Ideales del anillo de los polinomios de una variable

Objetivos. Demostrar que el anillo de los polinomios de una variable es un anillo de ideales principales (en otras palabras, es un dominio de ideales principales).

Requisitos. Multiplicación y división de polinomios. Para comprender mejor el tema, se recomienda conocer el concepto de ideal de un anillo.

Polinomios como un anillo euclideano

1. Polinomios como un anillo asociativo conmutativo con unidad. El conjunto $\mathcal{P}(\mathbb{F})$ de todos los polinomios con coeficientes en $\mathbb{F}$ se considera con dos operaciones binarias: adición y multiplicación. Notemos que la multiplicacion por escalares se puede considerar como un caso particular de multiplicación de polinomios, a saber, como multiplicación por polinomios constantes. Los polinomios con la operación de adición forman un grupo abeliano (la adición es asociativa, conmutativa, existe un elemento neutro con respecto a la adición y para cada elemento existe un elemento inverso aditivo). La multiplicación es distributiva con respecto a la adición, asociativa, conmutativa, y existe un elemento neutro con respecto a la multiplicación. Todo esto significa que $\mathcal{P}(\mathbb{F})$ es un anillo asociativo conmutativo con unidad.

2. Grado del producto de dos polinomios. Sean $f, g \in \mathcal{P}(\mathbb{F}) \setminus \{0\}$. Entonces

$$\deg(fg) = \deg(f) + \deg(g).$$

Esta fórmula se puede extender al caso cuando $f = 0$ o $g = 0$ si se pone $\deg(0) = -\infty$.

3. Anillo de los polinomios es un dominio de integridad. Sean $f, g \in \mathcal{P}(\mathbb{F})$ tales que $fg = 0$. Demuestre que $f = 0$ o $g = 0$.

4. Los polinomios forman un anillo euclideano. La función

$$\deg\colon \mathcal{P}(\mathbb{F}) \setminus \{0\} \to \{0, 1, 2, \dots\}$$

cumple con las siguientes propiedades:

1. Para todo $f \in \mathcal{P}(\mathbb{F})$ y todo $g \in \mathcal{P}(\mathbb{F}) \setminus \{0\}$ existen $q, r \in \mathcal{P}(\mathbb{F})$ tales que
$$f = qg + r \qquad \wedge \qquad (r = 0 \quad \vee \quad \deg(r) < \deg(g)).$$
2. Para todo $f, g \in \mathcal{P}(\mathbb{F}) \setminus \{0\}$
$$\deg(fg) \geq \deg(f).$$

Por definición, esto significa que $\mathcal{P}(\mathbb{F})$ con la función deg es un *anillo euclideano*.

5. Elementos invertibles del anillo de los polinomios. Un polinomio $f \in \mathcal{P}(\mathbb{F})$ se llama *elemento invertible del anillo de los polinomios* $\mathcal{P}(\mathbb{F})$ si existe un polinomio $g \in \mathcal{P}(\mathbb{F})$ tal que $fg = 1$. Usando la fórmula del grado del producto es fácil demostrar el siguiente "criterio de invertibilidad de un polinomio":

$$f \text{ es invertible en } \mathcal{P}(\mathbb{F}) \qquad \Longleftrightarrow \qquad \deg(f) = 0.$$

Ideales del anillo de los polinomios: definición y ejemplos

6. Definición (ideal de polinomios). Un subconjunto J de $\mathcal{P}(\mathbb{F})$ se llama *ideal* de $\mathcal{P}(\mathbb{F})$ si se cumplen las siguientes condiciones:

1. J es cerrado bajo la adición:

$$\forall f, g \in J \qquad f + g \in J.$$

2. J tiene "propiedad absorbente" respecto a la multiplicación:

$$\forall f \in J \qquad \forall g \in \mathcal{P}(\mathbb{F}) \qquad fg \in J.$$

3. $0 \in J$.

4. $1 \notin J$.

7. Corolarios de los axiomas de ideal. Sea J un ideal de $\mathcal{P}(\mathbb{F})$. Entonces:

1. J es cerrado bajo la multiplicación:

$$\forall f, g \in J \qquad fg \in J.$$

2. J es cerrado bajo la multiplicación por escalares:

$$\forall f \in J \qquad \forall \lambda \in \mathbb{F} \qquad \lambda f \in J.$$

3. J es un subespacio vectorial del espacio vectorial $\mathcal{P}(\mathbb{F})$.

8. Proposición (criterio de ideal de polinomios). Sea J un subconjunto de $\mathcal{P}(\mathbb{F})$ que cumple con las siguientes propiedades:

1' J es un subespacio vectorial de $\mathcal{P}(\mathbb{F})$.

2' J tiene propiedad absorbente respecto a la multiplicación:

$$\forall f \in J \qquad \forall g \in \mathcal{P}(\mathbb{F}) \qquad fg \in J.$$

3' $J \neq \mathcal{P}(\mathbb{F})$.

Entonces J es un ideal de $\mathcal{P}(\mathbb{F})$ en el sentido de la definición anterior.

9. Ejercicio. Demuestre que $J = \{f \in \mathcal{P}(\mathbb{R})\colon f'(2) = 0\}$ no es ideal de $\mathcal{P}(\mathbb{R})$.

