TEMA 3 EL ANILLO DE LOS POLINOMIOS CON COEFICIENTES EN UN CUERPO

Un anillo es una terna $(R,+,\cdot)$ donde R es un conjunto y $+$ y $\cdot$ son dos operaciones sobre ese conjunto que verifican las siguientes propiedades:

1) La operacion $+$ es conmutativa, asociativa, tiene elemento neutro (que denotaremos por 0) y todo elemento tiene inverso (al inverso de x lo denotaremos $-x$)

2) La operacion $\cdot$ es asociativa, tiene elemento neutro (que denotaremos por 1) y es distributiva.

Si ademas la operacion $\cdot$ es conmutativa, entonces diremos que el anillo es conmutativo. Un cuerpo es un anillo conmutativo en el que todo elemento distinto de 0 tiene inverso para el producto (al inverso de x lo denotaremos por x^{-1}).

EJEMPLOS

$(\mathbb{N},+,\cdot)$ no es un anillo.

$(\mathbb{Z},+,\cdot)$ es un anillo conmutativo y no es cuerpo.

$(\mathbb{Q},+,\cdot)$ y $(\mathbb{R},+,\cdot)$ son cuerpos.

PROPOSICION

Si m es un entero mayor o igual que 2, entonces $(\mathbb{Z}_m, +, \cdot)$ es un anillo conmutativo. Además, es un cuerpo si y sólo si m es un número primo.

Sea $\mathbb{K}$ un cuerpo. El conjunto de los polinomios con coeficientes en el cuerpo $\mathbb{K}$ en la indeterminada x es $\mathbb{K}[x] = \{a_0 + a_1 x + \cdots + a_n x^n \text{ tq } n \in \mathbb{N} \text{ y } \{a_0, a_1, \ldots, a_n\} \subseteq \mathbb{K}\}$.

EJERCICIO

Sea $a(x) = 3 + 4x + 3x^2$ y $b(x) = 4 + 2x + x^2 + 2x^3$ dos polinomios de $\mathbb{Z}_5[x]$. Calcular $a(x) + b(x)$ y $a(x) \cdot b(x)$.

-D-

- $a(x) + b(x) = (3+4) + (4+2)x + (3+1)x^2 + 2x^3 = 2 + x + 4x^2 + 2x^3$
- Vamos a calcular ahora $a(x) \cdot b(x)$

$$
\begin{array}{r}
2x^3 + x^2 + 2x + 4 \\
3x^2 + 4x + 3 \\
\hline
x^5 + 3x^4 + x^3 + 2x^2 \qquad\qquad \\
3x^4 + 4x^3 + 3x^2 + x \qquad \\
x^3 + 3x^2 + x + 2 \\
\hline
x^5 + x^4 + x^3 + 3x^2 + 2x + 2
\end{array}
= a(x) \cdot b(x)
$$

PROPOSICION

Si $\mathbb{K}$ es un cuerpo, entonces $(\mathbb{K}[x], +, \cdot)$ es un anillo conmutativo. Además no es cuerpo.

Si $a(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{K}[x]$ y $a_n \neq 0$, entonces diremos que $a(x)$ es un polinomio de grado n y lo denotaremos $gr(a(x)) = n$. Por definición $gr(0) = -\infty$

PROPOSICION

Si $\mathbb{K}$ es un cuerpo y $a(x), b(x) \in \mathbb{K}[x]$ entonces $gr(a(x) \cdot b(x)) = gr(a(x)) + gr(b(x))$.

Un elemento de un anillo R es una unidad si tiene inverso para el producto. Denotaremos por $\mathcal{U}(R)$ al conjunto formado por todas las unidades del anillo R.

EJEMPLO

1) $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$.
2) Si $\mathbb{K}$ es cuerpo, entonces $\mathcal{U}(\mathbb{K}) = \mathbb{K} \setminus \{0\}$.
3) $\mathcal{U}(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$.
4) $\mathcal{U}(\mathbb{Z}_5) = \{1, 2, 3, 4\}$.

PROPOSICION

Si $\mathbb{K}$ es un cuerpo, entonces $\mathcal{U}(\mathbb{K}[x]) = \{a(x) \in \mathbb{K}[x]$ tq $gr(a(x)) = 0\}$.

EJEMPLO

$\mathcal{U}(\mathbb{Z}_7[x]) = \{1,2,3,4,5,6\}$.

Sea $\mathbb{K}$ un cuerpo. Un elemento $a(x) \in \mathbb{K}[x]$ es irreducible si verifica lo siguiente:

1) $gr(a(x)) \geq 1$.

2) si $a(x) = b(x) \cdot c(x)$ entonces $gr(b(x)) = 0$ ó $gr(c(x)) = 0$.

