Capítulo 6

Anillo de Polinomios.

Una forma de definir los polinomios en forma intuitiva es la siguiente:

Sea $(\mathbb{K}, +, \cdot)$ un cuerpo, entonces un polinomio con coeficiente en $\mathbb{K}$ es de la siguiente forma

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0$$

donde $n \in \mathbb{N}$, $a_n, a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ son los coeficientes del polinomio, elementos de $\mathbb{K}$

Se dice que el grado de $p(x)$ es n si y sólo si $a_n \neq 0$, y se denota por $\text{gr}(p(x)) = n$

Se denota el conjunto de los polinomios con coeficiente en $\mathbb{K}$ del siguiente modo

$$\mathbb{K}[x] := \{p(x) \mid a_i \in \mathbb{K} \text{ y } n \in \mathbb{N}\}$$

Sean $p(x), q(x) \in \mathbb{K}[x]$, se dice que los polinomios son iguales o $p(x) = q(x)$ si y sólo si son iguales coeficiente a coeficiente.

Definición 56 *Sea $F(\mathbb{N}, \mathbb{K})$ el conjunto de la funciones de $\mathbb{N}$ en $\mathbb{K}$, entonces el conjunto de los polinomios con coeficiente en $\mathbb{K}$ en la variable x es*

$$\mathbb{K}[x] := \{\ p \in F(\mathbb{N}, \mathbb{K}) \mid p^{-1}(\mathbb{K}^*) \quad \textit{es finito}\ \}$$

Además si $p \in \mathbb{K}[x]$ no nulo, entonces se define el grado

$$\text{gr}(p) = \text{máx}(p^{-1}(\mathbb{K}^*)).$$

Notación: Sea $p \in \mathbb{K}[x]$, y $\text{gr}(p) = n$ entonces

$$p(x) = p_0 + p_1 x^1 + \cdots + p_{n-1}x^{n-1} + p_n x^n = \sum_{i=0}^{n} p_i x^i$$

La igual de polinomio corresponde a una igual de funciones

6.1. Estructura Anillo.

Adición: Sean $p(x), q(x) \in \mathbb{K}[x]$, entonces la suma es la suma funcional, es decir,

$$\begin{array}{rccc} p+q & : & \mathbb{N} & \to & \mathbb{K} \\ & & i & \rightsquigarrow & p_i + q_i \end{array}$$

luego se tiene para que el valor $p_i + q_i$ es distinta de cero, al menos un de ello debe ser distinto de cero. Por lo tanto

$$\mathrm{gr}(p+q) \leq \mathrm{máx}\{\mathrm{gr}(p), \mathrm{gr}(q)\}$$

Con la notación intuitiva, tenemos que esta definición se transforma del siguientes modo: Sean $p(x) = a_n x^n + \cdots + a_0$ y $q(x) = b_m x^m + \cdots + b_0$ para ello consideraremos 3 casos

(i) Si $\mathrm{gr}(p(x)) > \mathrm{gr}(q(x))$ entonces $n > m$ por lo tanto

$$\begin{aligned} p(x) + q(x) &= (a_n x^n + \cdots + a_0) + (b_m x^m + \cdots + b_0) \\ &= (a_n x^n + \cdots + a_m x^m + \cdots + a_0) + (b_m x^m + \cdots + b_0) \\ &= a_n x^n + \cdots + (a_m + b_m) x^m + (a_0 + b_0). \end{aligned}$$

(ii) Si $\mathrm{gr}(p(x)) = \mathrm{gr}(q(x))$ entonces $n = m$ por lo tanto

$$\begin{aligned} p(x) + q(x) &= (a_n x^n + \cdots + a_0) + (b_m x^m + \cdots + b_0) \\ &= (a_n x^n + \cdots + a_0) + (b_n x^n + \cdots + b_0) \\ &= (a_n + b_n) x^n + \cdots + (a_0 + b_0). \end{aligned}$$

(iii) Si $\mathrm{gr}(p(x)) < (q(x))$ entonces $n < m$ por lo tanto

$$\begin{aligned} p(x) + q(x) &= (a_n x^n + \cdots + a_0) + (b_m x^m + \cdots + b_0) \\ &= (a_n x^n + \cdots + a_0) + (b_m x^m + \cdots + b_n x^n + \cdots + b_0) \\ &= b_m x^m + \cdots + (a_n + b_n) x^n + (a_0 + b_0). \end{aligned}$$

6.1.1. Suma en $\mathbb{K}[x]$

Propiedad 163 *Sea $\mathbb{K}[x]$ el anillo de polinomios se cumple*

$$(\mathbb{K}[x], +) \quad \textit{forman un grupo abeliano.}$$

Demostración: Sean $p(x), q(x), r(x) \in \mathbb{K}[x]$,
Asociativa:

$$p(x) + [q(x) + r(x)] = [p(x) + q(x)] + r(x)$$

Luego

$$\begin{aligned} (p + (q + r))_i &= p_i + (q + r)_i \\ &= p_i + (q_i + r_i) \\ &= (p_i + q_i) + r_i \\ &= (p + q)_i + r_i \\ &= ((p + q) + r)_i \end{aligned}$$

Neutro Aditivo: existe $0(x) \in \mathbb{K}[x]$ función nula

$$p(x) + 0(x) = p(x)$$

Para ello

$$\begin{aligned}(p+0)_i &= p_i + 0_i \\ &= p_i + 0 \\ &= p_i\end{aligned}$$

Observación: Notemos que $0(x) = 0x^m + \cdots + 0 = 0x^n + \cdots + 0$.
Inverso Aditivo: Sea $p(x) \in \mathbb{K}[x]$, existe

$$\begin{array}{rccc} -p & : & \mathbb{N} & \to & \mathbb{K} \\ & & i & \rightsquigarrow & -p_i \end{array}$$

tal que

$$p(x) + (-p(x)) = 0(x)$$

Para ello

$$\begin{aligned}(p+(-p))_i &= p_i + (-p_i) \\ &= 0 \\ &= 0_i\end{aligned}$$

Observación: Notemos que $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{K}[x]$, entonces $-p(x) = -a_n x^n - a_{n-1}x^{n-1} \cdots - a_0$.
Conmutatividad: Debemos probar

$$p(x) + q(x) = q(x) + p(x)$$

Para ello

$$\begin{aligned}(p+q)_i &= p_i + q_i \\ &= q_i + p_i \\ &= (q+p)_i\end{aligned}$$

