y $d = \operatorname{mcd}(f, g)$.

18. Lema sobre los máximos comunes divisores de dos polinomios, uno de los cuales es cero. Sea $f \in \mathcal{P}(\mathbb{C})$. Demuestre que

$$\operatorname{MCD}(f, \mathbf{0}_{\mathcal{P}}) = \{h \in \mathcal{P}(\mathbb{C}) \colon \quad \exists c \in \mathbb{C} \setminus \{0\} \quad h = cf\}.$$

19. Lema: conservaciones de máximos comunes divisores en el algoritmo de Euclides. Sean $f, g, q, r \in \mathcal{P}(\mathbb{C})$, $g \neq \mathbf{0}_{\mathcal{P}}$,

$$f = gq + r.$$

Demuestre que $\operatorname{MCD}(f, g) = \operatorname{MCD}(g, r)$.

20. Teorema (existencia de un máximo común divisor de dos polinomios). Sean $f, g \in \mathcal{P}(\mathbb{C})$ no ambos cero. Usando el algoritmo de Euclides y dos lemas anteriores demuestre que el conjunto de los máximos comunes divisores de f y g no es vacío.

21. Proposición (unicidad de máximos comunes divisores salvo múltiplos constantes no nulos). Sean $f, g \in \mathcal{P}(\mathbb{C})$ no ambos cero, y sean $d_1, d_2 \in \operatorname{MCD}(f, g)$. Demuestre que existe $c \in \mathbb{C} \setminus \{0\}$ tal que $d_2 = cd_1$.

22. Proposición (existencia y unicidad del máximo común divisor mónico de dos polinomios, no ambos cero). Sean $f, g \in \mathcal{P}(\mathbb{C})$ no ambos cero. Demuestre que en el conjunto $\operatorname{MCD}(f, g)$ existe un único polinomio mónico.

23. Definición (el máximo común divisor mónico de dos polinomios, no ambos cero). Sean $f, g \in \mathcal{P}(\mathbb{C})$ no ambos cero. Sabemos que en el conjunto $\operatorname{MCD}(f, g)$ existe un único polinomio mónico. Este polinomio se denota por $\operatorname{mcd}(f, g)$.

Polinomios primos relativos

24. Definición (polinomios primos relativos). Dos polinomios $f, g \in \mathcal{P}(\mathbb{C})$, no ambos cero, se llaman *primos relativos* si

$$\operatorname{MCD}(f, g) = \{h \in \mathcal{P}(\mathbb{C}) \colon \ \deg(h) = 0\}.$$

25. Descripción de polinomios primos relativos. Sean $f, g \in \mathcal{P}(\mathbb{C})$ dos polinomios no ambos cero. Demuestre que las siguientes condiciones son equivalentes:

(a) $\operatorname{MCD}(f, g) = \{h \in \mathcal{P}(\mathbb{C})\colon \ \ \deg(h) = 0\}$.

(b) $\operatorname{mcd}(f, g) = 1$.

(c) $\mathcal{D}(f, g) = \{h \in \mathcal{P}(\mathbb{C})\colon \ \ \deg(h) = 0\}$.

26. Sean $f, g, u, v, \in \mathcal{P}(\mathbb{C})$ tales que

$$fu + gv = 1.$$

Demuestre que f y g son primos relativos.

27. Sean $f, g, u, v, d \in \mathcal{P}(\mathbb{C})$ tales que f y g no son ambos cero, $d = \operatorname{mcd}(f, g)$ y

$$fu + gv = d.$$

Demuestre que u y v son primos relativos.

28. Sean $f, g, h \in \mathcal{P}(\mathbb{C})$ tales que $f \mid h$, $g \mid h$, y $\operatorname{mcd}(f, g) = 1$. Demuestre que $(fg) \mid h$.