PROPOSICION

Si $\mathbb{K}$ es un cuerpo entonces:

1) Todo polinomio de $\mathbb{K}[x]$ de grado 1 es irreducible.

2) Si $a(x) \in \mathbb{K}[x]$ es irreducible y $u \in \mathbb{K} \setminus \{0\}$ entonces $u \cdot a(x)$ es también irreducible.

Un polinomio $a(x) \in \mathbb{K}[x]$ es mónico si el coeficiente del termino de mayor grado (llamado coeficiente lider) vale 1.

Ejemplo

El polinomio $x^2+2x+3 \in \mathbb{Z}_5[x]$ es monico.

El polinomio $3x^2+4x+1 \in \mathbb{Z}_7[x]$ no es monico.

TEOREMA

Sea $\mathbb{K}$ un cuerpo. Todo polinomio $a(x) \in \mathbb{K}[x]$ de grado mayor o igual que uno se puede expresar de forma unica (salvo reordenaciones) como $a(x) = u \cdot P_1(x)^{\alpha_1} \cdot \ldots \cdot P_r(x)^{\alpha_r}$ donde $u \in \mathbb{K} \setminus \{0\}$, $\{\alpha_1, \ldots, \alpha_r\} \subseteq \mathbb{N} \setminus \{0\}$ y $P_1(x), \ldots, P_r(x)$ son polinomios monicos e irreducibles.

A la expresión $a(x) = u \cdot P_1(x)^{\alpha_1} \cdot \ldots \cdot P_r(x)^{\alpha_r}$ la llamaremos la descomposición en irreducibles de $a(x)$.

EJERCICIO

Calcular la descomposición en irreducibles de $a(x) = (4x+3)(3x+2) \in \mathbb{Z}_7[x]$.

-D-

Como $4x+3$ y $3x+2$ son irreducibles (ya que tienen grado 1). Entonces tenemos una descomposición en irreducibles de $a(x)$, pero dicha descomposición no es la descomposición en irreducibles ya que los polinomios no son mónicos.

Para pasar de una descomposición en irreducibles a la descomposición en irreducibles hacemos lo siguiente:

$$a(x) = (4x+3)(3x+2) = 4 \cdot 2(4x+3) 3 \cdot 5(3x+2) = 4 \cdot (x+6) \cdot 3 \cdot (x+3) =$$
$$= 5(x+6)(x+3).$$

Como $5 \in \mathbb{Z}_7 \setminus \{0\}$ y $x+6$ y $x+3$ son polinomios mónicos e irreducibles, entonces podemos afirmar que $5(x+6)(x+3)$ es la descomposición en irreducibles de $a(x)$.

Sea $\mathbb{K}$ un cuerpo y $\{a(x), b(x)\} \subseteq \mathbb{K}[x]$. Diremos que $a(x)$ divide a $b(x)$ (ó que $a(x)$ es un divisor de $b(x)$) (ó que $b(x)$ es un múltiplo de $a(x)$) y lo denotaremos $a(x) | b(x)$ si existe $c(x) \in \mathbb{K}[x]$ tq $b(x) = a(x) \cdot c(x)$.

• Si $\{a(x), b(x)\} \subseteq \mathbb{K}[x]$ y $a(x) \neq 0$ ó $b(x) \neq 0$, entonces un elemento $d(x) \in \mathbb{K}[x]$ diremos que es un maximo comun divisor de $a(x)$ y $b(x)$ si verifica lo siguiente:

1) $d(x) | a(x)$ y $d(x) | b(x)$
2) si $c(x) | a(x)$ y $c(x) | b(x)$ entonces $c(x) | d(x)$.

NOTA

Si $d(x)$ es un m.c.d de $a(x)$ y $b(x)$ entonces tambien lo es $u \cdot d(x)$ para todo $u \in \mathbb{K} \setminus \{0\}$. Cuando escribamos m.c.d$\{a(x), b(x)\}$ nos referiremos al m.c.d de $a(x)$ y $b(x)$ que es monico. Asi, por ejemplo si $\{a(x), b(x)\} \subseteq \mathbb{Z}_5[x]$ y $3x^2+x+1$ es un m.c.d de $a(x)$ y $b(x)$ entonces $2(3x^2+x+1) = x^2+2x+2$, $3(3x^2+x+1) = 4x^2+3x+3$ y $4(3x^2+x+1) = 2x^2+4x+4$ son tambien m.c.d de $a(x)$ y $b(x)$. Ademas,

m.c.d$\{a(x), b(x)\} = x^2+2x+2$.