10. Ejemplo. El conjunto $J = \{f \in \mathcal{P}(\mathbb{R})\colon f(2) = 0\}$ es un ideal de $\mathcal{P}(\mathbb{R})$.

11. Ejemplo. El conjunto $J = \{f \in \mathcal{P}(\mathbb{R})\colon f(7) = f(-2) = 0\}$ es un ideal de $\mathcal{P}(\mathbb{R})$.

12. Ejemplo. El conjunto $J = \{f \in \mathcal{P}(\mathbb{R})\colon f(4) = f'(4) = 0\}$ es un ideal de $\mathcal{P}(\mathbb{R})$.

13. Ejemplo. El conjunto $J = \{f \in \mathcal{P}(\mathbb{R})\colon f(-3) = f'(-3) = f(7) = 0\}$ es un ideal de $\mathcal{P}(\mathbb{R})$.

14. Proposición (del ideal generado por un polinomio). Sea $g \in \mathcal{P}(\mathbb{F})$, $\deg(g) \neq 0$. Entonces

$$J \coloneqq g\mathcal{P}(\mathbb{F}) = \big\{gh\colon \quad h \in \mathcal{P}(\mathbb{F})\big\} = \big\{f \in \mathcal{P}(\mathbb{F})\colon \quad g \mid f\big\}$$

es un ideal de $\mathcal{P}(\mathbb{F})$. Además es el ideal más pequeño que contiene al polinomio g.

15. Definición (el ideal generado por un polinomio, ideales principales). En las condiciones de la proposición anterior se dice que J es el ideal *generado* por g y que g es un *generador* de J. Cualquier ideal generado por un elemento se llama *ideal principal*.

16. Ejercicio. Muestre que los ideales de los ejemplos 10–13 son ideales principales.

17. Ejercicio. Sean J_1 y J_2 dos ideales del anillo de polinomios $\mathcal{P}(\mathbb{F})$. Demuestre que $J_1 \cap J_2$ también es un ideal de $\mathcal{P}(\mathbb{F})$.

Anillo de los polinomios es un dominio de ideales principales

18. Ideal nulo está generado por el polinomio nulo. Notemos que el ideal nulo $J = \{0\}$ se puede representar como $0\mathcal{P}(\mathbb{F})$. Vamos a excluir este caso trivial del siguiente teorema.

19. Definición (polinomio mónico). Un polinomio se llama mónico si es distinto del polinomio cero y su coeficiente mayor es 1.

20. Teorema (de los ideales del anillo de los polinomios de una variable). Sea J un ideal no nulo de $\mathcal{P}(\mathbb{F})$. Entonces existe un único polinomio mónico $g \in \mathcal{P}(\mathbb{F})$ con $\deg(g) > 0$ tal que

$$J = g\mathcal{P}(\mathbb{F}).$$

Este polinomio g es de grado menor entre todos los polinomios no nulos que pertenecen a J.

Demostración. Existencia. Denotemos por G al conjunto de los grados de los polinomios pertenecientes a $J \setminus \{0\}$:

$$G \coloneqq \big\{\deg(p)\colon\ p \in J \setminus \{0\}\big\}$$

Por la hipótesis, $J \setminus \{0\} \neq \varnothing$. La definición de ideal implica que los polinomios de grado 0 (es decir, constantes no nulas) no pertenecen a J. Así que G es un subconjunto no vacío del conjunto de los números enteros positivos $\{1, 2, \ldots\}$. Por lo tanto G tiene un elemento mínimo. Lo denotamos por d:

$$d \coloneqq \min_{p \in J \setminus \{0\}} \deg(p).$$

Sea $h \in J \setminus \{0\}$ tal que $\deg(h) = d$. Denotemos por g al polinomio h dividido entre su coeficiente mayor. Entonces g es un polinomio mónico y $\deg(g) = d$.

Para cualquier polinomio $p \in J$ existen $q, r \in \mathcal{P}(\mathbb{F})$ tales que

$$p = qg + r \qquad \wedge \qquad \deg(r) < \deg(g).$$

Como $r = p - qg \in J$ y $\deg(r) < \deg(g) = d$, el polinomio r debe ser cero. Por lo tanto g divide a p. Concluimos que g divide a cualquier elemento p de J. En otras palabras, g genera a J:

$$J = g\mathcal{P}(\mathbb{F}).$$

Unicidad. Sean f y g polinomios mónicos tales que

$$J = f\mathcal{P}(\mathbb{F}) = g\mathcal{P}(\mathbb{F}).$$

Entonces f divide a g y viceversa. Como $f \neq 0$ y $g \neq 0$, esto implica que $f = cg$ con una constante $c \in \mathbb{F} \setminus \{0\}$. Ahora de la hipótesis que f y g son mónicos sigue que $f = g$. □

21. Nota. El teorema se generaliza de manera natural a cualquier anillo euclideano.

22. Ejemplo. El conjunto

$$J = \big\{f \in \mathcal{P}(\mathbb{R})\colon \quad f(4) = 0, \quad f(-3) = 0, \quad f'(-3) = 0\big\}$$

es un ideal del anillo $\mathcal{P}(\mathbb{R})$. Es fácil ver que el generador mónico de J es el polinomio $f(x) = (x - 4)(x + 3)^2$.