Capítulo

9

Anillo de Polinomios

9.1 Introducción

Hemos dejado el estudio de los polinomios para el final, pues este ejemplo nos permitirá repasar todas las definiciones y propiedades de anillos, estudiadas en capítulos anteriores. Realmente los polinomios es uno de los ejemplos de anillos, más estudiados desde la antigüedad por estar estrechamente relacionado con la solución de ecuaciones en una o varias incógnitas.

Muchas de las propiedades básicas de los polinomios como lo son las operaciones de suma, producto y división, el cálculo de raíces y la factorización, ya las hemos estudiado en la escuela secundaria, de un modo operacional.

En este capítulo, los polinomios serán estudiados desde el punto de vista de su estructura de anillo. Este nuevo enfoque aclarará muchos de los conceptos ya estudiados en cursos anteriores al, considerarlos dentro de propiedades más generales de anillos, y al mismo tiempo abrirá nuevos caminos que nos conduciran a resultados bastante vigorosos, resando las técnicas desarrolladas en el Capítulo 6.

Definición 9.1.1 *Sea A un anillo. Un* **polinomio** *en la indeterminada x es una suma formal*

$$f(x) = \sum_{i=1}^{\infty} a_i x^i$$

donde $a_i \in A$, para todo $i \geq 0$, y $a_i = 0$ para todo i, excepto para un número finito de ellos.

Observación: Podemos dar otra definición de lo que es un polinomio, sin hacer referencia a la variable x.

Definición 9.1.2 *Sea A un anillo. Un* **polinomio** *sobre A es una sucesión infinita $(a_0, a_1, \ldots, a_n, \ldots)$ donde $a_i \in A$; para todo i y $a_i = 0$ para casi todos los i.*

Una sucesión $(a_0, a_1, \ldots, a_n, \ldots)$ donde casi todos los a_i son iguales a cero, se denomina una **sucesión casi nula**.

La definición (**??**) es más formal que la definición (**??**) pues no hace uso de la variable x. Sin embargo el símbolo x se ha utilizado para expresar los polinomios desde hace mucho tiempo y aún se usa en la actualidad. Para mantenernos en esta tradición usaremos la definición (**??**) de polinomios. Si hacemos $x = (0, 1, 0, 0, \ldots)$, y entonces la variable x es un polinomio en si misma, y deja de ser un objeto misterioso. Nosotros seguiremos denotando los polinomios a la manera clásica

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

donde se sobre entiende que $a_i = 0$ para $i > n$.

El conjunto de los polinomios sobre el anillo A, será denotado por $A[x]$.

Definición 9.1.3 *Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0$ un polinomio en $A[x]$. Entonces los a_i se llaman los* **coeficientes** *del polinomio.*

Definición 9.1.4 *El polinomio que tiene todos sus coeficientes iguales a 0, se llama* **polinomio nulo o polinomio cero** *y se denota por 0.*

Definición 9.1.5 *El polinomio que tiene todos sus coeficientes a_i iguales a cero, para $i \geq 1$ se llama* **polinomio constante**.

Definición 9.1.6 *Dados dos polinomios $f(x) = a_n x^n + \cdots + a_1 x + a_0$ y $g(x) = b_m x^m + \cdots + b_1 x + b_0$, diremos que son iguales y lo denotamos por $f(x) = g(x)$, si y sólo si*

$$a_i = b_i \qquad \forall i \geq 0$$

En el conjunto de polinomios $A[x]$ se pueden definir un par de operaciones

Suma de Polinomios

$$(a_n x^n + \cdots + a_1 x + a_0) + (b_m x^m + \cdots + b_1 x + b_0)$$

$$= \quad C_k x^k + \cdots + C_1 x + C_0 \tag{9.1}$$

donde $C_i = a_i + b_i, \quad a \leq i \leq k$

Producto de Polinomios

$$(a_n x^n + \cdots + a_1 x + a_0)(b_m x^m + \cdots + b_1 x + b_0)$$

$$= \quad C_k x^k + \cdots + C_1 x + C_0 \tag{9.2}$$

donde $C_s = \sum_{i+j=s} a_i b_j$, para todo $0 \leq s \leq k$.

Ejemplo: Sean $f(x) = 2x^2 + 3x - 1$ y $g(x) = x^3 + 1$ dos polinomios en $\mathbb{Z}[x]$. Entonces para poder sumar f y g es necesario introducir coeficientes nulos en ambos polinomios, de la manera siguiente

$$\begin{aligned} f(x) &= 0x^3 + 2x^2 + 3x - 1 \\ &= a_3 x^3 + a_2 x^2 + a_1 x + a_0 \\ g(x) &= x^3 + 0x^2 + 0x + 1 \\ &= b_3 x^3 + b_2 x^2 + b_1 x + b_0 \end{aligned}$$

luego sumamos los polinomios, de acuerdo a la definición, es decir, sumamos los coeficiente de potencias de x iguales

$$\begin{aligned} f(x) + g(x) &= (0+1)x^3 + (2+0)x^2 + (3+0)x + (1-1) \\ &= x^3 + 2x^2 + 3x \end{aligned}$$

Para multiplicar los polinomios, construimos los elementos C_i en la expresión (**??**). Luego

$$\begin{aligned} C_0 &= a_0b_0 \\ &= (-1)(1) \\ &= -1 \end{aligned}$$

$$\begin{aligned} C_1 &= a_0b_1 + a_1b_0 \\ &= (-1)0 + 3(1) \\ &= 3 \end{aligned}$$

$$\begin{aligned} C_2 &= a_0b_2 + a_1b_1 + a_2b_0 \\ &= (-1)(0) + 3(0) + (2)(1) \\ &= 2 \end{aligned}$$

$$\begin{aligned} C_3 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 \\ &= (-1)(1) + 3(0) + 2(0) + (0)1 \\ &= -1 \end{aligned}$$

$$\begin{aligned} C_4 &= a_1b_3 + a_2b_2 + a_3b_1 \\ &= 3(1) + (2)(0) + (0)(0) \\ &= 3 \end{aligned}$$

$$\begin{aligned} C_5 &= a_2b_3 + a_3b_2 \\ &= 2(1) + (0)(0) \\ &= 2 \end{aligned}$$

$$\begin{aligned} C_6 &= a_3b_3 \\ &= (0)(1) \\ &= 0 \end{aligned}$$

Luego el resultado de multiplicar $f(x)$ y $g(x)$ viene expresado por

$$f(x)g(x) = 2x^5 + 3x^4 - x^3 + 2x^2 + 3x + 1$$

Observación: Se recomienda al estudiante hacer la multiplicación por el método tradicional, y luego comparar ambos resultados.

A continuación definimos una función que asocia a cada polinomio no nulo $f(x)$ un entero no negativo.

Definición 9.1.7 *Sea $f(x) = a_s x^s + \cdots + a_1 x + a_0$ en $A[x]$, no nulo. Entonces el* **grado de** $f(x)$*, denotado por $g(f(x))$, es el mayor entero no negativo n, tal que $a_n \neq 0$.*

Observación 1: Si el grado de $f(x)$ es n, entonces $a_k = 0$, para todo $k > n$ y escribimos

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

es decir, no se colocan aquellos términos $a_x x^i$ con $i > n$, pues son todos nulos.

El término a_n se llama **coeficiente principal de** $f(x)$.

Definición 9.1.8 *Un polinomio de la forma $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ se llama* **mónico**.

Observación 2: Si $f(x)$ es un polinomio constante no nulo, entonces $g(f(x)) = 0$.

Observación 3: El grado del polinomio 0 lo definimos mediante el símbolo especial $-\infty$, de acuerdo a las siguientes reglas

i) $-\infty < n$, para todo $n \in \mathbb{Z}$

ii) $-\infty + (-\infty) = -\infty$

iii) $-\infty + n = -\infty$, para todo $n \in \mathbb{Z}$

Proposición 9.1.1 *Sea A un Dominio de Integridad. Sean $f(x)$ y $h(x)$ dos polinomios no nulos en $A[x]$, de grados n y m respectivamente. Entonces*

i) $g(f(x)+h(x)) \leq \max\{n,m\}$

ii) $g(f(x)h(x)) = n+m$

Demostración: i) Supongamos que $n > m$. Entonces el coeficiente principal de $f(x)+h(x)$ es igual al coeficiente principal de $f(x)$ y por lo tanto

$$g(f(x)+h(x)) = g(f(x)) = n = \max\{n,m\}$$

Si suponemos que $n = m$, entonces pueden ocurrir dos casos

I) La suma de los coeficientes principales de f y h es cero. Luego $g(f(x)+h(x)) < n$.

