Capítulo 2

Anillo de polinomios con coeficientes en un cuerpo

En el conjunto $\mathbb{Z}$ se ha visto cómo la relación "ser congruente módulo m" para un entero $m > 1$, es compatible con las operaciones suma y producto. Esto permitió definir en el conjunto cociente $\mathbb{Z}/\equiv_m = \mathbb{Z}_m$ las operaciones

suma módulo m: $[a]+[b] = [a+b]$, con $a, b \in \mathbb{Z}$, y
producto módulo m: $[a]\cdot[b] = [a \cdot b]$, con $a, b \in \mathbb{Z}$,

sin que dependan del representante elegido.

Al ser $(\mathbb{Z}, +, \cdot)$ un anillo, lo es $(\mathbb{Z}_m, +, \cdot)$. Así + y $\cdot$ son asociativas y conmutativas en $\mathbb{Z}_m$ el producto es distributivo respeto a la suma, [0] es el elemento neutro para + y [1] es el elemento neutro para $\cdot$ en $\mathbb{Z}_m$. Además, si $-a$ es opuesto de a para + en $\mathbb{Z}$, $[-a]$ es el opuesto de $[a]$ para + en $\mathbb{Z}_m$.

Ejemplo: En $(Z, +)$ consideramos la relación "ser congruentes módulo 6", que es compatible con la suma y el producto, la tabla de las operaciones suma y producto en el conjunto cociente $\mathbb{Z}_6$ son

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Sea ahora $(K, +, \cdot)$ un cuerpo. A continuación veremos cómo las propiedades de divisibilidad (y los resultados que de ellas se deducen) en $K[x]$ son las mismas que en $\mathbb{Z}$.

Definición 2.0.1 *Un polinomio en la indeterminada x con coeficientes en K es una expresión de la forma $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ donde $a_i \in K$, para todo $0 \leq i \leq n$.*

El conjunto de polinomios en la indeterminada x con coeficientes en K se denota por $K[x]$.

Definición 2.0.2 *Sea $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ un polinomio en $K[x]$.*

1. *Si $a_i = 0$, para todo $0 \leq i \leq n$, $a(x)$ se llama polinomio cero.*

2. *Si $a(x)$ no es el polinomio cero,*

   (a) *el mayor entero s tal que $a_s \neq 0$ se llama grado del polinomio $a(x)$, denotado por $\partial a(x)$;*

   (b) *a_s se llama coeficiente principal y $a_s x^s$ término principal;*

   (c) *a_i es el coeficiente de grado i*

   (d) *$a_i x^i$ el término de grado i, para $0 \leq i \leq n$.*

3. *Un polinomio de grado 0 se llama polinomio constante.*

4. *Cuando el coeficiente principal es 1, el polinomio se llama mónico.*

5. *Dos polinomios, $a(x)$ y $b(x)$, son iguales si tienen el mismo grado y $a_i = b_i$, para todo i, $0 \leq i \leq \partial a(x) = \partial b(x)$.*

6. *Los símbolos $x, x^2, x^3, \cdots$ sólo indican las posiciones de los coeficientes, por ello, también se define un polinomio con coeficientes en un cuerpo K como una sucesión finita $(a_0, a_1, a_2, \cdots, a_n)$ de elementos de K o una aplicación $a : \mathbb{N} \to K$ tal que $a(n) = 0$, si $n > \partial a$.*

Ejemplo 2.0.3 *En $(\mathbb{Z}_5, +, \cdot)$ la expresión $3x^6 + 4x^5 + x^2 + 4x + 2$ es un polinomio de grado 6, con coeficiente principal 3 y término constante 2.*

2.1 Suma y producto en K[x]

Sean $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ y $b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ polinomios de $K[x]$. Podemos suponer que $n \geq m$, y si $n > m$ ponemos $b_{m+1} = b_{m+2} = \cdots = b_n = 0$.