6.1.2. Multiplicación en $\mathbb{K}[x]$

Multiplicación: Consideremos $p(x), q(x) \in \mathbb{K}[x]$, entonces la multiplicación es dada por

$$\begin{array}{rccc} p \cdot q & : & \mathbb{N} & \to & \mathbb{K} \\ & & i & \rightsquigarrow & \sum_{k=0}^{i} p_{k-i} q_k \end{array}$$

note que el valor $\sum_{k=0}^{i} p_{k-i}q_k$ es cero, si el $i > n + m$ y $\sum_{k=0}^{n+m} p_{k-i}q_k = p_n q_m$, cuando $n = \text{gr(p(x))}$ y $m = \text{gr(q(x))}$. Por lo tanto

$$\text{gr}(p \cdot q) \leq \text{gr}(p) + \text{gr}(q)$$

Con la notación intuitiva, tenemos que esta definición se transforma del siguientes modo: Sean

$$p(x) = a_n x^n + \cdots + a_0 \quad \text{y} \quad q(x) = b_m x^m + \cdots + b_0$$

tenemos

$$\begin{aligned} p(x) \cdot q(x) &= (a_n x^n + \cdots + a_0)(b_m x^m + \cdots + b_0) \\ &= a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \cdots + (a_1 b_o + a_0 b_1) x + a_0 b_0. \end{aligned}$$

Propiedad 164 $(\mathbb{K}[x], +, \cdot)$ *es un anillo conmutativo.*

Demostración: Sean $p(x), q(x), r(x) \in \mathbb{K}[x]$,
Asociativa:

$$p(x) \cdot [q(x) \cdot r(x)] = [p(x) \cdot q(x)] \cdot r(x)$$

Neutro:

$$p(x) \cdot 1 = p(x)$$

Conmutatividad:

$$p(x) \cdot q(x) = q(x) \cdot p(x)$$

Distributividad:

$$p(x) \cdot [q(x) + r(x)] = [p(x) \cdot q(x)] + [p(x) \cdot r(x)]$$

Definición 57 *Sean $p(x), q(x) \in \mathbb{K}[x]$, se dice que $p(x)$ divide a $q(x)$ si y sólo si existe $r(x) \in \mathbb{K}[x]$ tal que*

$$q(x) = p(x) \cdot r(x).$$

La notación es similar:

$$p(x) \text{ divide a } q(x), \text{ lo denotamos por } p(x) | q(x).$$

Definición 58 *Las unidades de $\mathbb{K}[x]$, corresponde a lo elementos que tiene inverso multiplicativos, es decir,*

$$p(x) \in \mathcal{U}(\mathbb{K}[x]) \quad \Leftrightarrow \quad (\exists\ q(x) \in \mathbb{K}[x])(\ p(x)q(x) = 1\ )$$

Propiedad 165 *Sea $\mathbb{K}$ un cuerpo entonces*

$$\mathcal{U}(\mathbb{K}[x]) = \mathbb{K}^*.$$

6.2. Algoritmo de la División en $\mathbb{K}[x]$.

Sean $\mathbb{K}$ un cuerpo y $p(x), q(x) \in \mathbb{K}[x]$ tal que $q(x)$ no nulo, entonces existe $r(x), s(x) \in \mathbb{K}[x]$ tal que

$$p(x) = q(x) \cdot s(x) + r(x) \qquad \text{gr}(r(x)) < \text{gr}(q(x)) \text{ o } r(x) = 0.$$

Demostración: Tomemos el conjunto de los polinomios de la siguiente forma

$$\mathcal{H} := \{p(x) - q(x) \cdot a(x) \mid a(x) \in \mathbb{K}[x]\}$$

Si consideramos $r(x)$ como el polinomio de menor grado o $r(x) = 0$, que pertenece a $\mathcal{H}$ tenemos

$$\begin{aligned} r(x) &= p(x) - q(x) \cdot s(x) \\ p(x) &= q(x) \cdot s(x) + r(x) \end{aligned}$$

Supongamos que $r(x) \neq 0$ y $\text{gr}(r(x)) \geq \text{gr}(q(x))$, con

$$r(x) = a_n x^n + \cdots + a_0, \quad q(x) = b_m x^m + \cdots + b_0$$

luego

$$r_1(x) = r(x) - \frac{a_n}{b_m} x^{n-m} q(x) \in \mathbb{K}[x]$$

Tiene grado menor y pertenece a $\mathcal{H}$. □

Notación: En el algoritmo de la división el polinomio $s(x)$ se llama cuociente y $r(x)$ el resto.

6.3. División Sintética.

Ejemplo 124 *Determinar el resto y el cuociente al dividir* $p(x) = x^4 + 6x^3 + 7x^2 - 6x - 8 \in \mathbb{R}[x]$ *por* $x + 1$

$$\begin{array}{rrrrrl} x^4 & +6x^3 & +7x^2 & -6x & -8 & : x+1 \quad = x^3 + 5x^2 + 2x - 8 \\ \cline{1-1} -x^4 & -x^3 & & & & \\ \cline{2-5} & 5x^3 & +7x^2 & -6x & -8 & \\ & -5x^3 & -5x^2 & & & \\ \cline{3-5} & & 2x^2 & -6x & -8 & \\ & & -2x^2 & -2x & & \\ \cline{4-5} & & & -8x & -8 & \\ & & & 8x & +8 & \\ \cline{5-5} & & & & 0 & \end{array}$$

Luego tenemos

$$x^4 + 6x^3 + 7x^2 - 6x - 8 = (x+1)(x^3 + 5x^2 + 2x - 8) + (0)$$

El proceso anterior, lo podemos resumir de la siguiente manera

-1	1	6	7	-6	-8
		-1	-5	-2	8
	1	5	2	-8	0

El proceso de la división sintética es un regla, que permite resumir la división de polinomios para un caso particular.