II) La suma de los coeficientes principales de f y h es distinta de cero. En este caso $g(f(x)+h(x)) = n$.

Luego en cualquiera de los dos casos obtenemos la desigualdad deseada.

ii) Para calcular el grado del producto, sean

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

y

$$h(x) = b_m x^m + \cdots + b_1 x + b_0$$

entonces hacemos la multiplicación.

$$f(x)h(x) = C_s x^s + \cdots + C_1 x + C_0$$

Afirmamos que $C_{n+m} \neq 0$. En efecto, se tiene $C_{n+m} = a_n b_m \neq 0$, pues tanto a_n como b_m son no nulos. Por otra parte si $s > n+m$ se tiene

$$C_s = \sum_{i+j=s} a_i b_j$$

Luego cada término $a_i b_j$ en dicha suma es igual a cero, pues se debe tener $i > n$ ó bien $j > m$, lo cual implica $a_i = 0$ ó bien $b_j = 0$.

Por lo tanto $C_s = 0$ para $s > n + m$, y así hemos probado que el grado de $f(x)g(x)$ es $m + n$.

♠

Teorema 9.1.1 *El conjunto $A[x]$ de polinomios sobre un anillo A, es un anillo con las operaciones de suma y producto de polinomios. Si A es un anillo conmutativo con unidad, entonces $A[x]$ es un anillo conmutativo con unidad.*

Demostración: Es claro que $A[x]$ es un grupo abeliano con la suma de polinomios. El elemento neutro para la suma es el polinomio nulo. Si $p(x) = a_n x^n + \cdots a_1 x + a_0$, entonces el opuesto de $p(x)$ es

$$-p(x) = (-a_n)x^n + \cdots + (-a_1)x - a_0.$$

Con respecto al producto, se demuestra que esta operación es asociativa y satisface las leyes distributivas.

Además, si A es conmutativo sean $f(x)$ y $h(x)$ dos polinomios en $A[x]$, luego

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

y

$$h(x) = b_m x^m + \cdots + b_1 x + b_0$$

Entonces se tiene

$$\begin{aligned} f(x)h(x) &= C_s x^s + \cdots + C_1 x + C_0 \\ h(x)f(x) &= d_s x^s + \cdots + d_1 x + d_0 \end{aligned}$$

con $s = m + n$.

Pero todo $0 \leq i \leq s$, obtenemos

$$\begin{aligned} C_i &= \sum_{k+j=i} a_k b_j \\ &= \sum_{j+k=i} b_j a_k \\ &= d_i \end{aligned}$$

Luego $f(x)h(x) = h(x)f(x)$ por tener todos sus coeficientes iguales.

Si A tiene unidad 1, entonces el polinomio constante $f(x) = 1$ es el polinomio unidad para el producto.

♠

Proposición 9.1.2 *Si el anillo A es un Dominio de Integridad, entonces el anillo $A[x]$ es un Dominio de Integridad.*

Demostración: Es claro que $A[x]$ es un anillo conmutativo con unidad, de acuerdo al teorema anterior.

Por otro lado, sean $f(x)$ y $h(x)$ son dos polinomios en $A[x]$, tal que $f(x)h(x) = 0$.

Si $f(x) \neq 0$ y $h(x) \neq 0$ se tiene entonces

$$\begin{aligned} g(f(x)) &\leq g(f(x)h(x)) \\ &= g(0) \\ &= -\infty \end{aligned}$$

de donde

$$g(f(x)) = -\infty$$

y por lo tanto $f(x) = 0$, lo cual es una contradicción. Luego $f(x) = 0$ ó $h(x) = 0$.

♠

Observación: Sabemos que todo Dominio de Integridad posee un cuerpo de cocientes. Por lo tanto $A[x]$ tiene su cuerpo de cocientes, el cual se llama **cuerpo de funciones racionales en** x y sus elementos son cocientes de polinomios en $A[x]$.

9.2 El Algoritmo de División

En esta sección consideramos el anillo de polinomios sobre un cuerpo K, el cual será denotado por $K[x]$. Probaremos que este anillo tienen la propiedad de ser euclideano y por lo tanto valen todas las propiedades de los Dominios Euclideanos descritas en el capítulo 6.

Proposición 9.2.1 *Sean $f(x)$ y $h(x)$ polinomios no nulos en $K[x]$. Entonces $g(f(x)) \leq g(f(x)h(x))$.*

Demostración: De acuerdo a la proposición (**??**) se tiene

$$g(f(x)h(x)) = g(f(x)) + g(h(x))$$

luego

$$g(f(x)) \leq g(f(x)h(x)).$$

♠

Teorema 9.2.1 *(Algoritmo de División) Sean $f(x)$ y $h(x)$ dos polinomios en $K[x]$, con $h(x) \neq 0$. Luego existen polinomios $q(x)$ y $r(x)$ en $K[x]$, tales que*

$$f(x) = h(x)q(x) + r(x)$$

con

$$r(x) = 0 \quad ó \quad g(r(x) < g(h(x))$$

Demostración: Si $f(x) = 0$, tomamos entonces $q(x) = 0$ y $r(x) = 0$.

Si $g(f(x)) < g(h(x))$, tomamos $q(x) = 0$ y $r(x) = f(x)$.

Supongamos entonces que $g(f(x)) \geq g(h(x))$ y pongamos

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

y

$$g(x) = b_m x^m + \cdots + b_1 x + b_0$$

con $n \geq m$.

Podemos entonces usar inducción sobre n para obtener el resultado. Si $n = 0$, entonces

$$f(x) = a_0, \quad h(x) = b_0 \quad \text{y}$$

$$f(x) = a_0 b_0^{-1} h(x) + 0$$

luego tomando $q(x) = a_0 b_0^{-1}$ y $r(x) = 0$ se obtiene el resultado.

Supóngase que el teorema es cierto para todo polinomio de grado k, con $k < n$. Luego

$$f(x) - a_n b_m^{-1} x^{n-m} h(x)$$

es un polinomio de grado menor que n y por la hipótesis de inducción existen $q'(x)$ y $r'(x)$ tales que

$$f(x) - a_n b_m^{-1} x^{n-m} h(x) = h(x) q'(x) + r'(x)$$

con $r'(x) = 0$ ó $g(r'(x)) < g(h(x))$

Por lo tanto, tenemos

$$f(x) = h(x) \left[q'(x) + a_n b_m^{-1} x^{n-m} \right] + r'(x)$$

Si tomamos $q(x) = q'(x) + a_n b^{-1} m x^{n-m}$ y $r(x) = r'(x)$ se tiene el resultado deseado

♠

Observación: Los polinomios $q(x)$ y $r(x)$ se llaman respectivamente **cociente** y **resto** de la división de $f(x)$ entre $h(x)$.

Si definimos la función $d : K[x] \longrightarrow \mathbb{Z}^+$ por $d(f(x)) = g(f(x))$, entonces se tiene

Corolario 9.2.1 *El anillo de polinomios $K[x]$ es un* **Dominio de Euclideano**.

Definición 9.2.1 *Sea K un cuerpo y $f(x)$, $h(x)$ en $K[x]$. Diremos que el polinomio $f(x)$ es divisible entre $h(x)$, si existe otro polinomio $c(x)$ en $K[x]$, tal que*

$$f(x) = h(x)c(x)$$

Definición 9.2.2 *Sea $f(x)$ un polinomio en $K[x]$. Diremos que $f(x)$ es un* **polinomio irreducible** *en $K[x]$, o irreducible sobre K, si cada vez que*

$$f(x) = h(x)q(x),$$

entonces $h(x)$ o $q(x)$ es una constante.

Observación: Como consecuencia directa del corolario anterior se tiene que $K[x]$ es un Dominio de Ideales Principales y por lo tanto un Dominio de Factorización Unica. Luego se tienen los hechos siguientes

Teorema 9.2.2 *Sea $f(x)$ un polinomio en $K[x]$. Entonces existen polinomios irreducibles $p_1(x), \cdots, p_s(x)$, los cuales son únicos salvo asociados, tales que*

$$f(x) = p_1(x) \cdots p_s(x).$$

Teorema 9.2.3 *Si $f(x)$ y $h(x)$ son polinomios en $K[x]$, entonces el Máximo Común Divisor entre $f(x)$ y $h(x)$, el cual denotamos por $d(x)$, siempre existe. Además se tiene*

$$d(x) = p(x)f(x) + q(x)h(x),$$

para algunos polinomios $p(x)$ y $q(x)$ en $K[x]$.