Se define la suma $a(x) + b(x)$ y el producto $a(x)\cdot b(x)$ de los polinomios de la forma siguiente:

$$a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_n + b_n)x^n$$

$$a(x)\cdot b(x) = (a_0 \cdot b_0) + (a_0 \cdot b_1 + a_1 \cdot b_0)x + (a_0 \cdot b_1 + a_1 \cdot b_1 + a_2 \cdot b_0)x^2 + \cdots + a_n \cdot b_m x^{n+m}$$

Es decir, el coeficiente de x^i en $a(x) + b(x)$ es $a_i + b_i$, para cada $0 \leq i \leq n$. El coeficiente de x^i en $a(x)\cdot b(x)$ para $0 \leq i \leq n + m$, es

$$a_0 \cdot b_i + a_1 \cdot b_{i-1} + a_2 \cdot b_{i-2} + \cdots + a_i \cdot b_0 = \sum_{k=0}^{i} a_k \cdot b_{i-k} = \sum_{j+k=i} a_j \cdot b_k$$

donde las sumas y productos son las operaciones correspondientes del cuerpo K. De estas definiciones se deduce que los coeficientes de $a(x) + b(x)$ y de $a(x)\cdot b(x)$ pertenecen a K, es decir, la suma y el producto son operaciones internas en $K[x]$. Además, si $a(x) + b(x) \neq 0$ y $a(x)\cdot b(x) \neq 0$ entonces

$$\partial(a(x) + b(x)) \leq max\{\partial a(x), \partial b(x)\} \text{ y } \partial(a(x)\cdot b(x)) = \partial a(x) + \partial b(x).$$

Ejemplos:

1. Si $a(x) = 3 + 2x + 4x^2 + 4x^5$ y $b(x) = 3x + 2x^2 + 4x^3$ en $\mathbb{R}[x]$,
   $a(x)+b(x) = (3+0)+(2+3)x+(4+2)x^2+(0+4)x^3+(4+0)x^5 = 3+5x+6x^2+4x^3+4x^5$ $a(x)\cdot b(x) = (3\cdot 0)+(3\cdot 3+2\cdot 0)x+(3\cdot 2+2\cdot 3+4\cdot 0)x^2+\cdots = 16x^8+8x^7+12x^6+16x^5+16x^4+28x^3+12x^2+9x$.

2. En $\mathbb{Z}_5[x]$, si $a(x) = 3 + 2x + 4x^2 + 4x^5$ y $b(x) = 3x + 2x^2 + 4x^3$
   $a(x) + b(x) = (3 + 0) + (2 + 3)x + (4 + 2)x^2 + (0 + 4)x^3 + (4 + 0)x^5 = 3 + 1x^2 + 4x^3 + 4x^5$
   $a(x)\cdot b(x) = (3\cdot 0)+(3\cdot 3+2\cdot 0)x+(3\cdot 2+2\cdot 3+4\cdot 0)x^2+\cdots = x^8+3x^7+2x^6+x^5+x^4+3x^3+2x^2+4x$.

Observación 2.1.1 *Con estas operaciones $(K[x], +, \cdot)$ es un anillo conmutativo unitario sin divisores de cero propios, es decir, es un dominio. Sin embargo, $K[x]$ no es un cuerpo, los únicos elementos inversibles son los polinomios constantes no nulos.*

2.2 Algoritmo de división en K[x]

En cursos anteriores se aprendió a dividir polinomios con coeficientes reales, se vió cómo se obtiene el cociente y el resto. La misma técnica se aplica cuando los coeficientes de los polinomios se toman en un cuerpo K.

Proposición 2.2.1 *Algoritmo de división. Sean $a(x)$ y $b(x)$ polinomios con coeficientes en un cuerpo K, siendo $b(x) \neq 0$. Se verifica que existen polinomios únicos $q(x)$, $r(x)$ de $K[x]$ tales que*

$$a(x) = q(x)b(x) + r(x), \text{ donde } \partial r(x) < \partial b(x) \text{ ó } r(x) = 0.$$

Demostración. Para obtener la existencia, se considerará $b(x)$ fijo y se demostrará por inducción en el grado de $a(x)$.

1. Caso $\partial a(x) = 0$. Si $\partial b(x) = 0$, $b(x) = b_0 \neq 0$ y $a(x) = a_0 = (a_0 b_0^{-1})b_0 + 0$ y basta tomar $q(x) = (a_0 b_0^{-1})$ y $r(x) = 0$. Si $\partial b(x) > 0$, el resultado se cumple para $q(x) = 0$ y $r(x) = a(x)$.