Para ello supongamos que deseamos dividir $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ deseamos dividir por $x - \alpha$.

Lo cual lo denotamos por:

α	a_n	a_{n-1}		a_1	a_0
		αb_{n-1}		αb_1	αb_0
	a_n	$a_{n-1} + \alpha a_n$		$a_1 + \alpha b_1$	$a_0 + \alpha b_0$
	b_{n-1}	b_{n-2}	$\cdots$	b_0	c_0

y obtenemos el siguiente resultado

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - \alpha)(b_{n-1}x^{n-1} + \cdots + b_1 x + b_0) + c_0.$$

6.4. Máximo Común Divisor

Definición 59 *Sean $a(x), b(x) \in \mathbb{K}[x]$. Se dice que $d(x) = MCD(a(x), b(x)) \in \mathbb{K}[x]$ si y sólo si*

1. *$d(x)|a(x) \ \wedge \ d(x)|b(x)$*
2. *Si $h(x)|a(x) \ \wedge \ h(x)|b(x)$ entonces $h(x)|d(x)$*

Observación: si $d(x)$ es un máximo común divisor de $a(x), b(x)$ y $\alpha \in \mathbb{K}^*$ entonces $\alpha d(x)$ también es máximo común divisor de $a(x), b(x)$

Teorema 166 *Sean $a(x), b(x) \in \mathbb{K}[x]$. Si $d(x) = MCD(a(x), b(x)) \in \mathbb{K}[x]$ entonces existe $p(x), q(x) \in \mathbb{K}[x]$ tal que*

$$d(x) = a(x)p(x) + b(x)q(x)$$

Demostración: Sea $\mathcal{A} = \{a(x)p(x) + b(x)q(x) \mid p(x), q(x) \in \mathbb{K}[x]\}$.

Primero notemos que si $r(x), s(x) \in \mathcal{A}, c(x) \in \mathbb{K}[x]$, entonces $r(x) + c(x)s(x) \in \mathcal{A}$, para ello sea

$$r(x) = a(x)p_1(x) + b(x)q_1(x), \quad s(x) = a(x)p_2(x) + b(x)q_2(x)$$

luego tenemos

$$\begin{aligned} r(x) + c(x)s(x) &= a(x)p_1(x) + b(x)q_2(x)(+c(x)(a(x)p_2(x) + b(x)q_2(x)) \\ &= a(x)(p_1(x) + c(x)p_2(x)) + b(x)(q_1(x) + c(x)q_2(x)) \end{aligned}$$

Sea $d(x)$ el polinomio no nulo de grado menor en $\mathcal{A}$, demostraremos que todo polinomio en $\mathcal{A}$ es un múltiplo de $d(x)$.

Sea $h(x) \in \mathcal{A}$, luego aplicando el algoritmo de la división obtenemos

$$h(x) = d(x)s(x) + r(x) \quad \text{con } \mathrm{gr}(r(x)) < \mathrm{gr}(d(x)) \text{ o } r(x) = 0.$$

Luego tenemos que $r(x) = h(x) - d(x)s(x) \in \mathcal{A}$, por lo tanto $r(x) = 0$, es decir,

$$h(x) = d(x)s(x).$$

Notemos que $a(x), b(x) \in \mathcal{A}$, luego $d(x)|a(x)$ y $d(x)|b(x)$.
Ahora supongamos que $h(x)|a(x)$ y $h(x)|b(x)$, como $d(x) \in \mathcal{A}$, luego tenemos

$$\begin{aligned} d(x) &= a(x)p(x) + b(x)q(x) \\ d(x) &= h(x)s_1(x)p(x) + h(x)s_2(x)q(x) \\ d(x) &= h(x)(s_1(x)p(x) + s_2(x)q(x)) \end{aligned}$$

de lo cual tenemos $h(x)|d(x)$. □

6.5. Raíces de un Polinomio.

En esta sección se relaciona las raíces de un polinomio con una factorización, pero antes veremos la diferencia entre polinomio y función polinomial Sea $p(x) \in \mathbb{K}[x]$, luego

$$\begin{array}{rccc} p & : & \mathbb{N} & \to & \mathbb{K} \\ & & i & \rightsquigarrow & p_i \end{array}$$

y la función polinomial

$$\begin{array}{rccc} : & \mathbb{K} & \to & \mathbb{K} \\ & \alpha & \rightsquigarrow & p_0 + \sum_{k=1}^{\mathrm{gr(p)}} p_i \cdot \alpha^i \end{array}$$

Definición 60 *Sea $p(x) \in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$.*
Se dice que α una raíz o un cero de $p(x)$ si y sólo si $p(\alpha) = 0$

Teorema 167 (del factor) *Sean $p(x) \in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$ con $\mathrm{gr}(p(x)) \geq 1$ tenemos*

$$\alpha \text{ es raíz de } p(x) \text{ si y sólo si } (x - \alpha)|p(x).$$

Demostración: En primer lugar suponemos que α una raíz de $p(x)$
Aplicando el algoritmo de la división a $p(x)$ con $(x - \alpha)$ tenemos

$$p(x) = (x - \alpha) \cdot s(x) + r(x) \tag{6.1}$$

donde $r(x)$ es una constante.
Si evaluamos la función polinomial en α obtenemos

$$\begin{aligned} p(\alpha) &= (\alpha - \alpha) \cdot s(\alpha) + r(\alpha) \\ 0 &= r(\alpha) \end{aligned}$$

Luego $r(x) = 0$, reemplazando en 6.1 tenemos

$$p(x) = (x - \alpha) \cdot s(x)$$

Por lo tanto $(x - \alpha)|p(x)$.

En el otro sentido, si $(x - \alpha)|p(x)$ entonces

$$p(x) = (x - \alpha) \cdot q(x)$$

Evaluando en α obtenemos

$$\begin{aligned} p(\alpha) &= (\alpha - \alpha) \cdot q(\alpha) \\ &= 0. \end{aligned}$$

Por lo tanto α es raíz de $p(x)$. □

Notación: Sea $p(x) \in \mathbb{K}[x]$, si consideramos $p(x) = 0$, la llamaremos ecuación polinomial. Y las solución entregan las raíces de $p(x)$.