A fin de tener una mejor información sobre el anillo de polinomios $K[x]$, el paso siguiente será determinar todas las unidades en $K[x]$ y los elementos irreducibles.

Para hallar las unidades usaremos un resultado que hemos probado sobre los Dominios Euclideanos, el cual establece:

"El polinomio $u(x)$ es una unidad, si y sólo si el grado de $u(x)$ es igual al grado del polinomio 1". Luego las unidades de $K[x]$ son precisamente los polinomios constantes (distintos de cero), pues grado(1)=0.

El problema de determinar cuando un polinomio es irreducible, es uno de los más difíciles en Algebra y ha sido estudiado desde hace varios siglos. No se tiene un criterio general para decidir la condición de irreducibilidad. Sólo existen criterios que se pueden aplicar en situaciones especiales, como se verá más adelante.

Veamos mediante un ejemplo como se puede determinar si un polinomio es irreducible, usando las técnicas de la teoría de Anillos.

Ejemplo: Probar que $f(x) = x^2 + 1$ es irreducible en $\mathcal{Q}[x]$.

Solución: Sea $I = (x^2 + 1)$ el ideal principal generado por el elemento $f(x)$ en $\mathcal{Q}[x]$. Consideremos el anillo cociente $\mathcal{Q}[x]/I$.

Sea $f(x)$ un polinomio en $\mathcal{Q}[x]$, entonces por el algoritmo de división, existen polinomios $q(x)$ y $r(x)$ tales que

$$f(x) = q(x)(x^2 + 1) + r(x)$$

con $r(x) = 0$ ó $g(r(x)) < g(x^2 + 1)$.

Luego el polinomio $f(x)$ se puede reducir módulo I a un polinomio $r(x)$ de grado 1. Por lo tanto los elementos de $\mathcal{Q}[x]/I$ son polinomios lineales $ax + b$, con a y b en $\mathcal{Q}$. Además de la relación $x^2 + 1 = 0$, se sigue $x^2 = -1$.

Afirmamos que $\mathcal{Q}[x]/I$ es un cuerpo, para lo cual sea $t = ax + b \in \mathcal{Q}[x]/I$ y probaremos que si t es distinto de cero, entonces es invertible. En efecto, $t \neq 0$ implica que $a^2 + b^2 \neq 0$. Además

$$\begin{aligned}(ax+b)(-ax+b) &= -a^2x^2+b^2\\ &= a^2+b^2\end{aligned}$$

Luego hacemos $S=\lambda x+r$ con

$$\lambda=\frac{-a}{a^2+b^2} \quad \text{y} \quad r=\frac{b}{a^2+b^2}$$

Es claro que $S\in\mathcal{Q}[x]/I$, y además $ts=1$. Luego t es invertible.

Una vez demostrado que $\mathcal{Q}[x]/I$ es un cuerpo, se deduce que el ideal I es maximal y por lo tanto ideal primo. Luego el elemento x^2+1 es irreducible en $\mathcal{Q}[x]$.

Ejercicios

1) Sean $f(x)=3x^4+2x^3-5x^2+1$ y $h(x)=4x^2+10x-3$. Calcule $f(x)+g(x)$ y $f(x)h(x)$.

2) Mostrar que si $f(x), h(x)$ y $g(x)$ son polinomios en $\mathbb{Z}[x]$ entonces

i) $(f(x)+h(x))+g(x)=f(x)+(h(x)+g(x))$
ii) $[f(x)+h(x)]\,g(x)=f(x)g(x)+h(x)g(x)$

3) Si $f(x)=a_nx^n+\cdots+a_1x+a_0$, hallar los coeficientes del polinomio $f(x)(x-1)$.

4) Sea $f(x)=6x^3+3x^2-2$ y $h(x)=2x^2-6$ dos polinomios en $\mathbb{Z}_7[x]$. Hallar:

a) $f(x)+h(x)$
b) $f(x)h(x)$

5) Hallar el cociente y el resto de la división de los siguientes polinomios en $\mathcal{Q}[x]$.

a) $f(x)=10x^8-2x^2+6, \quad h(x)=x^2+2$
b) $f(x)=5x^6-3x^3+18x-1, \quad h(x)=2x^4+15x-3$
c) $f(x)=16x^7+8x^4+5x^3-6x^2, \quad h(x)=3x^4-8x^3$
d) $f(x)=x^5+x^4+x^3+x^2+x+1, \quad h(x)=x-1$

6) Hallar el Máximo Común Divisor entre $x^6 - 4x^3 + 1$ y $3x^2 + 5x - 1$ en $\mathcal{Q}[x]$.

7) Demuestre que $p(x) = x^2 - 2$ es irreducible sobre $\mathcal{Q}[x]$.

8) Sea $p(x) = 1 + x + x^2 + \cdots + x^{n-1}$ en $\mathcal{Q}[x]$. Probar que $x^n - 1 = p(x)(x - 1)$.

9) Sea $\phi : A \longrightarrow A'$ un homomorfismo de anillos. Probar que existe un homomorfismo de anillos entre $A[x]$ y $A'[x]$.

10) Demuestre que todo **polinomio lineal** $f(x) = ax + b$ en $K[x]$ es irreducible.

11) Usando las notaciones del problema 9, probar que si $f(x)$ es reducible en $A[x]$, entonces su imágen es reducible en $A'[x]$.

12) ¿Cuántos polinomios de grado 3 se pueden construir en $\mathbb{Z}_5$? Generalize este resultado para cualquier grado.

9.3 Raíces de Polinomios

A lo largo de esta sección veremos la relación existente entre un polinomio $f(x)$ y la resolución de la ecuación

$$f(x) = 0$$

Definición 9.3.1 *Sea K un cuerpo. Una* **extensión** F **de** K *es un cuerpo que contiene a K como subcuerpo. Es decir K es un cuerpo con las mismas operaciones definidas en F.*

Ejemplo: Los números complejos $\mathbb{C}$ son una extensión del cuerpo de los números reales $\mathbb{R}$.

Observación: Si F es una extensión de K y $f(x)$ es un polinomio en $K[x]$, entonces los coeficientes de $f(x)$ están todos en K y por lo tanto en F, luego $f(x)$ está en el anillo $F[x]$.

Definición 9.3.2 *Sea K un cuerpo, F una extensión de K y*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

un polinomio en $K[x]$. Entonces si $\lambda \in F$, **el valor del polinomio** *$f(x)$ en el elemento λ, denotado por $f(\lambda)$ es el elemento de F dado por*

$$f(b) = a_n \lambda^n + \cdots + a_1 \lambda + a_0$$

Proposición 9.3.1 *Sea K un cuerpo F una extensión de K, y $\lambda \in F$. Entonces la función*

$$\begin{array}{rcl} \phi_\lambda : K[x] & \longrightarrow & F \\ f(x) & \longrightarrow & f(\lambda) \end{array}$$

es un homomorfismo de anillos.

La imágen de $f(x)$ bajo ϕ_λ se llama **la sustitución** de x por λ, o la **evaluación de $f(x)$ en λ**.