• Si $\{a(x), b(x)\} \subseteq \mathbb{K}[x]$, entonces un polinomio $m(x) \in \mathbb{K}[x]$ diremos que es un minimo comun multiplo de $a(x)$ y $b(x)$ si verifica lo siguiente:

1) $a(x) | m(x)$ y $b(x) | m(x)$
2) si $a(x) | c(x)$ y $b(x) | c(x)$ entonces $m(x) | c(x)$

NOTA

Si $m(x)$ es un m.c.m. de $a(x)$ y $b(x)$ entonces también lo es $u \cdot m(x)$ para todo $u \in \mathbb{K} \setminus \{0\}$. Cuando escribamos $m.c.m\{a(x), b(x)\}$ nos referiremos al m.c.m. de $a(x)$ y $b(x)$ que es mónico.

TEOREMA

Sea $\mathbb{K}$ un cuerpo, $a(x) = u \cdot P_1(x)^{\alpha_1} \cdot \ldots \cdot P_r(x)^{\alpha_r}$, $b(x) = v\, P_1(x)^{\beta_1} \cdot \ldots \cdot P_r(x)^{\beta_r}$ con $\{u, v\} \subseteq \mathbb{K} \setminus \{0\}$, $\{\alpha_1, \beta_1, \ldots, \alpha_r, \beta_r\} \subseteq \mathbb{N}$ y $P_1(x), \ldots, P_r(x)$ polinomios mónicos e irreducibles de $\mathbb{K}[x]$. Entonces:

1) $m.c.d\{a(x), b(x)\} = P_1(x)^{\min\{\alpha_1, \beta_1\}} \cdot \ldots \cdot P_r(x)^{\min\{\alpha_r, \beta_r\}}$

2) $m.c.m.\{a(x), b(x)\} = P_1(x)^{\max\{\alpha_1, \beta_1\}} \cdot \ldots \cdot P_r(x)^{\max\{\alpha_r, \beta_r\}}$

EJERCICIO

Dados los polinomios $a(x) = (x+1)(2x+3)$ y $b(x) = (x+2)(4x+1)$ de $\mathbb{Z}_5[x]$. Calcular $m.c.d\{a(x), b(x)\}$ y $m.c.m\{a(x), b(x)\}$.

-D-

$a(x) = (x+1)(2x+3) = (x+1)2 \cdot 3(2x+3) = 2(x+1)(x+4)$.

$b(x) = (x+2)(4x+1) = (x+2)4 \cdot 4(4x+1) = 4(x+2)(x+4)$.

Por tanto $a(x) = 2(x+1)^1(x+4)^1(x+2)^0$ y $b(x) = 4(x+1)^0(x+4)^1(x+2)^1$.

Aplicando el Teorema anterior obtenemos que

$m.c.d\{a(x), b(x)\} = (x+1)^0(x+4)^1(x+2)^0 = x+4$. y

$m.c.m\{a(x), b(x)\} = (x+1)^1 \cdot (x+4)^1 \cdot (x+2)^1$.

Propiedad de la división

Sea $\mathbb{K}$ un cuerpo y $\{a(x), b(x)\} \subseteq \mathbb{K}[x]$ tq $b(x) \neq 0$. Entonces existen unos únicos polinomios $q(x)$ y $r(x)$ de $\mathbb{K}[x]$ tales que $a(x) = q(x)b(x) + r(x)$ y $gr(r(x)) < gr(b(x))$.

A los polinomios $q(x)$ y $r(x)$ los llamaremos el cociente y el resto de dividir $a(x)$ entre $b(x)$ y los denotaremos por $a(x) \operatorname{div} b(x)$ y $a(x) \bmod b(x)$ respectivamente

EJERCICIO

Calcular el cociente y el resto de dividir $3x^3+4x^2+2x+3$ entre $2x^2+2x+1$ en $\mathbb{Z}_5[x]$.

-D-

$$
\begin{array}{l|l}
3x^3+4x^2+2x+3 & 2x^2+2x+1 \\
\cline{2-2}
2x^3+2x^2+x & 4x+3 \\
\cline{1-1}
\quad x^2+3x+3 & \\
\quad 4x^2+4x+2 & \\
\cline{1-1}
\qquad 2x &
\end{array}
$$

$$3x^3+4x^2+2x+3 \operatorname{div} 2x^2+2x+1 = 4x+3$$

$$3x^3+4x^2+2x+3 \bmod 2x^2+2x+1 = 2x.$$

Algoritmo de Euclides

Entrada: Dos polinomios $a(x)$ y $b(x)$ distintos de cero.

Salida: Un m.c.d de $a(x)$ y $b(x)$.

$$(a_0(x), a_1(x)) = (a(x), b(x))$$

Mientras $a_1(x) \neq 0$

$$(a_0(x), a_1(x)) = (a_1(x),\ a_0(x) \bmod a_1(x))$$

Devuelve $a_0(x)$.

NOTA

El Algoritmo anterior también nos sirve para calcular un m.c.m. de $a(x)$ y $b(x)$ ya que si $d(x)$ es un m.c.d de $a(x)$ y $b(x)$ entonces $a(x)b(x) \operatorname{div} d(x)$ es un m.c.m. de $a(x)$ y $b(x)$.