2. Paso inductivo. Supongamos $\partial a(x) > 0$ y que el teorema se cumple para polinomios de grado estrictamente menor que el grado de a(x). En primer lugar, observemos que si $\partial a(x) < \partial b(x)$, el resultado se cumple para $q(x) = 0$ y $r(x) = a(x)$. Veamos el caso $\partial a(x) \geq \partial b(x)$.

   Si $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, con $a_n \neq 0$ y $b(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$, con $b_m \neq 0$, el polinomio $\alpha(x) = a(x) - a_n b_m^{-1} x^{n-m} b(x)$ cumple que $\partial\alpha(x) < \partial a(x)$. Por hipótesis de inducción, existen polinomios $\gamma(x), \rho(x)$ tales que $\alpha(x) = \gamma(x)b(x) + \rho(x)$ con $\partial\rho(x) < \partial b(x)$, o bien $\rho(x) = 0$. Así pues, $a(x) = a_n b_m^{-1} x^{n-m} b(x) + \alpha(x) = (a_n b_m^{-1} x^{n-m} + \gamma(x))b(x) + \rho(x)$ y tomando $q(x) = a_n b_m^{-1} x^{n-m} + \gamma(x)$ y $r(x) = \rho(x)$ se obtiene $a(x) = q(x)b(x) + r(x)$, donde $\partial r(x) < \partial b(x)$ ó $r(x) = 0$. Esto completa la inducción y el resultado es cierto para todos los valores de $\partial a(x)$.

Unicidad: si $a(x) = q_1(x)b(x) + r_1(x) = q_2(x)b(x) + r_2(x)$, donde $\partial r_i(x) < \partial b(x)$ o $r_i(x) = 0, (i = 1, 2)$ entonces $(q_1(x) - q_2(x))b(x) = r_2(x) - r_1(x)$. Si $q_1(x) \neq q_2(x)$, $\partial[(q_1(x) - q_2(x))b(x)] \geq \partial b(x)$, mientras que $\partial(r_2(x) - r_1(x)) \leq max\{\partial r_1(x), \partial r_2(x)\} < \partial b(x)$. Se llega así a una contradicción y, en consecuencia, $q_1(x) = q_2(x)$ y $r_1(x) = r_2(x)$.

Los polinomios $q(x)$ y $r(x)$ se llaman cociente y resto, respectivamente, de dividir $a(x)$ por $b(x)$. Nótese que la construcción de $\alpha(x)$ en la demostración indica la manera (algoritmo) de dividir dos polinomios.

Ejemplo: Si $a(x) = 5x^4 + 2x^3 + 4x^2 + 3x + 2$ y $b(x) = 3x^2 + 5$ en $(\mathbb{Z}_7[x], +, \cdot)$, el cociente es $c(x) = 4x^2 + 3x + 4$ y el resto $r(x) = 2x + 3$.

Definición 2.2.2 *Al igual que en $\mathbb{Z}$, si $a(x)$ y $b(x)$ son polinomios con coeficientes en K tales que el resto de dividir $a(x)$ por $b(x)$ es 0, se dice que $a(x)$* ***es múltiplo de*** *$b(x)$ o que $b(x)$* ***es divisor (o factor) de*** *$a(x)$; es decir, $a(x) = q(x)b(x)$ para algún $q(x)$ de $K[x]$. Se representa $b(x) \mid a(x)$.*

Ejemplos:

1. $x - 1$ es divisor de $x^2 - 1$ en $\mathbb{R}[x]$.

2. $x + 3$ es divisor de $x^2 + 1$ en $\mathbb{Z}_5[x]$ pero no lo es en $\mathbb{R}[x]$.

Definición 2.2.3 *Sean $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in K[x]$ y $\alpha \in K$, se llama valor del polinomio $a(x)$ en α al elemento de K, $a(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n \in K$. Se dice que α es* ***raíz*** *de $a(x)$ si $a(\alpha) = 0$.*

Proposición 2.2.4 *Teorema del resto.*
Sean $a(x) \in K[x]$ y $\alpha \in K$; el resto de la división de $a(x)$ por $x - \alpha$ es $a(\alpha)$.