29. Sean $a, b \in \mathbb{C}$, $a \neq b$. Consideremos los polinomios

$$f(x) \coloneqq x - a, \qquad g(x) \coloneqq x - b.$$

Encuentre dos polinomios $u, v \in \mathcal{P}(\mathbb{C})$ tales que

$$fu + gv = 1.$$

30. Sean $a, b \in \mathbb{C}$, $a \neq b$. Consideremos los polinomios

$$f(x) \coloneqq x - a, \qquad g(x) \coloneqq x - b.$$

Dado $m \in \mathbb{N}$, encuentre dos polinomios $u, v \in \mathcal{P}(\mathbb{C})$ tales que

$$f^m u + gv = 1.$$

31. Sean $a, b \in \mathbb{C}$, $a \neq b$. Consideremos los polinomios

$$f(x) \coloneqq x - a, \qquad g(x) \coloneqq x - b.$$

Dados $m, n \in \mathbb{N}$, encuentre dos polinomios $u, v \in \mathcal{P}(\mathbb{C})$ tales que

$$f^m u + g^n v = 1.$$

Sugerencia: usar el resultado del problema anterior.

Polinomios irreducibles

Se denota por $\mathbb{F}$ un campo, por ejemplo, $\mathbb{F} = \mathbb{Q}$ o $\mathbb{F} = \mathbb{R}$ o $\mathbb{F} = \mathbb{C}$.

32. Un polinomio $f \in \mathcal{P}(\mathbb{F}) \setminus \{\mathbf{0}_\mathcal{P}\}$ se llama *irreducible* sobre $\mathbb{F}$ si para cualesquiera $g, h \in \mathcal{P}(\mathbb{F})$ la igualdad $gh = f$ implica que $\deg(g) = 0$ o $\deg(h) = 0$.

33. Demuestre que el polinomio $f(x) = x^2 - 6$ es irreducible sobre el campo $\mathbb{Q}$.

34. Demuestre que el polinomio $f(x) = x^2 + 1$ es irreducible sobre el campo $\mathbb{R}$.

35. Sean $f, g, h \in \mathcal{P}(\mathbb{F})$ tales que f es irreducible sobre $\mathbb{F}$ y $f \mid (gh)$. Demuestre que $f \mid g$ o $f \mid h$.

Raíces de polinomios

36. Teorema del resto. Sean $f \in \mathcal{P}(\mathbb{C})$ y $a \in \mathbb{C}$. Entonces el resto al dividir $f(x)$ entre $x - a$ es igual al valor del polinomio f en el punto a. En otras palabras, si

$$f(x) = (x - a)q(x) + r,$$

donde $q \in \mathcal{P}(\mathbb{C})$ y $r \in \mathbb{C}$, entonces $f(a) = r$.

37. Sean $f \in \mathcal{P}(\mathbb{C})$, $a, b \in \mathbb{C}$, $a \neq 0$. Demuestre que el residuo de dividir el polinomio $f(x)$ entre el binomio $ax - b$ es $f(b/a)$.

38. Sean $f \in \mathcal{P}(\mathbb{C})$, $a, b \in \mathbb{C}$, $a \neq 0$. Demuestre que el residuo de dividir el polinomio $f(x)$ entre el binomio $ax + b$ es $f(-b/a)$.

39. Criterio de divisibilidad de un polinomio entre un binomio mónico (corolario del teorema del resto). Sean $f \in \mathcal{P}(\mathbb{C})$ y $a \in \mathbb{C}$. Entonces $(x - a)$ divide a $f(x)$ si, y sólo si, $f(a) = 0$.

40. Criterio de divisibilidad de un polinomio entre un producto de dos binomios mónicos. Sea $f \in \mathcal{P}(\mathbb{C})$ y sean $a_1, a_2 \in \mathbb{C}$, $a_1 \neq a_2$. Demuestre que las siguientes condiciones son equivalentes:

(a) $(x - a_1)(x - a_2) \mid f(x)$.

(b) $f(a_1) = 0$, $f(a_2) = 0$.

41. Demuestre que $x^2 + x + 1$ divide a $(x + 1)^n - x^n - 1$, si y sólo si, n es impar y $3 \nmid n$.

42. Criterio de divisibilidad de un polinomio entre un producto de binomios mónicos. Sea $f \in \mathcal{P}(\mathbb{C})$ y sean $a_1, \ldots, a_m \in \mathbb{C}$ diferentes a pares. Demuestre que las siguientes condiciones son equivalentes:

(a) $\left(\prod_{j=1}^{m}(x-a_j)\right) \mid f(x)$.

(b) $f(a_1)=0,\ f(a_2)=0,\ \ldots,\ f(a_m)=0$.