EJERCICIO

Calcular un m.c.d y un m.c.m de los polinomios x^3+x^2+4x+4 y $2x^2+x+4$ de $\mathbb{Z}_5[x]$.

-D-

Para calcular un m.c.d utilizaremos el algoritmo de Euclides

$(a_0(x), a_1(x)) = (x^3+x^2+4x+4,\ 2x^2+x+4) = (2x^2+x+4,\ 3x+3) =$

$= (3x+3,\ 0)$. Por tanto $3x+3$ es un m.c.d.

Para calcular un m.c.m. utilizaremos la nota anterior.

Un m.c.m es $(x^3+x^2+4x+4)(2x^2+x+4)$ div $3x+3$.

$$
\begin{array}{r}
x^3+x^2+4x+4 \\
2x^2+x+4 \\
\hline
2x^5+2x^4+3x^3+3x^2 \\
x^4+x^3+4x^2+4x \\
4x^3+4x^2+x+1 \\
\hline
2x^5+3x^4+3x^3+x^2+0\cdot x+1.
\end{array}
$$

$$
\begin{array}{l|l}
2x^5+3x^4+3x^3+x^2+0\cdot x+1 & 3x+3 \\
\cline{2-2}
3x^5+3x^4 & 4x^4+2x^3+4x^2+3x+2 \\
\cline{1-1}
\quad x^4+3x^3+x^2+0\cdot x+1 & \\
\quad 4x^4+4x^3 & \\
\cline{1-1}
\qquad 2x^3+x^2+0x+1 & \\
\qquad 3x^3+3x^2 & \\
\cline{1-1}
\qquad\quad 4x^2+0x+1 & \\
\qquad\quad x^2+x & \\
\cline{1-1}
\qquad\qquad x+1 & \\
\qquad\qquad 4x+4 & \\
\cline{1-1}
\qquad\qquad\quad 0 &
\end{array}
$$

Por consiguiente un m.c.m es $4x^4+2x^3+4x^2+3x+2$.

Sea $a(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{K}[x]$. Un elemento $\alpha \in \mathbb{K}$ diremos que es una raiz de $a(x)$ si $a(\alpha) = a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$.

Ejercicio

Calcular las raices del polinomio $a(x) = x^3 + 2x^2 + x + 2 \in \mathbb{Z}_5[x]$.

-D-

$a(0) = 2$, $a(1) = 1$, $a(2) = 0$, $a(3) = 0$ y $a(4) = 2$

Las raices de $a(x)$ son 2 y 3.

Teorema del factor

Sea $a(x) \in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$. Entonces α es una raiz de $a(x)$ si y solo si $x - \alpha \mid a(x)$.

COROLARIO

Un polinomio $a(x) \in \mathbb{K}[x] \setminus \{0\}$ es multiplo de un polinomio de grado uno si y solo si $a(x)$ tiene al menos una raiz.

COROLARIO

Sea $a(x) \in \mathbb{K}[x]$ tq $gr(a(x)) \in \{2, 3\}$. Entonces $a(x)$ es irreducible si y solo si no tiene raices.

EJERCICIO

Estudiar la reducibilidad ó irreducibilidad de los siguientes polinomios. $2X+1$, X^3+X+1 y X^2+1 de $\mathbb{Z}_3[X]$.

-D-

- $2X+1$ es irreducible ya que es de grado 1.
- X^3+X+1 es reducible ya que 1 es una raiz
- X^2+1 es irreducible ya que tiene grado 2 y no tiene raices.

TEOREMA

Sea $a(x) \in \mathbb{K}[x]$. Entonces:

1) Si $gr(a(x)) = 1$, entonces $a(x)$ es irreducible.

2) Si $gr(a(x)) \geq 2$ y $a(x)$ tiene al menos una raiz entonces $a(x)$ es reducible.

3) Si $gr(a(x)) \in \{2,3\}$, entonces $a(x)$ es irreducible si y solo si no tiene raices.

4) Si $gr(a(x)) \in \{4,5\}$, entonces $a(x)$ es irreducible si y solo si no tiene raices y no es divisible por ningun polinomio monico e irreducible de grado 2.

5) Si $gr(a(x)) \in \{6,7\}$, entonces $a(x)$ es irreducible si y solo si no tiene raices y no es divisible por ningun polinomio monico e irreducible de grado 2 ó 3.

EJERCICIO

¿Es irreducible el polinomio $x^4+x^2+2 \in \mathbb{Z}_3[x]$?

-D-

Lo primero que observamos es que no tiene raices. Por tanto sera irreducible si y solo si ningun polinomio de $\mathbb{Z}_3[x]$ de grado 2 monico e irreducible lo divide.