Demostración. Por el teorema de división, $a(x) = (x - \alpha)q(x) + r(x)$ con $r = 0$ o $\partial r(x) < \partial(x - \alpha) = 1$. Por lo tanto, $r(x) = r$ es un elemento de K. Si evaluamos $a(x)$ en α se obtiene $a(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = 0 + r = r$.

Proposición 2.2.5 *Teorema del factor.*
Sean $a(x) \in K[x]$ y $\alpha \in K$; $x - \alpha$ divide a (es un factor de) $a(x)$ si, y sólo si, α es raíz de $a(x)$.

Demostración. $x - \alpha$ divide a $a(x)$ si y sólo si $r(x) = 0$ si y sólo si $a(\alpha) = 0$.
Ejemplos:

1. $a(x) = -7 + 3x - x^2 + 4x^4 - 6x^5 + x^7 \in \mathbb{Q}[x]$. El resto de dividir $a(x)$ por $x - 2$ es $a(2) = -5$ y el resto de dividir $a(x)$ por $x + 1$ es $a(-1) = -2$.
2. Si se divide $b(x) = 2 + 2x + x^2 + x^3 + 3x^4 + x^5 \in \mathbb{Z}_5[x]$ por $x + 4 = x - 1$, el resto es $b(1) = 0$ en $\mathbb{Z}_5$. En consecuencia, $x + 4$ divide a $b(x)$, es decir, $b(x) = (x + 4)q(x)$ con $\partial q(x) = 4$. El polinomio $q(x) = 3 + x + 4x^3 + x^4$, tiene a 3 como raíz, y por lo tanto, también $b(x)$, con lo cual $b(x) = (x - 1)(x - 3)(x^3 + 2x^2 + x + 4)$.

Observación 2.2.6 *Si $\alpha \in K$ es una raíz de $a(x)$, entonces $a(x) = (x - \alpha)q_1(x)$. Si α es de nuevo raíz de $q_1(x)$, entonces $q_1(x) = (x - \alpha)q_2(x)$ y así $a(x) = (x - \alpha)^2 q_2(x)$. Siguiendo este proceso se llegará a un m, con $1 \leq m \leq \partial a(x)$, tal que $a(x) = (x - \alpha)^m q_m(x)$ con $q_m(\alpha) \neq 0$ y se dice que α es raíz de multiplicidad m del polinomio $a(x)$.*

Proposición 2.2.7 *Si $a(x) \in K[x]$ tiene grado $n \geq 1$, entonces $a(x)$ tiene a lo sumo n raíces en K (considerando cada una de ellas tantas veces como indica su multiplicidad como raíz de a(x)).*

Demostración. Por inducción en $\partial a(x)$.

Ejemplos:

1. $a(x) = 9 - 6x + x^2 \in \mathbb{R}[x]$ tiene a lo sumo dos raíces, en este caso 3 es raíz de multiplicidad 2 y $a(x) = (x - 3)(x - 3)$ es una factorización de $a(x)$.
2. $a(x) = 4 + x^2 \in \mathbb{R}[x]$ no tiene raíces reales, lo que no contradice la nota anterior.
3. $a(x) = 4 + x^2 \in \mathbb{C}[x]$ tiene dos raíces complejas, $2i$ y $-2i$, se factoriza como $a(x) = (x - 2i)(x + 2i)$.
4. Si $a(x) = 6 + 2x + x^2 \in \mathbb{Z}_7[x]$, entonces $a(2) = 0$, $a(3) = 0$ y éstas son las únicas raíces del polinomio. Así, $a(x) = (x - 2)(x - 3) = (x + 5)(x + 4)$.

Observación 2.2.8 *En general, si $a(x) \in K[x]$ y $\alpha_1, \alpha_2, \cdots, \alpha_s$ son las raíces de $a(x)$ en K, entonces $a(x) = a_n(x - \alpha_1) \cdots (x - \alpha_s)q(x)$ donde a_n es el coeficiente principal de $a(x)$ y $q(x)$ un polinomio mónico sin raíces.*

2.3 Máximo común divisor de polinomios.

A partir del algoritmo de división en $K[x]$, veremos definiciones y resultados sobre divisibilidad de polinomios análogos a los ya conocidos en $\mathbb{Z}$.