Teorema 168 *Sea $p(x) \in \mathbb{K}[x]$, $\text{gr}(p(x)) \geq 1$ entonces existe un cuerpo $\overline{\mathbb{K}}$ tal que $p(x)$ tiene todas las raíces en $\mathbb{K}$.*

Teorema 169 *Sea $p(x) \in \mathbb{K}[x]$, si $\text{gr}(p(x)) = n \geq 1$ entonces $p(x)$ tiene exactamente n raíces en $\overline{\mathbb{K}}$.*

Demostración: Sea $\alpha_1 \in \mathbb{K}$ una raíz del polinomio $p(x)$ entonces $(x - \alpha_1)$ divide a $p(x)$ y por algoritmo de la división

$$p(x) = (x - \alpha_1) \cdot r(x) \quad \text{y} \quad \text{gr}(r(x)) = n - 1$$

Ahora consideremos $\alpha_2 \in \mathbb{K}$ otra raíz pero del polinomio $r(x)$ entonces $(x - \alpha_2)$ divide a $r(x)$ y además

$$r(x) = (x - \alpha_1) \cdot s(x) \quad \text{y} \quad \text{gr}(s(x)) = n - 2$$

reemplazando obtenemos

$$p(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot s(x)$$

Si repetimos el proceso sucesivamente y suponiendo que todas las raíces están en $\mathbb{K}$ tenemos

$$p(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdots (x - \alpha_n)$$

donde α_i es una raíz de $p(x)$. Sea β una raíz entonces

$$0 = p(\beta) = (\beta - \alpha_1) \cdot (\beta - \alpha_2) \cdots (\beta - \alpha_n)$$

Como $\mathbb{K}$ es cuerpo, luego $\beta - \alpha_i = 0$ entonces $\beta = \alpha_i$. □

Observación: Si el polinomio $p(x)$ no tiene todas sus raíces en $\mathbb{K}[x]$ entonces

$$p(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdots (x - \alpha_i) \cdot q(x) \quad \text{y} \quad \text{gr}(q(x)) = n - i$$

Teorema 170 *Sea $p(x) \in \mathbb{K}[x]$, si $\text{gr}(p(x)) \leq 4$ entonces existe una formular para determinar todas las raíces de $p(x)$.*

Teorema 171 *Sea $p(x) \in \mathbb{C}[x]$ tal que $\text{gr}(p(x)) = n > 1$ entonces $p(x)$ tiene todas sus n raíces en $\mathbb{C}$.*

Teorema 172 *Sea $p(x) \in \mathbb{Z}[x]$ donde $\text{gr}(p(x)) = n$ y*

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

Si $\frac{a}{b} \in \mathbb{Q}$ es raíz de $p(x)$, con a, b primos relativos entonces $a|a_0$ y $b|a_n$.

Demostración: Si $\frac{a}{b}$ es una raíz de $p(x)$ entonces $p\left(\frac{a}{b}\right) = 0$. Como

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

luego

$$\begin{aligned}
p\left(\frac{a}{b}\right) = a_n \left(\frac{a}{b}\right)^n + \cdots + a_0 &= 0 \\
a_n \frac{a^n}{b^n} + \cdots + a_0 &= 0 \quad / \cdot b^n \\
a_n \frac{a^n}{b^n} \cdot b^n + \cdots + a_0 \cdot b^n &= 0 \\
a_n a^n + \cdots + a_0 b^n &= 0 \\
a_n a^n + \cdots + a_1 a b^{n-1} &= -a_0 b^n \\
a(a_n a^{n-1} + \cdots + a_1 b^{n-1}) &= -a_0 b^n
\end{aligned}$$

Ya que $(a_n a^{n-1} + \cdots + a_1 b^{n-1}) \in \mathbb{Z}$ entonces

$$a| - a_0 b^n$$

como $(a, b^n) = 1$ por ser primos relativos entonces $a|a_0$ Tomando

$$\begin{aligned}
a(a_n a^{n-1} + \cdots + a_1 b^{n-1}) &= -a_0 b^n \\
a_n a^n + \cdots + a_1 a b^{n-1} + a_0 b^n &= 0 \\
a_{n-1} a^{n-1} b + \cdots + a_1 a b^{n-1} + a_0 b^n &= -a_n a^n \\
b(a_{n-1} a^{n-1} + \cdots + a_1 a b^{n-2} + a_0 b^{n-1}) &= -a_n a^n
\end{aligned}$$

Como $(a_{n-1} a^{n-1} + \cdots + a_1 a b^{n-2} + a_0 b^{n-1}) \in \mathbb{Z}$ entonces

$$b| - a_n a^n$$

pero $(b, a^n) = 1$ por ser primos relativos entonces $b|a_n$. □

Teorema 173 *Sea $p(x) \in \mathbb{R}[x]$ y $\alpha \in \mathbb{C}$ tal que α es una raíz de $p(x)$ entonces $\overline{\alpha}$ es raíz de $p(x)$.*

Demostración: Dado un $p(x) \in \mathbb{R}[x]$ y $\alpha \in \mathbb{C}$ una raíz de $p(x)$, entonces $p(\alpha) = 0$

Sea $p(x) = a_n x^n + \cdots + a_0$ y calculamos $p(\alpha)$ tenemos

$$p(\alpha) \quad = \quad a_n(\alpha)^n + \cdots + a_0 = 0$$

Si aplicamos la función conjugado tenemos

$$\begin{aligned}
\overline{a_n(\alpha)^n + \cdots + a_0} &= \overline{0} \\
\overline{a_n(\alpha)^n + \cdots + a_0} &= 0 \\
\overline{a_n(\alpha)^n} + \cdots + \overline{a_0} &= 0 \\
\overline{a_n}\overline{(\alpha)^n} + \cdots + \overline{a_0} &= 0 \\
\overline{a_n}\overline{(\alpha)}^n + \cdots + \overline{a_0} &= 0
\end{aligned}$$

ya que $a_i \in \mathbb{R}$ con $i = 0, \cdots, n$ tenemos $\overline{a_i} = a_i$ entonces

$$\begin{aligned}
\overline{a_n}\overline{(\alpha)^n} + \cdots + \overline{a_0} &= 0 \\
a_n\overline{(\alpha)}^n + \cdots + a_0 &= 0
\end{aligned}$$

Por lo tanto $p(\overline{\alpha}) = 0$ entonces $\overline{\alpha}$ es raíz de $p(x)$.