Vamos a construir todos los polinomios de $\mathbb{Z}_3[x]$ de grado 2 monicos e irreducibles. Para ello construiremos todos los policinimios monicos de grado y tacharemos los que tienen raices.

$\cancel{x^2}$, x^2+1, $\cancel{x^2+2}$, $\cancel{x^2+x}$, $\cancel{x^2+x+1}$, x^2+x+2, $\cancel{x^2+2x}$,

$\cancel{x^2+2x+1}$, x^2+2x+2

Los polinomios monicos e irreducibles de grado 2 de $\mathbb{Z}_3[x]$ son

x^2+1, x^2+x+2 y x^2+2x+2.

Ahora vamos a dividir el polinomio x^4+x^2+2 entre cada uno de estos polinomios. Si algun resto da cero el polinomio es reducible y si los tres restos dan distintos de cero el polinomio es irreducible.

$$\begin{array}{l|l} x^4+x^2+2 & x^2+1 \\ \hline 2x^4+2x^2 & x^2 \\ \hline 2 & \end{array}$$

$$\begin{array}{l|l} x^4+x^2+2 & x^2+x+2 \\ \hline 2x^4+2x^3+x^2 & x^2+2x \\ \hline 2x^3+2x^2+2 & \\ x^3+x^2+2x & \\ \hline 2x+2 & \end{array}$$

$$\begin{array}{l|l} x^4+x^2+2 & x^2+2x+2 \\ \hline 2x^4+x^3+x^2 & x^2+x \\ \hline x^3+2x^2+2 & \\ 2x^3+x^2+x & \\ \hline x+2 & \end{array}$$

Por tanto el polinomio $x^4+x^2+2 \in \mathbb{Z}_3[x]$ es irreducible.

Teorema del Resto

Sea $a(x) \in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$. Entonces $a(x) \bmod x-\alpha = a(\alpha)$.

Ejercicio

Sea $a(x) = 3x^4+x^3+2x^2+x+4 \in \mathbb{Z}_5[x]$. Calcular el resto de dividir $a(x)$ entre $x+4$.

-D-

$$a(x) \bmod x+4 = a(x) \bmod x-1 = a(1) = 3+1+2+1+4 = 1$$

Ejercicio

Calcular en $\mathbb{Z}_5[x]$ el resto de dividir $x^{1002}+x^{77}+1$ entre $x+3$

-D-

$$x^{1002}+x^{77}+1 \bmod x+3 = x^{1002}+x^{77}+1 \bmod x-2 =$$
$$= 2^{1002}+2^{77}+1$$

Veamos que vale $2^{1002}+2^{77}+1$ en $\mathbb{Z}_5$.

$2^1=2,\ 2^2=4,\ 2^3=3,\ 2^4=1.$

$$\begin{array}{r|l} 1002 & 4 \\ \hline 20 & 250 \\ 02 & \end{array} \qquad 1002 = 4 \cdot 250 + 2 \qquad \begin{array}{r|l} 77 & 4 \\ \hline 37 & 19 \\ 1 & \end{array} \qquad 77 = 4 \cdot 19 + 1$$

$$2^{1002}+2^{77}+1 = 2^{4\cdot 250+2}+2^{4\cdot 19+1}+1 = (2^4)^{250}\cdot 2^2+(2^4)^{19}\cdot 2^1+1$$
$$= 4+2+1 = 2$$

La solución del problema es 2

Sea $a(x) \in \mathbb{K}[x] \setminus \{0\}$. Si α es una raiz de $a(x)$, entonces tenemos que $a(x) = (x-\alpha)^m \cdot b(x)$ con $m \in \mathbb{N} \setminus \{0\}$ y $b(\alpha) \neq 0$. Al numero m lo llamaremos la multiplicidad de la raiz α. Si $m=1$ entonces diremos que α es una raiz simple y si $m \geq 2$ entonces diremos que α es una raiz multiple.

PROPOSICION

Si $a(x) \in \mathbb{K}[x] \setminus \{0\}$, entonces la suma de las multiplicidades de las raices de $a(x)$ es menor o igual que $gr(a(x))$.

EJERCICIO

Calcula las raices y sus multiplicidades del polinomio $x^3+2x+3 \in \mathbb{Z}_5[x]$.

-D-

Lo primero que observamos es que el polinomio tiene como raices 2 y 4.

• Vamos a calcular la multiplicidad de la raiz 2. Para ello dividimos x^3+2x+3 entre $x-2 = x+3$.

$$
\begin{array}{l|l}
x^3 + 2x + 3 & x+3 \\ \cline{2-2}
4x^3 + 2x^2 & x^2 + 2x + 1 \\ \cline{1-1}
2x^2 + 2x + 3 & \\
3x^2 + 4x & \\ \cline{1-1}
x + 3 & \\
4x + 2 & \\ \cline{1-1}
0 &
\end{array}
$$

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

Como x^2+2x+1 no se anula en 2 podemos afirmar que 2 es una raiz de multiplicidad 1.