Definición 2.3.1 *Dados dos polimonios $a(x)$ y $b(x)$ de $K[x]$, se dice que $d(x)$ es un máximo común divisor de $a(x)$ y $b(x)$ si*

1. *$d(x)$ es divisor de $a(x)$ y $b(x)$*
2. *todo divisor de $a(x)$ y $b(x)$ es también divisor de $d(x)$.*

Según esta definición, en general no existe un único polinomio que sea m. c. d. de dos polinomios. Si $d_1(x)$ y $d_2(x)$ verifican las condiciones 1 y 2, entonces $d_1(x) = \lambda d_2(x)$, para alguna constante λ.

De esta forma, existirá un único máximo común divisor mónico y definiremos **el máximo común múltiplo** de $a(x)$ y $b(x)$, m. c. d.$(a(x), b(x))$, como el polinomio mónico que verifica las condiciones 1 y 2.

Observemos que si $a(x) = b(x)q(x) + r(x)$ entonces

$$\text{m. c. d.}(a(x), b(x)) = \text{m. c. d.}(b(x), r(x)).$$

Teorema 2.3.2 Teorema de Bezout. *Sean $a(x), b(x) \in K[x]$, existe $d(x) = \text{m. c. d.}(a(x), b(x))$. Además existen polinomios $\lambda(x)$ y $\mu(x)$ en $K[x]$ tales que $d(x) = \lambda(x)a(x) + \mu(x)b(x)$.*

Demostración. Sea $S = \{u(x) \cdot a(x) + v(x) \cdot b(x);$ con $u(x), v(x) \in K[x]\}$. El conjunto S es distinto del vacío pues el polinomio cero, y los polinomios $a(x)$ y $b(x)$ son elementos de dicho conjunto.

De entre todos los polinomios no nulos de S, consideramos el polinomio $d(x)$ del menor grado posible. Demostraremos que $d(x)$ es un máximo común divisor de $a(x)$ y $b(x)$.

Dado que $d(x) \in S$, existen polinomios $\lambda(x)$ y $\mu(x)$ tales que $d(x) = \lambda(x) \cdot a(x) + \mu(x) \cdot b(x)$. Dividimos $a(x)$ por $d(x)$, $a(x) = q(x) \cdot d(x) + r(x)$ con $r(x) = 0$ ó $\partial r(x) < \partial d(x)$. Despejando se obtiene que:

$$\begin{aligned} r(x) &= a(x) - q(x) \cdot d(x) = a(x) - q(x) \cdot (\lambda(x) \cdot a(x) + \mu(x) \cdot b(x)) \\ &= (1 - q(x) \cdot \lambda(x))a(x) + (-q(x) \cdot \mu(x)) \cdot b(x) \in S \end{aligned}$$

Por la elección del polinomio $d(x)$ se concluye que $r(x) = 0$, es decir $d(x)|a(x)$. Análogamente se demuestra que $d(x)|b(x)$.

Por otra parte, si $d'(x)$ es un divisor de $a(x)$ y $b(x)$ entonces $d'(x)$ es un divisor de $\lambda(x) \cdot a(x) + \mu(x) \cdot b(x) = d(x)$.

Si el polinomio $d(x)$ no fuese mónico, bastará multiplicarlo por el inverso de su coeficiente principal para obtener $\text{m. c. d.}(a(x), b(x))$.

Observación 2.3.3 *Para calcular el* m. c. d. *de $a(x)$ y $b(x)$ en $K[x]$ imitaremos el método utilizado en $\mathbb{Z}$ de dividir repetidamente; éste es el algoritmo de Euclides para $K[x]$. Sean $a(x), b(x) \in K[x]$, supongamos $\partial a(x) \geq \partial b(x)$, con $b(x) \neq 0$. Llamamos $a_0(x) = a(x)$, $a_1(x) = b(x)$ y hacemos las divisiones siguientes:*

$$\begin{array}{ccc} a_0(x) = q_1(x)a_1(x) + a_2(x) & con & \partial a_2(x) < \partial a_1(x) \\ a_1(x) = q_2(x)a_2(x) + a_3(x) & & \partial a_3(x) < \partial a_2(x) \\ a_2(x) = q_3(x)a_3(x) + a_4(x) & & \partial a_4(x) < \partial a_3(x) \\ \cdots & \cdots & \cdots \\ a_{s-2}(x) = q_{s-1}(x)a_{s-1}(x) + a_s(x) & & \partial a_s(x) < \partial a_{s-1}(x) \\ a_{s-1}(x) = q_s(x)a_s(x) + 0 & & \end{array}$$