43. Polinomio básico de Lagrange. Sean $a_1,\ldots,a_n$ algunos números complejos diferentes a pares. Definimos al polinomio f mediante la regla:

$$f(x)=\prod_{j=2}^{n}\frac{x-a_j}{a_1-a_j}$$

I. Demuestre que $\deg(f)=n-1$, $f(a_1)=1$, $f(a_2)=\ldots=f(a_n)=0$.

II. Demuestre f es el único polinomio con las propiedades del inciso I, esto es, si $g\in\mathcal{P}(\mathbb{C})$, $\deg(g)=n-1$, $g(a_1)=1$, $g(a_2)=\ldots=g(a_n)=0$, entonces $g=f$.

44. Cualquier polinomio que tiene más raíces que su grado debe ser cero. Sea $f\in\mathcal{P}(\mathbb{C})$ tal que $\deg(g)\le m$ y f tiene al menos $m+1$ raíces diferentes a pares. Demuestre que $f=\mathbf{0}_{\mathcal{P}}$.

45. Cualquier polinomio que tiene una infinidad de raíces debe ser cero. Sea $f\in\mathcal{P}(\mathbb{C})$ y sea C un subconjunto infinito de $\mathbb{C}$ tal que $f(a)=0$ para cada $a\in C$. Demuestre que $f=\mathbf{0}_{\mathcal{P}}$.

46. Dos polinomios que coinciden en una infinidad de puntos deben tener los mismos coeficientes. Sean $f,g\in\mathcal{P}(\mathbb{C})$ y sea C un subconjunto infinito de $\mathbb{C}$ tal que $f(a)=g(a)$ para cada $a\in C$. Demuestre que $f=g$.

47. Dos polinomios que coinciden como funciones deben tener los mismos coeficientes. Sean $f,g\in\mathcal{P}(\mathbb{C})$ tales que $f(a)=f(b)$ para cada $a\in\mathbb{C}$. Demuestre que $f=g$, esto es, f y g tienen los mismos coeficientes.

48. Teorema sobre raíces racionales de un polinomio con coeficientes enteros. Sea f un polinomio con coeficientes enteros:

$$f(x)=\sum_{m=0}^{n}a_m x^m,\qquad a_0,\ldots,a_n\in\mathbb{Z},$$

y sean $j,k\in\mathbb{Z}$ tales que $k\ne 0$, $\operatorname{mcd}(j,k)=1$, y $f(j/k)=0$. Demuestre que $j\mid a_0$ y $k\mid a_n$.

49. Teorema sobre raíces racionales de un polinomio mónico con coeficientes enteros. Sea f un polinomio mónico con coeficientes enteros:

$$f(x)=a_0x^0+\ldots+a_{n-1}x^{n-1}+x^n,\qquad a_0,\ldots,a_{n-1}\in\mathbb{Z},$$

y sean $j,k\in\mathbb{Z}$ tales que $k>0$, $\operatorname{mcd}(j,k)=1$, y $f(j/k)=0$. Demuestre que $j\mid a_0$ y $k=1$.

50. Teorema sobre raíces complejas de un polinomio con coeficientes reales. Sea $f \in \mathcal{P}(\mathbb{R})$ y sea $z \in \mathbb{C}$ tal que $f(z) = 0$. Demuestre que $f(\overline{z}) = 0$.

51. Teorema principal del álgebra de polinomios (sin demostración). Sea $f \in \mathcal{P}(\mathbb{C})$, $\deg(f) \geq 1$. Entonces existe un $a \in \mathbb{C}$ tal que $f(a) = 0$.

El siguiente resultado podría llamarse "versión fuerte del teorema principal del álgebra de polinomios".

52. Teorema sobre la factorización de polinomios con coeficientes complejos. Sea $f \in \mathcal{P}(\mathbb{C})$, $\deg(f) = n \geq 1$. Demuestre que existen $c, a_1, \ldots, a_n \in \mathbb{C}$ tales que

$$f(x) = c \prod_{j=1}^{n} (x - a_j).$$

Observación: algunos de los números $a_1, \ldots, a_n$ pueden ser iguales entre si.
Sugerencia: utilice la inducción matemática y el resultado 51.

53. Sea $f \in \mathcal{P}(\mathbb{C})$ y sea $a \in \mathbb{C}$ una raíz de multiplicidad al menos m del polinomio f, esto es,

$$(x - a)^m \mid f(x).$$

Sea $d = \operatorname{mcd}(f, f')$. Demuestre que $(x - a)^{m-1} \mid d(x)$.