Demostración: Sean $f(x)$ y $h(x)$ dos polinomios en $K[x]$, entonces

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

y

$$h(x) = b_m x^m + \cdots + b_1 x + b_0$$

luego

$$f(x) + h(x) = C_s x^s + \cdots + C_1 x + C_0$$

donde $C_i = a_i + b_i$, $0 \leq i \leq s$, $s \leq \max\{n, m\}$

Por lo tanto

$$\phi_\lambda(f(x) + h(x)) = C_s \lambda^s + \cdots + C_1 \lambda + C_0$$

y por otra parte

$$\begin{aligned}\phi_\lambda(f(x)) + \phi_\lambda(h(x)) &= (a_s\lambda^s + \cdots + a_1\lambda + a_0) + (b_s\lambda^s + \cdots + b_1\lambda + b_0) \\ &= (a_s + b_s)\lambda^s + \cdots + (a_1 + b_1)\lambda + (a_0 + b_0)\end{aligned}$$

de donde concluimos que

$$\phi_\lambda(f(x) + h(x)) = \phi_\lambda(f(x)) + \phi_\lambda(h(x))$$

Con respecto al producto, hagamos

$$f(x)h(x) = d_t x^t + \cdots + d_1 x + d_0,$$

donde $t = m + n$ y

$$d_i = \sum_{k+j=i} a_k b_j \quad , \quad 0 \leq i \leq t$$

Luego

$$\phi_\lambda(f(x)h(x)) = d_t\lambda^t + \cdots + d_1\lambda + d_0 \tag{9.3}$$

y por otro lado

$$\begin{aligned}\phi_\lambda(f(x))\phi_\lambda(h(x)) &= (a_n\lambda^n + \cdots + a_1\lambda + a_0)(b_m\lambda^m + \cdots + b_1\lambda + b_0) \\ &= e_t\lambda^t + \cdots + e_1\lambda + e_0 \qquad (9.4)\end{aligned}$$

con $t = n + m$ y

$$e_i = \sum_{k+j=i} a_k b_j \quad , \quad 0 \leq i \leq t$$

Comparando las expresiones (**??**) y (**??**), vemos que ellas son iguales y por lo tanto

$$\phi_\lambda(f(x)h(x)) = \phi_\lambda(f(x))\phi_\lambda(h(x))$$

Luego ϕ_λ es un homomorfismo de anillos.

♠

Definición 9.3.3 *Una* **raíz** *o un* **cero de un polinomio** $f(x) \in K[x]$ *es un elemento* λ *en una extensión* F *de* K*, tal que* $f(\lambda) = 0$*.*

También diremos que el valor de λ **anula** al polinomio, o que λ es una **solución de la ecuación** $f(x) = 0$

Ejemplo 1: Los valores 1 y -1 anulan al polinomio $f(x) = x^4 - 1$ en $\mathcal{Q}[x]$, pues $f(1) = 1^4 - 1 = 0 \quad$ y $\quad f(-1) = (-1)^4 - 1 = 0$.

Ejemplo 2: Sea $f(x) = x^2 + 1$ en $\mathcal{Q}[x]$. Entonces $i = \sqrt{-1}$ es una raíz de $f(x)$, pues $f(i) = i^2 + 1 = 0$. Nótese que i esta en $\mathbb{C}$ pero no en $\mathcal{Q}$.

Teorema 9.3.1 *Sea* $f(x)$ *un polinomio en* $K[x]$*,* F *una extensión de* K *y* $\lambda \in F$ *una raíz de* $f(x)$*. Entonces* $f(x)$ *se factoriza en* $F[x]$

$$f(x) = (x - \lambda)q(x)$$

donde $q(x)$ *es un polinomio de grado igual al grado de* $f(x)$ *menos uno.*

Demostración: Haciendo la división de $f(x)$ entre el polinomio $x - \lambda$ se generan polinomios $q(x)$ y $r(x)$ tales que

$$f(x) = (x - \lambda)q(x) + r(x) \tag{9.5}$$

con $r(x) = 0 \quad$ ó $\quad g(r(x)) < g(x - \lambda) = 1$

Luego el grado de $r(x)$ debe ser cero y por lo tanto es un polinomio constante $r(x) = \sigma$; con $\sigma \in K$.

Haciendo la evaluación de los polinomios en (**??**) en el valor λ, tenemos

$$\begin{aligned} 0 &= f(\lambda) \\ &= (\lambda - \lambda)q(\lambda) + \sigma \\ &= \sigma \end{aligned}$$

de donde $\sigma = 0$ y por lo tanto en (**??**) se tiene

$$f(x) = (x - \lambda)q(x)$$

♠

Un polinomio del tipo $ax + b$ se llama **polinomio lineal**. Es claro que todo polinomio lineal es irreducible, pues si $ax + b = p(x)q(x)$, entonces la suma de los grados de ellos debe ser 1. Por lo tanto $p(x)$ o $q(x)$ es de grado cero y por ende constante.

Definición 9.3.4 *Sea $f(x)$ un polinomio en $K[x]$. Diremos que $f(x)$ se* **factoriza completamente** *en una extensión F de K, si existen raíces $\lambda_1, \ldots, \lambda_t$ en F tal que*

$$f(x) = a_n(x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_t)$$

donde $a_n \in K$.

Observación: Una de las metas más importantes en la teoría de los polinomios es poder factorizar cualquier polinomio como un producto de factores lineales. Lamentablemente esto no es posible en cualquier cuerpo K, pues, por ejemplo $f(x) = x^2 + 1$ no se puede factorizar en $\mathcal{Q}[x]$ como producto de factores lineales.

Sin embargo siempre se puede hallar una extensión del cuerpo K en donde este problema se resuelve.

Definición 9.3.5 *Una raíz λ de $f(x)$ se dice que tiene* **multiplicidad K**, *si $f(x) = (x - \lambda)^k q(x)$ y λ no es raíz de $q(x)$.*

Cuando contamos las raíces de un polinomio, aquellas que aparecen repetidas se cuentan tantas veces como sea su multiplicidad. Así, por ejemplo el polinomio $f(x) = x^3 - x^2$ tiene 3 raíces que son 0, con multiplicidad 2, y 1.

Teorema 9.3.2 *Sea $f(x)$ un polinomio en $K[x]$ de grado n. Entonces $f(x)$ tiene a lo sumo n raíces en cualquier extensión F de K.*

Demostración: La demostración será por inducción sobre el grado de $f(x)$.

Si el grado de $f(x)$ es 0, entonces $f(x)$ es constante y no tiene raíces. Por lo tanto no hay nada que probar en este caso.

Si el grado de $f(x)$ es 1, entonces $f(x)$ es un polinomio lineal, digamos, $f(x) = ax + b$, para algunos a y b en K.

Si λ es una raíz de $f(x)$, entonces $f(x) = a\lambda + b = 0$ y por lo tanto $\lambda = -b/a$. Luego existe una única raíz.

Supongamos el teorema cierto para todo polinomio de grado menor que n. Sea $f(x)$ de grado n. Sea F una extensión de K. Si $f(x)$ no tiene ninguna raíz en F, entonces estará listo. Si $f(x)$ tiene una raíz λ en F de multiplicidad m, entonces $f(x) = (x - \lambda)^m q(x)$, donde $q(x)$ es un polinomio de grado $n - m$ que no tiene a λ como raíz.

Podemos entonces aplicar la hipótesis de inducción a $q(x)$ para concluir que no tiene más de $n - m$ raíces en F. Como toda raíz de $q(x)$ es una raíz de $f(x)$, se deduce entonces que $f(x)$ tiene a lo sumo $m + (n - m) = n$ raíces en F. Con esto queda probada la proposición para n.

♠

A continuación daremos un resultado muy importante sobre las raíces de un polinomio con coeficientes en los complejos. La demostración de este hecho requiere algunos conocimientos de la teoría de funciones analíticas los cuales pueden ser estudiados en un curso introductorio de un semestre.

Teorema 9.3.3 *(Teorema Fundamental del Algebra) Todo polinomio $f(x) \in \mathbb{C}[x]$ de grado n, posee exactamente n raíces en $\mathbb{C}$*

Demostración: Sea $f(x) \in \mathbb{C}[x]$. Será suficiente con probar que $f(x)$ tiene una raíz en $\mathbb{C}$ (¿Por qué?)

Si suponemos $f(z) \neq 0$ para todo z en $\mathbb{C}$, entonces la función

$$g(z) = \frac{1}{f(z)}$$

es una función entera (analítica en todo el plano complejo).

Nótese que g es una función acotada en todo $\mathbb{C}$, pues g es acotada en cualquier conjunto de la forma:

$$B_r = \{z \in \mathbb{C} \mid |z| \leq r\}$$

Además si hacemos $|z| = r$, se puede probar que g es acotado en todo el plano complejo, pues se tiene

$$\lim_{r \longrightarrow \infty} g(z) = \lim_{|z| \longrightarrow \infty} \frac{1}{f(z)} = 0$$

Podemos ahora invocar el teorema de Liouville de las funciones analíticas, el cual establece:

"Toda función entera acotada en $\mathbb{C}$, es constante".

Entonces se concluye que g es una función constante, lo cual es una contradicción. Por lo tanto $f(z_0) = 0$ para algún $z_0 \in \mathbb{C}$.