- Vamos a calcular la multiplicidad de la raiz 4. Para ello dividimos x^3+2x+3 entre $x-4=x+1$.

$$\begin{array}{l|l}
x^3+2x+3 & x+1 \\ \cline{2-2}
4x^3+4x^2 & x^2+4x+3 \\ \cline{1-1}
4x^2+2x+3 & \\
x^2+x & \\ \cline{1-1}
3x+3 & \\
2x+2 & \\ \cline{1-1}
0 &
\end{array}$$

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

El polinomio x^2+4x+3 se anula en 4. Entonces divido x^2+4x+3 entre $x-4=x+1$

$$\begin{array}{l|l}
x^2+4x+3 & x+1 \\ \cline{2-2}
4x^2+4x & x+3 \\ \cline{1-1}
3x+3 & \\
2x+2 & \\ \cline{1-1}
0 &
\end{array}$$

$$x^2+4x+3=(x-4)(x+3) \Longrightarrow x^3+2x+3=(x-4)^2(x+3)$$

Como $x+3$ no se anula en 4, entonces podemos afirmar que 4 es una raiz de multiplicidad 2.

TEOREMA

Sea α una raiz de $a(x) \in \mathbb{K}[x]$. Entonces α es una raiz multiple si y solo si α es tambien raiz de $a'(x)$ (donde $a'(x)$ es la derivada de $a(x)$).

NOTA

Si $a(x) = 4x^3 + 3x^2 + 2x + 1 \in \mathbb{Z}_5[x]$, entonces $a'(x) = 2x^2 + x + 2$.

EJERCICIO

Calcula las raices multiples del polinomio $a(x) = x^3 + 4x^2 + 5x + 2$ de $\mathbb{R}[x]$.

-D-

Como es un polinomio de $\mathbb{R}[x]$ de grado 3 no sabemos calcular sus raices. Ahora bien, su derivada es de grado 2 y por tanto sabemos calcular sus raices. Las raices multiples del polinomio son las raices de la derivada que tambien sean raices del polinomio.

$$a'(x) = 3x^2 + 8x + 5$$

$$3x^2 + 8x + 5 = 0 \Rightarrow x = \frac{-8 \pm \sqrt{64 - 60}}{6} = \frac{-8 \pm 2}{6} \begin{cases} x = -1 \\ x = \frac{-10}{6} = \frac{-5}{3} \end{cases}$$

$a(-1) = 0$ y $a\left(-\frac{5}{3}\right) \neq 0$.

Por tanto -1 es la unica raiz multiple de $a(x)$.

COROLARIO

Sea $a(x) \in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$. Si $a(\alpha)=0$, $a'(\alpha)=0$, $\dots$, $a^{m-1)}(\alpha)=0$ y $a^{m)}(\alpha)\neq 0$. Entonces α es una raiz de multiplicidad m.

Ejercicio

Calcular las raices y sus multiplicidades del polinomio $a(x) = x^3+2x+3 \in \mathbb{Z}_5[x]$.

-D-

Las raices de $a(x)$ son 2 y 4.

$a'(x) = 3x^2+2$ como $a'(2)=4\neq 0$ entonces 2 es una raiz de multiplicidad 1.

Como $a'(4)=0$ entonces calculo $a''(x)=x$. Como $a''(4)=4\neq 0$ entonces 4 es una raiz de multiplicidad 2.

COROLARIO

Sea $a(x)\in \mathbb{K}[x]\setminus\{0\}$. Entonces las raices multiples de $a(x)$ son las raices de $m.c.d\{a(x), a'(x)\}$.

EJERCICIO

Calcular las raices multiples del polinomio

$x^5+x^4-5x^3-5x^2+6x+6 \in \mathbb{R}[x]$.

Sea $m(x)\in\mathbb{K}[x]\setminus\{0\}$. Denotaremos por

$\mathbb{K}[x]_{m(x)} = \{a(x)\in\mathbb{K}[x] \text{ tq } gr(a(x))<gr(m(x))\}$.

En el conjunto anterior definimos una operación $\oplus$ y una operación $\odot$ de la siguiente forma:

$$a(x)\oplus b(x) = (a(x)+b(x)) \bmod m(x)$$
$$a(x)\odot b(x) = (a(x)\cdot b(x)) \bmod m(x).$$

PROPOSICIÓN

$(\mathbb{K}[x]_{m(x)}, \oplus, \odot)$ es un anillo conmutativo.

EJERCICIO

Calcular $(x+3)\oplus(x+4)$ y $(x+3)\odot(x+4)$ en el anillo $\mathbb{Z}_5[x]_{x^2+x+1}$.