Dado que el grado de los restos decrece estrictamente, se llegará a un resto $a_{s+1}(x) = 0$. La última ecuación indica que $a_s(x)$ es divisor de $a_{s-1}(x)$; en consecuencia, $a_s(x)$ es un m. c. d. *de $a_{s-1}(x)$ y $a_s(x)$.*

Utilizando las igualdades anteriores en orden inverso se tiene:

$$\begin{aligned} a_s(x) &= \text{m. c. d.}(a_s(x), a_{s-1}(x)) = \text{m. c. d.}(a_{s-1}(x), a_{s-2}(x)) = \cdots = \text{m. c. d.}(a_2(x), a_1(x)) \\ &= \text{m. c. d.}(a_1(x), a_0(x)) = \text{m. c. d.}(a(x), b(x)). \end{aligned}$$

Entonces el último resto no nulo, $a_s(x)$, es un m. c. d. *de $a(x)$ y $b(x)$ y es un múltiplo del* m. c. d. *mónico de estos polinomios. Para obtener el* m. c. d.$(a(x), b(x))$ *bastará multiplicar $a_s(x)$ por el inverso de su coeficiente principal.*

Por substituciones sucesivas en las ecuaciones, podemos expresar $a_s(x)$ de la forma $\lambda(x)a(x) + \mu(x)b(x)$, donde $\lambda(x)$ y $\mu(x)$ son polinomios de $K[x]$. La existencia del m. c. d. de dos polinomios en $K[x]$ viene dada por el teorema de Bezout.

Ejemplos:

1. Hallar el $\text{m. c. d.}(x^3 + 2x^2 + x + 1, x^2 + 5)$ en $\mathbb{Z}_7[x]$ $x^3 + 2x^2 + x + 1 = (x + 2)(x^2 + 5) + (3x + 5)$ $x^2 + 5 = (3x + 5)(5x + 1)$. Entonces $\text{m. c. d.}(x^3 + 2x^2 + x + 1, x^2 + 5) = 3^{-1}(3x + 5) = x + 4$.

2. Hallar el $\text{m. c. d.}(x^4 + x^3 + x^2 + 1, x^4 + 1)$ en $\mathbb{Z}_2[x]$ $x^4 + x^3 + x^2 + 1 = 1.(x^4 + 1) + (x^3 + x^2)$ $x^4 + 1 = (x + 1)(x^3 + x^2) + (x^2 + 1)$ $x^3 + x^2 = (x + 1)(x^2 + 1) + (x + 1)$ $x^2 + 1 = (x + 1)(x + 1) + 0$. Entonces $\text{m. c. d.}(x^4 + x^3 + x^2 + 1, x^4 + 1) = x + 1$.

Definición 2.3.4 *Dados dos polimonios $a(x)$ y $b(x)$ de $K[x]$, se dice que $m(x)$ es* ***un mínimo común múltiplo*** *de $a(x)$ y $b(x)$ si*

1. *$m(x)$ es múltiplo de $a(x)$ y $b(x)$.*

2. *Todo múltiplo de $a(x)$ y $b(x)$ es también múltiplo de $m(x)$.*

Al igual que para el máximo común divisor, si pedimos que el polinomio $m(x)$ sea mónico se obtiene la unicidad; por ello, definiremos **el mínimo común múltiplo** de $a(x)$ y $b(x)$, $\text{m. c. m.}(a(x), b(x))$, como el polinomio mónico que verifica las condiciones 1 y 2.

El mínimo común múltiplo de dos polimonios $a(x)$ y $b(x)$ de $K[x]$, se obtiene de la siguiente igualdad

$$\text{m. c. m.}(a(x), b(x)) = \frac{a(x)b(x)}{\text{m. c. d.}(a(x), b(x))}$$

convertido en polinomio mónico si es necesario.

2.4 Polinomios irreducibles

En el estudio de los números enteros se vio cómo todo entero mayor o igual que 2, puede escribirse como producto de primos de forma única. En este apartado veremos los resultados análogos para $K[x]$, donde los primos serán los llamados polinomios irreducibles.