♠

Corolario 9.3.1 *Sea $f(x)$ un polinomio con coeficientes complejos de grado n. Entonces $f(x)$ se factoriza completamente*

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

donde $\alpha_i \in \mathbb{C}$ son las raíces de $f(x)$.

Ejercicios

1) Probar que los siguientes polinomios son irreducibles

a) $x^2 + x + 1$ en los enteros módulo 2.

b) $x^2 + x - 3$ en los enteros módulo 4.

c) $x^2 - x - 3$ en los enteros módulo 5.

d) $x^3 - 4$ en los enteros módulo 5.

e) $x^2 - 3$ en los enteros módulo 17.

f) $x^3 - 11$ en los enteros módulo 17.

2) Determine todos los polinomios irreducibles en $\mathbb{Z}_3[x]$.

3) Fórmula de interpolación de Lagrange.

Sea K un cuerpo, $n \geq 0$ y elementos $c_0, c_1, \ldots, c_n,\ b_0, b_1, \ldots, b_n$ en K. Entonces sea

$$f(x) = \sum_{i=0}^{n} b_i \prod_{k=0, k\neq i}^{n} (c_i - c_k)^{-1}(x - c_k)$$

Probar que

i) $f(c_i) = b_i$, para todo $0 \leq i \leq n$

ii) $f(x)$ es el único polinomio de grado n en $K[x]$ que satisface i).

4) Usando la fórmula anterior, determine un polinomio de grado 4, que satisfaga:

$$f(1) = 2, \quad f(2) = 3, \quad f(3) = 2, \quad \text{y} \quad f(4) = 3.$$

5) La Derivada de un polinomio. Si $f(x) \in K[x]$, entonces la derivada de $f(x)$, denotada por $f'(x)$, es el polinomio

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1$$

si

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

Probar las fórmula de derivación

i) $(f(x)+g(x))' = f'(x)+g'(x)$

ii) $(f(x)\cdot g(x))' = f'(x)g(x)+f(x)g'(x)$

6) Probar que un polinomio $f(x) \in K[x]$ tiene una raíz múltiple en alguna extensión de K, si y sólo si $f(x)$ y $f'(x)$ no son primos relativos.

7) Probar que si K es un cuerpo de característica 0, entonces $f'(x) = 0$ si y sólo si $f(x)$ es constante.

8) Solución de una ecuación cúbica. Sea

$$f(x) = x^3 + Ax^2 + Bx + C$$

un polinomio en $\mathcal{Q}[x]$.

i) Probar que el cambio de variable $x = t - \dfrac{a}{3}$ en el polinomio anterior nos da un polinomio de la forma

$$h(t) = x^3 + ax - b \tag{9.6}$$

con $a, b \in \mathcal{Q}$.

ii) En (**??**) haga el cambio de variables

$$x = s + t,$$

y entonces demuestre que:

$$s^3 + t^3 + 3st^2 + 3s^2t = b - a(s+t)$$

iii) Si hacemos $s^3 + t^3 = b$, probar que s^3 satisface la ecuación cuadrática

$$x^2 - bx - \left(\frac{a}{3}\right)^3 = 0 \tag{9.7}$$

iv) Calcule s y t y demuestre que la solución de la ecuación

$$x^3 + ax - b = 0$$

viene dada por

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{a}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{a} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}$$

9) Hallar las raíces del polinomio $f(x) = x^3 + 6x - 4$.

10) Sea D un Dominio de Integridad y $c_0, c_1, \ldots, c_n$ elementos en D. Probar que para cualquier conjunto de elementos $b_0, b_1, \ldots, b_n$ en D, existe un único polinomio $f(x)$ de grado a lo sumo $n+1$ tal que $f(c_i) = b_i$, $\leq i \leq n$.

9.4 Polinomios sobre $\mathcal{Q}$

En esta sección nos dedicaremos a estudiar la factorización de polinomios con coeficientes en el cuerpo de los números racionales $\mathcal{Q}$.

Sabemos que $\mathcal{Q}[x]$ es un Dominio de Factorización Unica y por lo tanto todo polinomio $f(x)$ en $\mathcal{Q}[x]$ se factoriza de manera única.

$$f(x) = p_1(x)p_2(x)\cdots p_s(x)$$

donde los $p_i(x)$ son irreducibles en $\mathcal{Q}[x]$.

Estudiaremos como determinar los $p_i(x)$ en la descomposición de arriba, usando el algoritmo de división. También daremos un criterio práctico para decidir si un polinomio es irreducible sobre $\mathcal{Q}[x]$.

Un hecho muy interesante, el cual será probado en el desarrollo de esta sección, es el siguiente: todo polinomio con coeficientes enteros que es irreducible en $\mathbb{Z}[x]$, también lo es en $\mathcal{Q}[x]$.

Proposición 9.4.1 *Sea $f(x)$ un polinomio de grado ≤ 3 en $\mathcal{Q}[x]$. Entonces si $f(x)$ es reducible en $\mathcal{Q}[x]$, existe $r \in Q$ tal que $f(r) = 0$.*

Demostración: Por ser $f(x)$ reducible, se tiene entonces $f(x) = h(x)g(x)$ para algunos polinomios $h(x)$ y $g(x)$ en $\mathcal{Q}[x]$ y además $h(x)$ y $g(x)$ no son constantes.

Luego se tiene

$$3 = grado(f(x)) = grado(h(x)) + grado(g(x))$$

Por lo tanto el grado de $h(x)$ o $g(x)$ debe ser igual a 1. Si suponemos que el grado de $h(x)$ es 1, entonces $h(x) = ax + b$ para $a, b \in \mathcal{Q}$, y luego

$$f(x) + (ax + b)g(x)$$

Si $b = 0$,entonces $r = 0$ es raíz de $f(x)$. Si $b \neq 0$, entonces $r = -\dfrac{a}{b}$ es raíz de $f(x)$. Con esto queda probado que $f(x)$ tiene una raíz en $\mathcal{Q}$.

♠

Definición 9.4.1 *Sea* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *un polinomio en* $\mathbb{Z}[x]$. *Se define* **el contenido** *de* $f(x)$ *como el Máximo Común Divisor de los coeficientes* $a_0, a_1, \ldots, a_n$.

Usaremos la notación $C(f)$ para el contenido de $f(x)$.

Ejemplo: Si $f(x) = 12x^3 - 6x^2 + 18x$ entonces, $C(f) = (12, 6, 18) = 6$.

Definición 9.4.2 *Sea* $f(x)$ *un polinomio con coeficientes enteros. Entonces se dice que* $f(x)$ **es primitivo**, *si* $C(f) = 1$.

Ejemplo: Sea $f(x) = 8x^5 - 13x + 4$. Luego $f(x)$ es primitivo.

Observación: Si $f(x)$ es un polinomio mónico con coeficientes en $\mathbb{Z}$, entonces $f(x)$ es primitivo.

Proposición 9.4.2 *Sean* $f(x)$ *y* $h(x)$ *polinomios primitivos en* $\mathbb{Z}[x]$, *entonces* $f(x)h(x)$ *es primitivo.*

Demostración: Supongamos que

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \quad \text{y} \quad h(x) = b_m x^m + \cdots + b_1 x + b_0$$

Entonces

$$f(x)h(x) = C_s x^s + \cdots + C_1 x + C_0$$

con $s = m + n$.

Supongamos por el absurdo que $f(x)h(x)$ no es primitivo. Entonces existe $d > 0$ tal que d divide a C_i para todo $0 \leq i \leq s$.

Como $f(x)$ es primitivo, d no puede dividir a todos los coeficientes de f. Sea a_k el primer coeficiente de f que no es divisible por d.

Similarmente, $h(x)$ es primitivo y supongamos que b_j es el primer coeficiente de $h(x)$ que no es divisible por d.

Luego $d|a_i,\ \ 0 \leq i \leq k$ y $d|b_i,\ \ 0 \leq i \leq j$ y

$$d \not| \ a_k b_j$$

Entonces el coeficiente C_{k+j} de $f(x)h(x)$ es de la forma

$$C_{k+j} = a_k b_j + (a_{k-1}b_{j+1} + \cdots + a_0 b_{j+k}) + (b_{j-1}a_{k+1} + \cdots + b_0 a_{j+k})$$

Tenemos entonces que

$$d|(a_{k-1}b_{j+1} + \cdots + a_0 b_{j+k})$$

y

$$d|(b_{j-1}a_{k+1} + \cdots + b_0 a_{j+k})$$

luego

$$d|C_{k+j} - a_k b_j$$

lo cual es una contradicción, pues $d|C_{k+j}$ y $d \not| \ a_k b_j$.