Teorema 174 *Sea $p(x) \in \mathbb{R}[x]$ y si $\mathrm{gr}(p(x))$ es un número impar entonces $p(x)$ tiene una raíz real.*

Demostración: Como $\mathbb{R}[x] \subset \mathbb{C}[x]$ tenemos que si $p(x) \in \mathbb{R}[x]$ entonces $p(x) \in \mathbb{C}[x]$.

Luego por la teorema tenemos que $p(x)$ se descompone completamente, es decir, tiene todas sus raíces en $\mathbb{C}$, ya que $\mathrm{gr}(p(x))$ es un número impar, $p(x)$ tiene un número impar de raíces.

Por teorema tenemos que si α_i con $i = 1, \cdots, n$ es una raíz de $p(x)$ entonces $\overline{\alpha_i}$ también es raíz de $p(x)$. Entonces existe $\alpha_j \in \mathbb{C}$ raíz de $p(x)$ tal que

$$\overline{\alpha_j} = \alpha_j$$

Por lo tanto $\alpha_j \in \mathbb{R}$.

Teorema 175 *Sean $p(x) \in \mathbb{R}[x]$ donde $\mathrm{gr}(p(x)) \geq 1$ y $a, b \in \mathbb{R}$ tales que*

$$a < b \quad \wedge \quad p(a) \cdot p(b) < 0$$

entonces $p(x)$ tiene una raíz real en el intervalo $]a, b[$.

6.6. Polinomios Reducibles e Irreducibles.

Sea $p(x) \in \mathbb{K}[x]$ con $\mathrm{gr}(p(x)) \geq 1$ diremos que $p(x)$ es un `polinomio reducible` en $\mathbb{K}[x]$ si existen $q(x), r(x) \in \mathbb{K}[x]$ tales que

$$p(x) = q(x) \cdot r(x) \quad \text{con} \quad \mathrm{gr}(q(x)) \geq 1 \quad \text{y} \quad \mathrm{gr}(r(x)) \geq 1$$

se dice que $p(x)$ es `irreducible` si y sólo si $p(x)$ no es reducible $\mathrm{gr}(p(x)) \geq 1$

Teorema 176 *Sea $p(x) \in \mathbb{R}[x]$ y si $\text{gr}(p(x)) \geq 3$ entonces $p(x)$ es reducible.*

Demostración: Si $p(x)$ tiene una raíz real, entonces es reducible.

Si $p(x)$ no tiene raíces reales, luego son compleja y se encuentra también el conjugado

$$p(x) = (x-\alpha_1)(x-\overline{\alpha_1})(x-\alpha_2)(x-\overline{\alpha_2})\cdots(x-\alpha_r)(x-\overline{\alpha_r})$$

Luego multiplicando obtenemos

$$p(x) = (x^2-(\alpha_1+\overline{\alpha_1})x+\alpha_1)\overline{\alpha_1})(x^2-(\alpha_2+\overline{\alpha_2})x+\alpha_2)\overline{\alpha_2})\cdots(x^2-(\alpha_r+\overline{\alpha_r})x+\alpha_r)\overline{\alpha_r})$$

Factorización en $\mathbb{R}$. □

Propiedad 177 *Sea $p(x) \in \mathbb{R}[x]$ tenemos que $p(x)$ es irreducible si y sólo si*

1. $\text{gr}(p(x)) = 1$
2. $p(x) = ax^2+bx+c$ *tal que*
$$\Delta = b^2-4ac < 0$$

Propiedad 178 *Sea $p(x) \in \mathbb{C}[x]$ tenemos que $p(x)$ es irreducible si y sólo si* $\text{gr}(p(x)) = 1$

Teorema 179 *Sea $p(x) \in \mathbb{K}[x]$ y si $\text{gr}(p(x)) \geq 1$ entonces $p(x)$ es producto de polinomios irreducibles.*

Demostración: sea $p(x) \in \mathbb{K}[x]$, si $p(x)$ es irreducible, listo

Si $p(x)$ es reducible entonces existen $a(x), b(x) \in \mathbb{K}[x]$, tal que

$$p(x) = a(x)b(x) \qquad \text{con } \text{gr}(a(x)) < \text{gr}(p(x)) \wedge \text{gr}(b(x)) < \text{gr}(p(x))$$

si $a(x), b(x) \in \mathbb{K}[x]$, son irreducible listo, en caso contrario se sigue las descomposición □

6.7. Congruencia de Polinomio

Sean $a(x), b(x), p(x) \in \mathbb{K}[x]$, con $p(x) \neq 0$ entonces se define la relación de congruencia módulo $p(x)$

$$a(x) \equiv b(x)(\texttt{mod } p(x)) \;\Leftrightarrow\; p(x)|(a(x)-b(x))$$

Ejemplo 125 *Sea $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \in \mathbb{K}[x]$ entonces*

1. $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \equiv a_0(\texttt{mod } x\ )$
2. $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \equiv a_1x+a_0(\texttt{mod } x^2\ )$

Teorema 180 *Sea $p(x) \in \mathbb{K}[x]$, con $p(x) \neq 0$ entonces la relación de congruencia módulo $p(x)$ en $\mathbb{K}[x]$ es una relación de equivalencia*