En primer lugar, nótese que la existencia de polinomios constantes no nulos permite factorizar trivialmente cualquier polinomio. Esto se debe a que una constante no nula α tiene inverso en K, que también es su inverso en $K[x]$; de manera que $a(x) = \alpha(\alpha^{-1}(a(x))$ es una factorización de $a(x)$ en $K[x]$. Por ese motivo los polinomios irreducibles se definen de la forma siguiente.

Definición 2.4.1 *Un polinomio $a(x) \in K[x]$ se denomina reducible si existen polinomios $b(x), c(x) \in K[x]$ con $\partial b(x), \partial c(x) \geq 1$ tales que $a(x) = b(x)c(x)$. En caso contrario, se dice que $a(x)$ es irreducible.*

Observación 2.4.2

1. *Como consecuencia de la definición, todo polinomio de grado menor o igual que 1 es irreducible.*

2. *Sea $a(x) \in K[x]$ con $\partial a(x) \geq 2$. Si $a(x)$ tiene alguna raíz en K, entonces $a(x)$ es reducible. Si $\alpha \in K$ una raíz de $a(x)$, entonces $a(x) = (x - \alpha)q(x)$ donde $\partial q(x) = \partial a(x) - 1 \geq 2 - 1 = 1$. Por lo tanto, $a(x)$ es reducible.*

3. *El recíproco no siempre es cierto; por ejemplo, $(x^2 + 1)(x^2 + 1)$ es reducible en $\mathbb{R}[x]$, pero no tiene raíces en $\mathbb{R}$.*

4. *Sin embargo, para $\partial a(x) = 2$ ó $\partial a(x) = 3$, $a(x)$ es reducible en $K[x]$ si, y sólo si, $a(x)$ tiene alguna raíz en K (o, si se prefiere, es irreducible en $K[x]$ si, y sólo si, no tiene raíces en K).*

   En efecto, si $a(x)$es reducible, $a(x) = b(x)c(x)$ con $\partial b(x), \partial c(x) \geq 1$. Como $\partial a(x) = 2$ ó 3, $\partial b(x) = 1$ ó $\partial c(x) = 1$, por lo tanto $b(x)$ ó $c(x)$ tiene una raíz en K (si $b(x) = b_0 + b_1 x$, entonces $-b_0 b_1^{-1}$ es una raíz de $b(x)$ en K).

Ejemplo 2.4.3

1. *$x^2 + 1$ es irreducible en $\mathbb{Q}[x]$ y $\mathbb{R}[x]$, pero $x^2 + 1 = (x + i)(x - i)$ y, por lo tanto, es reducible en $\mathbb{C}[x]$.*

2. *En $\mathbb{Z}_2[x]$, $a(x) = x^3 + x^2 + x + 1$ es reducible ya que $a(1) = 0$, de lo que se deduce que $a(x) = (x - 1)q(x)$. Sin embargo, $b(x) = x^2 + x + 1$ es irreducible porque $b(0), b(1) \neq 0$.*

3. *$x^4 + 3x^2 + 2 = (x^2 + 2)(x^2 + 1)$ es reducible en $\mathbb{R}[x]$, aunque no tiene raíces en $\mathbb{R}$.*

4. *El polinomio $x^4 + 1$ no tiene raíces en $\mathbb{Z}_3$, por lo que la única posible factorización sería como producto de dos polinomios de grado 2, $x^4 + 1 = (x^2 + \alpha x + \beta)(x^2 + \mu x + \delta)$. Las ecuaciones que se obtienen de la igualdad de los polinomios anteriores, permiten calcular los coeficientes: $\alpha = 1, \beta = 2, \mu = 2, \delta = 2$. Por lo tanto $x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$ y es reducible en $\mathbb{Z}_3[x]$.*

5. *El polinomio* $b(x) = x^4 + x^3 + x^2 + x + 1$ *tampoco tiene raíces en* $\mathbb{Z}_3$, *la posible factorización sería como producto de dos polinomios de grado 2,* $x^4+x^3+x^2+x+1 = (x^2+\alpha x+\beta)(x^2+\mu x+\delta)$. *Pero el sistema de ecuaciones que se obtiene de la igualdad de los polinomios anterior no tiene solución en* $\mathbb{Z}_3$, *por lo que* $b(x)$ *es irreducible en* $\mathbb{Z}_3[x]$.