Por lo tanto $f(x)h(x)$ es primitivo.

♠

Proposición 9.4.3 *(Lema de Gauss) Sea $f(x)$ un polinomio primitivo en $\mathbb{Z}[x]$. Si $f(x) = p(x)q(x)$ con $p(x), q(x)$ en $\mathcal{Q}[x]$, entonces $f(x) = p_1(x)q_1(x)$, donde $p_1(x), q_1(x)$ son polinomios con coeficientes enteros. Además*

$$p_1(x) = \lambda p(x) \qquad \text{y} \qquad q_1(x) = \beta q(x),$$

con λ y β números racionales.

Demostración: Sea

$$\begin{aligned} p(x) &= r_s x^s + \cdots + r_1 x + r_0 \quad , \quad r_i \in \mathcal{Q} \\ q(x) &= t_l x^l + \cdots + t_1 x + t_0 \quad , \quad t_i \in \mathcal{Q} \end{aligned}$$

Sean m_1, m_2, el mínimo común multiplo de los denominadores de $p(x)$ y $q(x)$ respectivamente.

Luego $m_1 p(x)$ y $m_2 q(x)$ son polinomios con coeficientes enteros. Si hacemos

$$C_1 = C(p(x)) \quad \text{y} \quad C_2 = C(q(x))$$

Definimos entonces

$$p_1(x) = \frac{m_1}{C_1} p(x) \quad \text{y} \quad q_1(x) = \frac{m_2}{C_2} q(x)$$

luego $p_1(x)$ y $q_1(x)$ son polinomios primitivos, y además

$$\begin{aligned} f(x) &= p(x)q(x) \\ &= \frac{C_1 C_2}{m_1 m_2} p_1(x) q_1(x) \end{aligned}$$

o sea

$$m_1 m_2 f(x) = C_1 C_2 p_1(x) q_1(x)$$

Como $f(x)$ es mónico, el contenido del lado izquierdo es $m_1 m_2$ y por lo tanto $m_1 m_2 = C_1 C_2$. Luego

$$f(x) = p_1(x)q_1(x).$$

♠

Observación: Si en la proposición anterior el polinomio $f(x)$ es mónico, entonces tanto $p_1(x)$ como $q_1(x)$ resultan ser mónicos con coeficientes enteros.

El siguiente teorema da una condición necesaria para la existencia de raíces racionales en polinomios de coeficientes enteros.

Teorema 9.4.1 *Sea* $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *y* $r = \dfrac{s}{t}$ *un número racional. Entonces si* r *es raíz de* $f(x)$ *se debe tener*

$$s|a_0 \quad y \quad t|a_n$$

Demostración: Supongamos que $(s,t) = 1$. Luego

$$f(x) = \left(x - \frac{s}{t}\right) q(x), \quad \text{con} \quad q(x) \in \mathcal{Q}[x]$$

Usando el Lema de Gauss se obtiene

$$f(x) = (tx - s)q_1(x), \tag{9.8}$$

donde $q_1(x)$ tiene coeficientes enteros.

Comparando el coeficiente de grado n en ambos lados de (**??**) se tiene que $t|a_n$. Igualmente, comparando el término constante en ambos lados de (**??**) se sigue que $s|a_0$.

♠

Corolario 9.4.1 *Sea* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *un polinomio con coeficientes enteros. Entonces si* r *es una raíz entera de* $f(x)$*, se debe tener* $r|a_0$.

Ejemplo: Hallar las raíces racionales de

$$f(x) = 27x^3 - 8$$

Tenemos que las posibles raíces son de la forma $\frac{s}{t}$, donde $s|8$ y $t|27$. Luego los posibles valores de s son $\pm 1,\ \pm 2,\ \pm 4,\ \pm 8$; y los posibles valores de t son $\pm 1,\ \pm 3,\ \pm 9,\ \pm 27$. Después de probar todas las combinaciones posibles de s y t, el valor $s = 2$, $t = 3$ nos da una raíz. Luego dividimos el polinomio $f(x)$ entre $x - \frac{2}{3}$ para obtener

$$\begin{aligned} 27x^3 - 8 &= \left(x - \frac{2}{3}\right)(27x^2 + 18x + 12) \\ &= 3\left(x - \frac{2}{3}\right)(9x^2 + 6x + 4) \end{aligned}$$

Las raíces de $9x^2 + 6x + 4$ son complejas y por lo tanto $f(x)$ tiene una sola raíz racional.

Veamos ahora un criterio muy simple para decidir si un polinomio con coeficientes enteros es irreducible.

Teorema 9.4.2 *Sea $f(x)$ un polinomio en $\mathbb{Z}[x]$. Si para algún entero m, se tiene que $f(x)$ es irreducible en $\mathbb{Z}_m[x]$, entonces $f(x)$ es irreducible en $\mathbb{Z}[x]$.*

Demostración: Si $f(x) = a_n x^n + \cdots + a_1 x + a_0$ entonces la imágen de $f(x)$ en $\mathbb{Z}_m[x]$ es el polinomio

$$\overline{f}(x) = \overline{a_n} x^n + \cdots + \overline{a_1} x + \overline{a_0}$$

donde $\overline{a_i}$ es la imágen de a_i bajo la proyección

$$\prod_m : \mathbb{Z} \longrightarrow \mathbb{Z}_m$$

Si $f(x)$ es reducible en $\mathbb{Z}[x]$, entonces

$$f(x) = h(x)q(x)$$

y por lo tanto

$$\overline{f}(x) = \overline{h}(x)\overline{q}(x)$$

luego $\overline{f}(x)$ es reducible en $\mathbb{Z}_m[x]$.

♠

Ejemplo: Sea $f(x)$ $x^3 + x - 3$. Entonces $f(x)$ es irreducible en $\mathbb{Z}_4$ (Verificarlo!), luego $f(x)$ es irreducible en $\mathbb{Z}$.

Teorema 9.4.3 *(Criterio de Eisenstein) Sea* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *un polinomio con coeficientes enteros. Sea* p *un número primo, tal que*

i) $p | a_i \qquad 0 \leq i < n$

ii) $p \nmid a_n$

ii) $p^2 \nmid a_0$

Entonces $f(x)$ *es irreducible en* $\mathcal{Q}[x]$.

Demostración: Dividimos la prueba en dos casos

Caso I: si $f(x)$ es primitivo y es reducible en $\mathcal{Q}[x]$ entonces por el lema de Gauss, se tiene

$$f(x) = h(x)q(x) \tag{9.9}$$

con $h(x), q(x)$ en $\mathbb{Z}[x]$.

Sea

$$h(x) = b_s x^s + \cdots + b_1 x + b_0,$$

y

$$q(x) = C_t x^t + \cdots + C_1 x + C_0$$

Comparando los coeficientes de grado 0, en (**??**) tenemos que

$$a_0 = b_0 C_0$$

Ahora bien, como $p|a_0$ y $p^2 \not| \, a_0$, se tiene que $p|b_0 C_0$, pero no puede dividir a ambos.

Luego, supongamos que $p|b_0$ y $p \not| \, C_0$.

Si $p|b_i$ para todos los i, entonces $p|a_i$ para todos los i, y por lo tanto $f(x)$ no es primitivo.

Supongamos que $p|b_i$ para $o \leq i < k < s$ y $p \not| \, b_k$, luego se tiene

$$a_k = b_k C_0 + b_{k-1} C_1 + \cdots + b_0 C_k$$

y por hipótesis $p|a_k$. Entonces

$$p| \, [a_k - (b_{k-1} C_1 + \cdots + b_0 C_k)]$$

lo cual es una contradicción, pues $p \not| \, b_k C_0$.

Por lo tanto $f(x)$ no es reducible en $\mathcal{Q}[x]$.

Caso II: Si $f(x)$ no es mónico, hacemos

$$f(x) = d f_1(x),$$

donde $f_1(x)$ es primitivo con coeficientes enteros. Luego los coeficientes de $f_1(x)$ satisfacen las hipótesis $i)$ $ii)$ $iii)$ del teorema, pues $p \not| \, a_n$ y por lo tanto $p \not| \, d$.