Demostración: Similar a la efectuada en $\mathbb{Z}$

6.7.1. Sistema de Representante

Sean $a(x), p(x) \in \mathbb{K}[x]$, con $p(x) \neq 0$,
Sea $\overline{a(x)}$ la clase de que contiene a $a(x)$,

$$\overline{a(x)} = \{b(x) \in \mathbb{K}[x] \mid a(x) \equiv b(x)(\mathtt{mod}\ p(x))\},$$

aplicando el algoritmo de la división, tenemos

$$a(x) = p(x)q(x) + r(x) \quad \text{con } \mathrm{gr}(r(x)) < \mathrm{gr}(p(x)) \text{ o } r(x) = 0.$$

luego tenemos

$$a(x) \equiv r(x)(\mathtt{mod}\ p(x)) \quad \text{con } \mathrm{gr}(r(x)) < \mathrm{gr}(p(x)) \text{ o } r(x) = 0.$$

es decir, $\overline{a(x)} = \overline{r(x)}$.
Notación: El conjunto de las clase de equivalencia módulo $p(x)$ se denota por

$$\mathbb{K}[x]/\!<p(x)>\, = \{\overline{r(x)} \mid r(x) \in \mathbb{K}[x], \text{ tal que } \mathrm{gr}(r(x)) < \mathrm{gr}(p(x)) \text{ o } r(x) = 0\}.$$

6.7.2. Suma y Producto

Sean $\overline{a(x)}, \overline{b(x)} \in \mathbb{K}[x]/\!<p(x)>$.

Suma

$$\overline{a(x)} + \overline{b(x)} = \overline{a(x) + b(x)}$$

Producto

$$\overline{a(x)} \cdot \overline{b(x)} = \overline{a(x) \cdot b(x)}$$

Teorema 181 *$(\mathbb{K}[x]/\!<p(x)>, +, \cdot)$ es un anillo conmutativo*

Demostración: La demostración, es similar a la efectuada en $\mathbb{Z}_n$, y los elementos notables están dado por:
El neutro aditivo es $\overline{0(x)}$, el inverso aditivo de $\overline{p(x)}$ es $\overline{-p(x)}$, el inverso multiplicativo es $\overline{1}$ y denotamos por $\mathcal{U}(\mathbb{K}[x]/\!<p(x)>)$ el conjunto de los elementos invertible por

Teorema 182 *Sea $r(x) \in \mathbb{K}[x]$ tal que es primo relativo con $p(x)$ entonces $\overline{r(x)}$ es invertible en $\mathbb{K}[x]/\!<p(x)>$*

Demostración: Como $r(x), p(x)$ son primos relativos entonces existen $q(x), s(x)$ tales que

$$\begin{aligned} 1 &= r(x)q(x) + p(x)s(x) \\ 1 &\equiv r(x)q(x)(\mathtt{mod}\ p(x)) \\ \overline{1} &= \overline{r(x)q(x)} \end{aligned}$$

Luego $\overline{r(x)}$ tiene inverso.

Teorema 183 *Si $p(x)$ polinomio irreducible en $\mathbb{K}[x]$, entonces $(\mathbb{K}[x]/< p(x) >, +, \cdot)$ es un cuerpo*

Demostración: Como $p(x)$ es irreducible y si $r(x) \in \mathbb{K}[x]$ no nulo, tal que

$$\text{gr}(r(x)) < \text{gr}(p(x)),$$

luego son primo relativos, por lo tanto $\overline{r(x)}$ es invertible. □

Ejemplo 126 *En $\mathbb{Z}_2[x]$ el polinomio x^2+x+1 es irreducible, luego*

$$\mathbb{Z}_2[x]/< x^2+x+1 >= \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$$

es un cuerpo con 4 elementos y las tabla de suma y producto son

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

Ejemplo 127 *En $\mathbb{R}[x]$ el polinomio x^2+1 es irreducible, luego*

$$\mathbb{R}[x]/< x^2+1 >= \{\overline{ax+b} \mid a, b \in \mathbb{R}\}$$

es un cuerpo

6.8. Ejercicios Desarrollados

Ejemplo 128 *Sea $p(x) = 3x^4 - 5ax^3 + 7cx^2 - 1$. Determinar $a, c \in \mathbb{R}$ tal que 1 es una raíz de $p(x)$ y al dividir $p(x)$ por $x+1$ el resto es 10*

Solución: Ya que 1 es una raíz de $p(x)$, luego $p(1) = 0$, además al dividir $p(x)$ por $x+1$ el resto 10, es decir, $p(-1) = 10$.

$$\begin{aligned} p(1) &= 3 - 5a + 7c - 1 = 0 \\ p(-1) &= 3 + 5a + 7c - 1 = 10 \end{aligned}$$

Luego tenemos

$$\left.\begin{aligned} -5a + 7c &= -2 \\ 5a + 7c &= 8 \end{aligned}\right|$$

Sumando la ecuaciones, obtenemos

$$\begin{aligned} 14c &= 6 \\ c &= \frac{6}{14} = \frac{3}{7} \end{aligned}$$

Reemplazando

$$5a = 8 - 7c = 8 - \frac{21}{7} = 8 - 3 = 5$$

Por lo tanto

$$a = 1, \qquad c = \frac{3}{7}$$

Ejemplo 129 *Sea $p(x) \in \mathbb{K}[x]$, tal que al dividir $p(x)$ por $x+2$ el resto es 4 y al dividir $p(x)$ por $x-3$ es resto es 5.*

Calcular el resto al dividir $p(x)$ por $(x+2)\cdot(x-3)$.

Solución: Como $\text{gr}((x+2)\cdot(x-3)) = 2$, luego el resto debe puede ser escrito de la forma $r(x) = ax + b$.

Sabemos que

$$\begin{aligned} p(x) &= q_1(x)\cdot(x+2)+4 \\ p(x) &= q_2(x)\cdot(x-3)+5 \end{aligned}$$

Además

$$p(x) = q(x)\cdot(x+2)\cdot(x-3)+ax+b$$

Evaluando tenemos

$$\begin{aligned} 4 = \quad p(-2) &= -2a+b \\ 5 = \quad p(3) &= 3a+b \end{aligned}$$

De lo cual, se obtiene el siguiente sistema

$$\begin{array}{rcl|} -2a+b & = & 4 \\ \hline 3a+b & = & 5 \\ \hline \end{array}$$

Cuya solución es:

$$a = \frac{1}{5} \qquad b = \frac{22}{5}$$

Por lo tanto $r(x) = \frac{1}{5}x + \frac{22}{5}$

Ejemplo 130 *Encontrar el valor de $a, b \in \mathbb{R}$ de manera que $(x-2)^2$ sea un factor del polinomio $p(x) = x^4 + (a-2)x^3 + bx^2 + (a+b)x + 4$*

Solución: Usemos división sintética, para obtener los resto que deben ser cero

2	1	$a-2$	b	$a+b$	4
		2	$2a$	$4a+2b$	$10a+6b$
2	1	a	$2a+b$	$5a+3b$	$\mathbf{10a+6b+4}$
		2	$2a+4$	$8a+2b+8$	
	1	$a+2$	$4a+b+4$	$\mathbf{13a+5b+8}$	

De lo cual tenemos el sistema

$$\begin{array}{rcl|} 10a+6b & = & -4 \\ \hline 13a+5b & = & -8 \\ \hline \end{array}$$

Cuya solución es:

$$a = -1 \qquad b = 1$$

Por lo tanto, el polinomio es $p(x) = x^4 - 3x^3 + x^2 + 4$.