-D-

$(x+3)\oplus(x+4) = (x+3+x+4) \bmod x^2+x+1 =$

$= 2x+2 \bmod x^2+x+1 = 2x+2.$

$(x+3)\odot(x+4) = (x+3)(x+4) \bmod x^2+x+1 =$

$= x^2+2x+2 \bmod x^2+x+1 = x+1.$

$$\begin{array}{r} x+3 \\ x+4 \\ \hline x^2+3x \\ 4x+2 \\ \hline x^2+2x+2 \end{array}$$

$$\begin{array}{rl} x^2+2x+2 & \underline{|\,x^2+x+1} \\ 4x^2+4x+4 & 1 \\ \hline x+1 & \end{array}$$

PROPOSICIÓN

Sea $a(x) \in \mathbb{K}[x]_{m(x)}$. Entonces $a(x)$ es una unidad del anillo $\mathbb{K}[x]_{m(x)}$ si y sólo si $m.c.d\{a(x), m(x)\} = 1$.

EJERCICIO

¿Es $x+3$ una unidad de $\mathbb{Z}_5[x]_{x^2+x+1}$?

-D-

Vamos a calcular $m.c.d\{x^2+x+1, x+3\}$. Para ello utilizaremos el Algoritmo de Euclides.

$$(a_0(x), a_1(x)) = (x^2+x+1, x+3) = (x+3, 2) = (2, 0).$$

Entonces 2 es un m.c.d de x^2+x+1 y $x+3$. Por tanto, $2 \cdot 2 = 4$, $2 \cdot 3 = 1$ y $2 \cdot 4 = 3$ son también m.c.d de x^2+x+1 y $x+3$. Por consiguiente $m.c.d\{x^2+x+1, x+3\} = 1$ y en consecuencia $x+3$ es una unidad.

COROLARIO

$\mathbb{K}[x]_{m(x)}$ es un cuerpo si y sólo si $m(x)$ es un polinomio irreducible.

Ejercicio

¿Es $\mathbb{Z}_5[x]_{x^2+x+1}$ un cuerpo?

-D-

Como x^2+x+1 es de grado 2 y no tiene raíces, entonces es irreducible y por tanto $\mathbb{Z}_5[x]_{x^2+x+1}$ es un cuerpo.

Proposición

El cardinal de un cuerpo finito siempre es la potencia de un número primo. Además, si p es un número primo positivo y $m(x) \in \mathbb{Z}_p[x] \setminus \{0\}$ entonces $\mathbb{Z}_p[x]_{m(x)}$ tiene cardinal igual a $p^{gr(m(x))}$.

Ejercicio

¿Existen cuerpos de cardinal 10?

-D-

No ya que 10 no es la potencia de un primo.

Ejercicio

Da un cuerpo de cardinal 9.

-D-

Sabemos que $\mathbb{Z}_3[x]_{x^2+1}$ es un anillo conmutativo de cardinal 9. Como además x^2+1 es irreducible (ya que es de grado 2 y no tiene raíces) entonces $\mathbb{Z}_3[x]_{x^2+1}$ es un cuerpo de cardinal 9.

Ejercicio

Da un cuerpo de cardinal 16.

-D-

Sabemos que $\mathbb{Z}_2[x]_{x^4+x+1}$ es un anillo conmutativo de cardinal 16. Además x^4+x+1 es irreducible (ya que no tiene raíces y no lo divide ningún polinomio mónico e irreducible de grado 2) entonces $\mathbb{Z}_2[x]_{x^4+x+1}$ es un cuerpo de cardinal 16.

Los polinomios mónicos de grado 2 de $\mathbb{Z}_2[x]$ son x^2, x^2+1, x^2+x, x^2+x+1 de ellos el único que no tiene raíces es x^2+x+1. Por tanto, x^2+x+1 es el único polinomio de grado 2 mónico e irreducible de $\mathbb{Z}_2[x]$.

$$\begin{array}{l|l} x^4 \qquad\quad +x+1 & x^2+x+1 \\ \cline{2-2} x^4+x^3+x^2 & x^2+x \\ \cline{1-1} x^3+x^2+x+1 & \\ x^3+x^2+x & \\ \cline{1-1} \qquad\qquad 1 & \end{array}$$

PROPOSICIÓN

Sea $m(x)\in\mathbb{K}[x]\setminus\{0\}$ y $a(x)\in\mathbb{K}[x]_{m(x)}$. Si $\{u(x),v(x)\}\subseteq\mathbb{K}[x]$ y $a(x)u(x)+m(x)v(x)=1$, entonces $a(x)^{-1}=u(x)\bmod m(x)$.

Algoritmo extendido de Euclides

Entrada: $a(x),b(x)\in\mathbb{K}[x]\setminus\{0\}$.