♠

Ejercicios

1) Factorizar completamente en el cuerpo de los números complejos los polinomios

a) $x^4 - 3x^3 - 4x^2 - 6x + 4$

b) $x^3 - 9x^2 + 20x - 12$

c) $x^4 - 8x^2 + 16$

d) $x^5 + 2x^4 + x^3 - 8x^2 - 16x - 8$

e) $x^5 - 3x^4 + 2x^3 - 2x^2 + 6x - 4$

f) $x^6 - 4x^5 - 12x^4 - x^2 + 4x + 12$

2) Si p es un número primo y n es un entero $n \geq 2$, probar que $f(x) = x^n - p$ es irreducible sobre los racionales.

3) Sea p un número primo. Entonces el **polinomio ciclotómico de orden** p se define por

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

Demuestre que $f(x)$ es irreducible sobre los racionales.

4) Sea $w = e^{2\pi i/p}$ la raíz p-ésima de la unidad en los números complejos.

Demuestre que el polinomio $f(x)$ del problema anterior se factoriza en $\mathcal{C}[x]$

$$f(x) = (x - w)(x - w^2) \cdots (x - w^{p-1})$$

5) Si a y b son dos números enteros, demostrar que

$$a^p + b^p = (a + b)(a + bw)(a + bw^2) \cdots (a + bw^{p-1})$$

donde $w = e^{2\pi i/p}$

6) Sean a y c enteros positivos, con $a > 0$ y $c > 0$. Probar que el polinomio $f(x) = x^3 + ax^2 + c$ no tiene raíces reales en el intervalo $[-a, +\infty]$.

7) Demuestre que $\mathbb{Z}_m[x]$ es un anillo finito para todo $m > 1$.

8) Factorizar en $\mathbb{Z}_5[x]$ los polinomios

a) $x^2 + 3x - 1$

b) $x^3 + 3$

c) $x^4 + x^3 + 2x$

d) $x^2 - 6x + 3$

9) Sea p un número primo. Hallar la factorización del polinomio $x^p - x$ en $\mathbb{Z}_p[x]$.

10) Usando el ejercicio 9, probar la congruencia

$$(p-1)! \equiv -1 \ mod \ p$$

11) Hallar todas las raíces de $f(x) = x^2 - x$ en $\mathbb{Z}_6$.

12) Determine los valores de s para los cuales $f(x) = x^4 + x + s$ es irreducible en $\mathbb{Z}_5$.

13) Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0$ un polinomio en $\mathbb{C}[x]$. El **polinomio conjugado** de $f(x)$, se define por

$$\overline{f}(x) = \overline{a}_n x^n + \cdots + \overline{a}_1 x + \overline{a}_0,$$

donde $\overline{a}i$ es el conjugado del número complejo a_i. Probar que $r \in \mathbb{C}$ es raíz de $f(x)$ si y sólo si $\overline{r}$ es raíz de $\overline{f}(x)$.

14) Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0$ un polinomio en $\mathbb{R}[x]$. Demostrar que si $f(x)$ tiene una raíz $r \in \mathbb{C}$, entonces $\overline{r}$ también es raíz de $f(x)$.

15) Halle un ejemplo de un anillo A, tal que el polinomio $f(x) = x^2 + a$ posea infinitas raíces.

9.5 Polinomios en Varias Variables

En el estudio de las curvas y superficies en el plano y el espacio, nos encontramos frecuentemente con ecuaciones con más de una variable.

Por ejemplo la circunferencia de radio 1 con centro en el origen se expresa analíticamente mediante la ecuación:

$$x^2 + y^2 - 1 = 0 \tag{9.10}$$

Es posible entonces, usar más de una variable para los polinomios y definir el polinomio en dos variables:

$$F(x, y) = x^2 + y^2 - 1$$

Entonces la ecuación (**??**) se expresa

$$F(x, y) = 0 \tag{9.11}$$

En esta sección se dara una definición formal del anillo de polinomios en varias variables, así como alguna de sus propiedades más importantes.

Si A es un anillo, entonces $A[x]$, es otro anillo y tiene significado la siguiente definición

Definición 9.5.1 *Sea A un anillo y x_1, x_2 indeterminadas. Entonces el* **anillo de polinomios en** *x_1, x_2, denotado por $A[x_1, x_2]$ es igual al anillo $(A[x_1])[x_2]$.*

Entonces un polinomio $f(x_1, x_2)$ en $A[x_1, x_2]$ es una expresión de la forma

$$f(x_1, x_2) = f_n(x_1)x_2^n + f_{n-1}(x_1)x_2^{n-1} + \cdots + f_1(x_1)x_2 + f_0(x_1)$$

donde $f_i \in A[x_1]$.

Luego $f(x_1, x_2)$ se expresa como una combinación de las incógnitas x_1 y x_2 de la forma

$$f(x_1, x_2) = \sum_{j=0}^{\infty} \sum_{i=0}^{\infty} a_{ij} x_1^i x_2^j$$

donde $a_{ij} = 0$ para casi todos los i, j.

Ejemplo: Sea $A = \mathbb{Z}$ y $f(x_1, x_2)$ el polinomio en $\mathbb{Z}[x_1, x_2]$, definido por

$$f(x_1, x_2) = x_1^2 + 3x_1x_2 + x_2^2$$

Entonces $a_{21} = 1$, $a_{12} = 1$, $a_{11} = 3$ y $a_{ij} = 0$ para los restantes subindices.

Podemos definir el anillo de polinomios de n variables $x_1, \ldots, x_n$ sobre A, en forma recursiva haciendo

$$A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n]$$

Entonces $A[x_1, \ldots, x_n]$ satisface todas las propiedades de anillo.

Definición 9.5.2 *Un elemento del anillo $A[x_1, \ldots, x_n]$ de la forma*

$$u = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \quad \alpha_i \geq 0$$

se llama **un monomio**

Podemos considerar la n-upla $\alpha = (\alpha_1, \ldots, \alpha_n)$ en

$$T = S \times \cdots \times S = S^n$$

donde $S = \mathbb{N} \cup \{0\}$. Luego usamos la notación para el monomio n,

$$u = X^\alpha$$

donde $X = (x_1, \cdots, x_n)$

Consideremos aquellas funciones

$$\phi : T \longrightarrow A$$

tales que $\phi(\alpha) = 0$ para todo α, excepto para un número finito. Con estas herramientas a la mano, se tiene la siguiente

Definición 9.5.3 *Sea A un anillo, un polinomio f en $A[x_1, \cdots, x_n]$ es una combinación lineal de monomios*

$$f(X) = \sum_{\alpha \in T} \phi(\alpha) X^{\alpha} \tag{9.12}$$

Ejemplo: El polinomio en $\mathbb{Z}[x_1, x_2, x_3]$, dado por

$$f(x_1, x_2, x_3) = 2x_1^3 + x_1 x_2^2 + x_1 x_2 - 6x_1 x_2 x_3.$$

Entonces $f(x_1, x_2, x_3)$ se expresa en la forma (**??**) tomando la función $\phi : S^3 \longrightarrow \mathbb{Z}$ de la forma siguiente

$\phi(3,0,0) = 2$
$\phi(1,2,0) = 1$
$\phi(1,1,0) = 1$
$\phi(1,1,1) = -6$
$\phi(\alpha) = 0$,
para α diferente de $(3,0,0)$, $(1,2,0)$, $(1,1,0)$ y $(1,1,1)$

Teorema 9.5.1 *Si A es un Dominio de Integridad, entonces el anillo de polinomios en n variables $A[x_1, \cdots, x_n]$ es un Dominio de Integridad.*

Demostración: Hemos probado en la proposición **??** que $A[x_1]$ es un Dominio de Integridad, entonces se demuestra que $A[x_1][x_2]$ es también Dominio de Integridad y podemos entonces continuar en forma recursiva, para concluir que $A[x_1, \cdots, x_n]$ es un Dominio de Integridad.

♠

Definición 9.5.4 *Si A es un Dominio de Integridad, entonces el cuerpo de fracciones de $A[x_1, \cdots, x_n]$, se llama* **cuerpo de funciones racionales** *en $x_1, \cdots, x_n$.*

Los elementos de este cuerpo son funciones en las n variables $x_1, \cdots, x_n$, del tipo

$$f(x_1, \ldots, x_n) = \frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)}$$

donde p y q son polinomios en $A[x_1, \ldots, x_n]$.

El objetivo más importante de esta sección será probar que si A es un Dominio de Factorización Unica entonces el anillo de polinomios $A[x_1, \ldots, x_n]$ es un Dominio de Factorización Unica.