Ejemplo 131 *Sea $p(x) \in \mathbb{R}[x]$, tal que al dividir $p(x)$ por $x-1$ el resto es 2, al dividir $p(x)$ por $x+2$ es resto es 4 y 2 es raíz de $p(x)$ Calcular el resto al dividir $p(x)$ por $(x-1)\cdot(x+2)\cdot(x-2)$.*

Solución: $\text{gr}((x-1)\cdot(x+2)\cdot(x-2)) = 3$, luego el resto debe tener la forma $r(x) = ax^2+bx+c$.
Sabemos que

$$\begin{aligned} p(x) &= q_1(x)\cdot(x-1)+2 \\ p(x) &= q_2(x)\cdot(x+2)+4 \\ p(x) &= q_3(x)\cdot(x-2)+0 \end{aligned}$$

Además

$$p(x) = q(x)\cdot(x-1)\cdot(x+2)\cdot(x-2)+ax^2+bx+c$$

Evaluando tenemos

$$\begin{aligned} 2 = \quad p(1) &= a+b+c \\ 0 = \quad p(2) &= 4a+2b+c \\ 4 = \quad p(-2) &= 4a-2b+c \end{aligned}$$

De lo cual tenemos el sistema

$$\left|\begin{array}{rcll} a+b+c &=& 2 & \\ 4a+2b+c &=& 0 & /\cdot -1 \\ 4a-2b+c &=& 4 & \end{array}\right|$$

Luego la solución es:

$$a = -\frac{1}{3}, \qquad b = -1, \qquad c = \frac{10}{3}$$

Por lo tanto $r(x) = -\frac{1}{3}x^2 - x + \frac{10}{3}$

Ejemplo 132 *Sea $p(x) = x^4-4$. Descomponer en factores irreducibles el polinomio $p(x)$ en $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$*

Solución:

a) En $\mathbb{Q}[x]$: $\quad x^4-4 = (x^2-2)\cdot(x^2+2)$

b) En $\mathbb{R}[x]$: $\quad x^4-4 = (x+\sqrt{2})\cdot(x-\sqrt{2})\cdot(x^2+2)$

c) En $\mathbb{C}[x]$: $\quad x^4-4 = (x+\sqrt{2})\cdot(x-\sqrt{2})\cdot(x+\sqrt{2}i)\cdot(x-\sqrt{2}i)$

Ejemplo 133 *Sea $p(x) = x^5+x^4+x^3+x^2+x+1$. Descomponer en factores irreducibles el polinomio $p(x)$ en $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$*

Solución: Como $p(-1) = 0$, luego tenemos $p(x) = (x+1)(x^4+x^2+1) = (x+1)((x^2+1)^2-x^2)$

a) En $\mathbb{Q}[x]$: $p(x) = (x+1)\cdot(x^2+x+1)\cdot(x^2-x+1)$

b) En $\mathbb{R}[x]$: $p(x) = (x+1)\cdot(x^2+x+1)\cdot(x^2-x+1)$

c) En $\mathbb{C}[x]$:

$$p(x) = (x+1)\left(x-\frac{1+\sqrt{3}i}{2}\right)\left(x-\frac{1-\sqrt{3}i}{2}\right)\left(x-\frac{-1+\sqrt{3}i}{2}\right)\left(x-\frac{-1-\sqrt{3}i}{2}\right)$$

Ejemplo 134 *Sea* $p(x) = x^4+5x^3+12x^2+22x-40$

a) Determine las raíces racionales de $p(x)$.

b) Factoricé $p(x)$ *como producto de polinomios irreducibles en* $\mathbb{Q}[x]$

c) Factoricé $p(x)$ *como producto de polinomios irreducibles en* $\mathbb{R}[x]$

d) Factoricé $p(x)$ *como producto de polinomios irreducibles en* $\mathbb{C}[x]$

Solución: Sea $p(x) = x^4+5x^3+12x^2+22x-40$

a) Determine las raíces racionales de $p(x)$.

La posibles raíces racionales $\frac{p}{q}$, tal que p, q primos relativos entonces $p|-40, \quad q|1$

$$p \in \{\pm1, \pm2, \pm4, \pm5, \pm8, \pm10, \pm20, \pm40\} \qquad q \in \{\pm1\}$$

Luego

$$\frac{p}{q} \in \{\pm1, \pm2, \pm4, \pm5, \pm8, \pm10, \pm20, \pm40\}$$

1	1	5	12	22	-40
		1	6	18	40
-4	1	6	18	40	0
		-4	-8	-40	
	1	2	10	0	

Por lo tanto las raíces racionales son: $1, -4$.

b) Factoricé $p(x)$ como producto de polinomios irreducibles en $\mathbb{Q}[x]$

$p(x) = (x-1)\cdot(x+4)\cdot(x^2+2x+10)$

c) Factoricé $p(x)$ como producto de polinomios irreducibles en $\mathbb{R}[x]$

$p(x) = (x-1)\cdot(x+4)\cdot(x^2+2x+10)$

d) Factoricé $p(x)$ como producto de polinomios irreducibles en $\mathbb{C}[x]$

El discriminante de $x^2+2x+10$ es $\Delta=-36$, la raíces son $-1+3i,\ -1-3i$. por lo tanto

$$p(x)=(x-1)\cdot(x-4)\cdot(x-(-1+3i))\cdot(x-(-1-3i))$$

Ejemplo 135 *Factorizar $x^6-x^5+x^4-x^3+x^2-x$ como producto de polinomios irreducibles en $\mathbb{Z}_7[x]$*