Salida: $s(x),t(x),d(x)\in\mathbb{K}[x]$ t.q. $d(x)$ es un m.c.d de $a(x)$ y $b(x)$, y $a(x)s(x)+b(x)t(x)=d(x)$

$(a_0(x),a_1(x))=(a(x),b(x))$, $(s_0(x),s_1(x))=(1,0)$, $(t_0(x),t_1(x))=(0,1)$

Mientras $a_1(x)\neq 0$

$q(x)=a_0(x)\operatorname{div} a_1(x)$

$(a_0(x),a_1(x))=(a_1(x),a_0(x)-q(x)a_1(x))$, $(s_0(x),s_1(x))=(s_1(x),s_0(x)-q(x)s_1(x))$, $(t_0(x),t_1(x))=(t_1(x),t_0(x)-q(x)t_1(x))$.

Devuelve $d(x)=a_0(x)$, $s(x)=s_0(x)$ y $t(x)=t_0(x)$.

EJERCICIO

Calcula el inverso para el producto de $2x+1$ en el anillo $\mathbb{Z}_5[x]_{x^2+2x+1}$.

-D-

Como $2x+1 = 2(x+3)$ y $x^2+2x+1 = (x+1)^2$ son las descomposiciones en irreducibles, entonces $m.c.d\{2x+1, x^2+2x+1\} = 1$ y por tanto existe $(2x+1)^{-1}$. Para calcular $(2x+1)$ aplicaremos el algoritmo extendido de Euclides a x^2+2x+1 y $2x+1$.

$$(a_0(x), a_1(x)) = (x^2+2x+1, 2x+1) \overset{q(x)=3x+2}{=} (2x+1, 4) = (4, 0)$$
$$(s_0(x), s_1(x)) = (1, 0) = (0, 1) = (1, m)$$
$$(t_0(x), t_1(x)) = (0, 1) = (1, 2x+3) = (2x+3, m)$$

$$\begin{array}{l|l} x^2+2x+1 & 2x+1 \\ \cline{2-2} 4x^2+2x & 3x+2 \\ \hline 4x+1 & \\ x+3 & \\ \hline 4 & \end{array}$$

el algoritmo nos proporciona la igualdad
$$(x^2+2x+1)\cdot 1 + (2x+1)(2x+3) = 4$$
Multiplicando por 4 tenemos que
$$(x^2+2x+1)\cdot 4 + (2x+1)(3x+2) = 1.$$

Por tanto, aplicando la Proposición anterior tenemos que
$$(2x+1)^{-1} = (3x+2) \bmod x^2+2x+1 = 3x+2.$$

EJERCICIO

Resuelve en el anillo $\mathbb{Z}_7[x]_{x^2+x+1}$ la ecuación

$$(3x+4)A + 3x+1 = (2x+5)A + x+5$$

-D-

$$(3x+4)A + 3x+1 = (2x+5)A + x+5 \Rightarrow (3x+4-2x-5)A = x+5-3x-1$$

$$\Rightarrow (x+6)A = 5x+4. \Rightarrow A = (x+6)^{-1}(5x+4).$$

Como $m.c.d\{x+6, x^2+x+1\} = 1$ entonces sabemos que existe $(x+6)^{-1}$.

Vamos a calcular $(x+6)^{-1}$. Para ello utilizamos el algoritmo extendido de Euclides.

$$q(x) = x+2$$

$$(a_0(x), a_1(x)) = (x^2+x+1, x+6) \overset{\downarrow}{=} (x+6, 3) = (3, 0)$$

$$(s_0(x), s_1(x)) = (1, 0) = (0, 1) = (1, m)$$

$$(t_0(x), t_1(x)) = (0, 1) = (1, 6x+5) = (6x+5, m)$$

$$\begin{array}{r|l} x^2+x+1 & x+6 \\ \hline 6x^2+x & x+2 \\ \hline 2x+1 & \\ 5x+2 & \\ \hline 3 & \end{array}$$

$$(x^2+x+1)\cdot 1 + (x+6)(6x+5) = 3$$

$$\Downarrow \text{(multiplico por 5)}$$

$$(x^2+x+1)\cdot 5 + (x+6)(2x+4) = 1.$$

$$\Downarrow$$

$$(x+6)^{-1} = 2x+4.$$

Por tanto $A = (2x+4)(5x+4) = (3x^2+2) \bmod x^2+x+1 = \underline{\underline{4x+6}}$

$$\begin{array}{r} 5x+4 \\ 2x+4 \\ \hline 3x^2+x \quad \\ 6x+2 \\ \hline 3x^2 \quad +2 \end{array}$$

$$\begin{array}{r|l} 3x^2 \quad +2 & x^2+x+1 \\ \hline 4x^2+4x+4 & 3 \\ \hline 4x+6 & \end{array}$$