Si A es un Dominio de Factorización Unica y $f(x) = a_n x^n + \cdots + a_1 x + a_0$ es un polinomio en $A[x]$, entonces su **contenido**, denotado por $C(f)$, es el máximo común divisor de los coeficientes $a_n, a_{n-1}, \ldots, a_0$. Si $C(f) = 1$, entonces diremos que el polinomio $f(x)$ es **primitivo**.

Proposición 9.5.1 *Sea A un Dominio de Factorización Unica y $f(x) \in A[x]$ un polinomio no constante. Entonces existe un único elemento c en A, salvo unidades, tales que*

$$f(x) = c.h(x)$$

con $h(x)$ primitivo.

El elemento c es el contenido de $f(x)$.

Demostración: Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Como A es un Dominio de Factorización única, cada elemento a_i se expresa de manera única como un producto de irreducibles, salvo asociados.

Luego $C(f) = (a_n, a_{n-1}, \ldots, a_1, a_0)$ es un elemento de A. Como $C(f)$ divide a a_i, para todo i, $0 \leq i \leq n$, se tiene

$$a_i = C(f)b_i, \qquad 0 \leq i \leq n$$

para algunos elementos $b_i \in A$.

Además se tiene que $(b_n, b_{n-1}, \ldots, b_1, b_0) = u$, donde u es una unidad, pues si hay algún factor común de $b_n, \ldots, b_0$, digamos d, se tiene que $d.C(f)$ es un divisor común de los a_i, y por lo tanto $d.C(f)$ divide a $C(f)$

Luego

$$C(f) = d.C(f).t$$

para algún $t \in A$, lo cual implica que d es una unidad. Esta unidad u, se puede factorizar y entonces definimos el polinomio

$$h(x) = b'_n x^n + b'_{n-1} x^{n-1} + \cdots + b'_1 x + b'_0$$

donde $b'_i u = b_i$, para $0 \leq i \leq n$.

Entonces $h(x)$ es un polinomio primitivo y se tiene

$$f(x) = C(f).u.h(x)$$

Si c' es otro elemento de A, y $h'(x)$ es un polinomio primitivo, tal que

$$f(x) = c'.h'(x)$$

Haremos entonces

$$C(f).uh(x) = c'.h'(x) \tag{9.13}$$

Tomando el contenido en ambos lados, se concluye que

$$C(f).u = c'$$

Luego $C(f)$ es único salvo unidades. Como $A[x]$ es un Dominio de Integridad, podemos cancelar c' en ambos lados de (**??**) para obtener

$$h(x) = h'(x)$$

♠

A continuación daremos sin demostración un resultado previo al Lema de Gauss para polinomios en $A[x]$, el cual fue estudiado en la sección anterior. La demostración es exactamente igual a la demostración dada para polinomios en $\mathbb{Z}[x]$

Proposición 9.5.2 *Si A es un Dominio de Factorización Unica, entonces el producto de dos polinomios primitivos es primitivo.*

Este resultado se generaliza fácilmente a n polinomios.

Corolario 9.5.1 *Sea A un Dominio de Factorización Unica. Si los polinomios $p_1(x), p_2(x), \ldots, p_s(x)$ son primitivos en $A[x]$, entonces el producto $p_1(x)p_2(x)\ldots p_s(x)$ es también primitivo en $A[x]$.*

Corolario 9.5.2 *Sea A un Dominio de Factorización Unica y K su cuerpo de fracciones. Entonces n $f(x)$ es un polinomio irreducible y primitivo en $A[x]$, se tiene que $f(x)$ es irreducible en $K[x]$*

Demostración: Si suponemos que $f(x)$ es reducible en $K[x]$ se tendrá

$$f(x) = p_1(x)p_2(x)$$

con $p_1(x)$, $p_2(x)$ en $K[x]$. Podemos sacar factor común de los denominadores en $p_1(x)$ y $p_2(x)$, para obtener

$$f(x) = \frac{c}{d}p_1'(x)p_2'(x)$$

donde c y d están en A y $p_1'(x), p_2'(x)$ son polinomios primitivos en $A[x]$. Luego el producto $p_1'(x).p_2'(x)$ es primitivo y por la proposición (**??**), se concluye que

$$c = d.u,$$

donde u es una unidad en A. Luego tendremos

$$f(x) = up_1'(x)p_2(x)$$

lo cual es una contradicción, pues $f(x)$ es irreducible en $A[x]$

♠

Teorema 9.5.2 *Si A es un Dominio de Factorización Unica, entonces $A[x]$ es un Dominio de Factorización Unica.*

Demostración: Sea $f(x)$ un polinomio en $A[x]$ no constante, si $f(x)$ es irreducible estará listo. Si $f(x)$ es reducible, existen polinomios $f_1(x)$ y $f_2(x)$, con $g(f_1(x)) < g(f(x))$ y $g(f_2(x)) < g(f(x))$, tales que

$$f(x) = f_1(x)f_2(x)$$

Si aplicamos inducción sobre el grado de $f(x)$, se deduce entonces que los polinomios $f_1(x)$ y $f_2(x)$ se expresa como un producto de irreducibles. Luego $f(x)$ es un producto de polinomios irreducibles en $A[x]$.

Unicidad: Supongamos que $f(x)$ tenga dos descomposiciones como producto de polinomios irreducibles en $A[x]$

$$p'_1(x)\cdots p'_s(x) = q'_1(x)\cdots q'_t(x) \tag{9.14}$$

Para cada i, j hacemos $p'_i(x) = d_i p_i(x)$, $q'_j = c_j q_j(x)$ donde d_i, c_j están en A y los polinomios $p_i(x)$ y $q_j(x)$ son primitivos. Luego tendremos

$$d_1\cdots d_s p_1(x)\cdots p_s(x) = c_1\cdots c_t q_1(x)\cdots q_t(x) \tag{9.15}$$

Como cada $p_i(x)$ es primitivo, entonces el producto de todos ellos es primitivo. De igual manera se concluye que el producto de todos los $q_j(x)$ es primitivo. Luego, por la proposición (**??**), se concluye que

$$ud_1\cdots d_s = c_1\cdots c_t,$$

donde u es una unidad en A.

Luego podemos hacer cancelación en (**??**) para obtener

$$p_1(x)\cdots p_s(x) = uq_1(x)\cdots q_t(x) \tag{9.16}$$

Ahora bien, si K es el cuerpo de fracciones de A, los polinomios $p_i(x)$, $q_j(x)$ están en $K[x]$, y además son irreducibles y primitivos, luego son irreducibles en $K[x]$.

Entonces aplicando el teorema de la factorización única para polinomios en $K[x]$, concluimos $s = t$ y

$$p_i(x) = c_i q_j(x) \qquad 1 \leq i \leq n$$

para algún $l_i \in K$.

Usando el hecho de que p_i y q_j son polinomios primitivos en $A[x]$, se concluye

$$p_i(x) = u_i q_j(x), \qquad 1 \leq i \leq 1$$

donde u_i es una unidad en A.

♠

Corolario 9.5.3 *Si A es un Dominio de Factorización Unica, entonces $A[x_1, \ldots, x_n]$ es un Dominio de Factorización Unica.*

Ejemplo: Sea $\mathbb{R}$ el anillo $\mathbb{Z}[x, y]$. Como $\mathbb{Z}$ es un Dominio de Factorización Unica, se tiene que $\mathbb{R}$ lo es también. Sin embargo este anillo no es un dominio de ideales principales, pues el ideal $I = (x, y)$ no es principal.

Ejercicios

1) Probar que $A[x, y] = A[y, x]$

2) Demuestre que $f(x) = x^2 + y^2 - 1$ es irreducible sobre el cuerpo de los racionales. ¿Será reducible sobre los complejos?

3) Sean $f(x, y) = 3x^2y^5 + 6y^2x - 12xy$, y $g(x, y) = 3x^2y^2 - xy^2 + 2x^2y$, polinomios en $\mathbb{Z}[x, y]$. Expresar estos polinomios en la forma de la definición (**??**)

$$f(X) = \sum_{\alpha \in T} \phi(\alpha) X^{\alpha}$$

Usando esta forma, ejecute las operaciones

a) $f(x, y)g(x, y)$

b) $g(x, y)f(x, y)$

4) Hallar una fórmula para el producto y la suma de dos polinomios de n variables.

5) Demuestre que el producto de polinomios es conmutativo.