Solución: $p(x)=x^6-x^5+x^4-x^3+x^2-x=x\cdot(x^5-x^4+x^3-x^2+x-1)$

1	1	-1	1	-1	1	-1
		1	0	1	0	1
2	1	0	1	0	1	0
		2	4	10	20	
-2	1	2	5	10	$21=0$	
		-2	0	-10		
3	1	0	5	0		
		3	9			
-3	1	3	$14=0$			
		-3				
	1	0				

Por lo tanto $p(x)=x\cdot(x-1)\cdot(x-2)\cdot(x+2)\cdot(x-3)\cdot(x+3)$

Ejemplo 136 *Encuentre los valores del parámetro k en la ecuación $x^3-7x+k=0$ de modo que una de sus raíces sea el doble de la otra. Y en cadas casos, determine las soluciones de la ecuación.*

Solución: Sean $a, 2a, c$ las distintas raíces

$$\begin{aligned}
x^3-7x+k &= (x-a)\cdot(x-2a)\cdot(x-c)\\
x^3-7x+k &= (x^2-2ax+2a^2-ax)\cdot(x-c)\\
x^3-7x+k &= x^3-x^2c-2ax^2+2acx+2a^2x-2a^2c-ax^2+acx\\
x^3-7x+k &= x^3+x^2\cdot(-c-3a)+x\cdot(3ac-2a^2)-2a^2c
\end{aligned}$$

De lo cual tenemos el sistema

$$\left.\begin{aligned}
-c-3a &= 0\\
3ac+2a^2 &= -7\\
-2a^2c &= k
\end{aligned}\right|$$

Luego la solución es:

$$((a=1\ \wedge\ c=-3\ \wedge\ k=6)\ \ \vee\ \ (a=-1\ \wedge\ c=3\ \wedge\ k=-6))$$

Por lo tanto, los polinomio se factorizan

$$x^3-7x+6=(x-1)(x-2)(x+3),\qquad x^3-7x-6=(x+1)(x+2)(x-3),$$

Ejemplo 137 *Dadas las raíces a, b, c de $x^3 - px + q = 0$, construya un polinomio de grado 3 cuyas raíces son a^2, b^2, c^2*

Solución: Como son las raíces luego tenemos

$$\begin{aligned} x^3 - px + q &= (x-a)\cdot(x-b)\cdot(x-c) \\ x^3 - px + q &= x^3 + (-a-b-c)\cdot x^2 + (ab+bc+ac)\cdot x - abc \end{aligned}$$

Igualando coeficiente se obtiene

$$\begin{aligned} -a-b-c &= 0 \\ ab+bc+ac &= -p \\ -abc &= q \end{aligned}$$

Por otra parte el polinomio construir

$$\begin{aligned} (x-a^2)(x-b^2)(x-c^2) &= (x^2 - a^2x - b^2x + a^2b^2)(x-c^2) \\ (x-a^2)(x-b^2)(x-c^2) &= x^3 + x^2(-a^2-b^2-c^2) + x(a^2b^2+b^2c^2+a^2c^2) - a^2b^2c^2 \end{aligned}$$

Necesitamos determinar los coeficiente en termino de p, q, el coeficiente constante del nuevo polinomio es

$$-a^2b^2c^2 = -(abc)^2 = -q^2$$

El coeficiente cuadrático

$$-a^2 - b^2 - c^2 = -(a-b-c)^2 + 2(ab+ac+bc) = 0 - 2p = -2p$$

El coeficiente lineal

$$a^2b^2 + b^2c^2 + a^2c^2 = (ab+bc+ac)^2 - 2(acb^2 + bca^2 + bac^2) = p^2 - 2abc(b+a+c) = p^2$$

Por lo tanto el polinomio pedido es

$$x^3 - 2px^2 + p^2x - q^2.$$

Ejemplo 138 *Sea $\mathbb{F}_9 = \mathbb{Z}_3[x]/< x^2+1 >$. Calcule $[x^5 + 2x^2 + 1]^{-1}$*

Solución: Sabemos que

$$\mathbb{F}_9 = \{\overline{ax+b} \quad | \quad a, b \in \mathbb{Z}_3\} = \mathbb{Z}_3[x]/< x^2+1 >$$

Además, aplicando el algoritmo de la división se tiene

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

Luego

$$\overline{x^5 + 2x^2 + 1} = \overline{x-1} \in \mathbb{F}_9$$

Ahora debemos determinar

$$(x-1)Y \equiv 1(\texttt{mod}\ x^2+1)$$

Pero notemos que

$$x^2+1=(x-1)(x+1)+2$$

De lo cual obtenemos

$$\overline{(x-1)(x+1)}=1$$

de esta manera tenemos

$$[x^5+2x^2+1]^{-1}=[x-1]^{-1}=[x+1]$$

Ejemplo 139 *Sea* $\mathbb{F}_9=\mathbb{Z}_3/<x^2+1>$ *y* $\overline{x^6+x^3+2}\in\mathbb{F}_9$. *Calcular* $\overline{x^6+x^3+2}^{-1}$

Solución: Sabemos que

$$\mathbb{F}_9 \quad = \quad \{\overline{ax+b} \quad | \quad a,b\in\mathbb{Z}_3\}=\mathbb{Z}_3/<x^2+1>$$

Además

$$x^6+x^3+2=(x^2+1)(x^4-x^2+x+1)+(-x+1)$$

Luego

$$\overline{x^6+x^3+2}=\overline{2x+1}\in\mathbb{F}_9$$

Ahora aplicando el algoritmo de la división tenemos

$$x^2+1=(2x+1)(2x-1)+2$$

De lo cual obtenemos

$$\overline{(2x+1)(2x-1)}=1$$

de esta manera tenemos

$$\overline{x^6+x^3+2}^{-1}=\overline{2x+1}^{-1}=\overline{2x-1}$$