Siguiendo el paralelismo con $\mathbb{Z}$, también en $K[x]$ todo polinomio no constante se puede expresar como producto de una constante (su coeficiente principal) por polinomios mónicos irreducibles de una única forma, salvo el orden de los factores. Igualmente, el m. c. d. y el m. c. m. de polinomios puede obtenerse a partir de la factorización de éstos en irreducibles.

2.5 Cuerpos finitos

Se pueden construir cuerpos finitos partiendo del anillo de polinomios $(\mathbb{Z}_p[x], +, \cdot)$.

Sea $p(x) \in K[x]$ un **polinomio mónico** fijo. Se define en $K[x]$ la siguiente relación de equivalencia:

$$a(x) \sim b(x) \Leftrightarrow p(x)\big|(a(x) - b(x)), \quad \forall a(x), b(x) \in K[x]$$

Si $a(x) \sim b(x)$ equivale a decir que existe $q(x) \in K[x]$ de modo que $a(x) - b(x) = q(x)p(x)$ o también que $a(x)$ y $b(x)$ dan el mismo resto al dividirlos por $p(x)$.

Dado que la relación definida en $K[x]$ es de equivalencia, podemos considerar el conjunto de clases que denotaremos por $K[x]/(p(x))$.

Consideremos el subconjunto de $K[x]$ formado por los posibles restos al dividir un polinomio por $p(x)$,

$$R = \{0\} \cup \{a(x) \in K[x]/\partial a(x) < \partial p(x)\}.$$

Consideremos la aplicación $K[x]/(p(x)) \xrightarrow{f} R$ dada por $f([a(x)]) = r(x)$ siendo $r(x)$ el resto de dividir $a(x)$ por $p(x)$. Se verifica que f es una aplicación biyectiva. En efecto,

1. f esta bien definida: $[a(x)] = [b(x)] \Leftrightarrow a(x) \sim b(x) \Leftrightarrow a(x), b(x)$ tienen el mismo resto al dividirlos por $p(x)$. Luego $f([a(x)]) = f([b(x)])$.

2. f es inyectiva: $f([a(x)]) = f([b(x)]) \Leftrightarrow a(x), b(x)$ tienen el mismo resto al dividirlos por $p(x) \Leftrightarrow a(x) \sim b(x) \Leftrightarrow [a(x)] = [b(x)]$.

3. f es sobreyectiva: Dado $r(x) \in K[x]/(p(x))$ consideramos la clase del propio polinomio $r(x)$ en $K[x]/(p(x))$ y tenemos que $f([r(x)]) = r(x)$.

En consecuencia $K[x]/(p(x))$ y R tienen el mismo cardinal y se podrían identificar al conjunto K^n, siendo $n = \partial p(x)$ (usando que $R = \{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1},\ a_i \in K\}$).

De hecho, al igual que pasa en $\mathbb{Z}_m$, $(K[x]/(p(x)), +, \cdot)$ tiene estructura de anillo conmutativo unitario con las operaciones

$$\begin{aligned} \text{suma:} \quad & [a(x)] + [b(x)] = [a(x) + b(x)] \\ \text{producto:} \quad & [a(x)] \cdot [b(x)] = [a(x) \cdot b(x)] \end{aligned}$$

con $a(x)$, $b(x) \in K[x]$.

En $(K[x]/(p(x)), +, \cdot)$ el producto es distributivo respeto a la suma, $[0_K]$ es el elemento neutro para $+$ y $[1_k]$ es el elemento neutro para $\cdot$ en $K[x]/(p(x))$.

Trasladando las operaciones al conjunto R, la definición de la suma sería, exactamente, la misma que la suma en $K[x]$, ya que $\partial(a(x) + b(x)) < \partial p(x)$ y la definición del producto sería el resto de dividir el producto usual $a(x) \cdot b(x)$ en $K[x]$ por el polinomio $p(x)$.

Al igual que sucede en $\mathbb{Z}_n$, los elementos de $K[x]/(p(x))$ son inversibles o son divisores de cero según sean primos con $p(x)$ como pone de manifiesto la siguiente proposición

Proposición 2.5.1 *Sea* $[a(x)] \in K[x]/(p(x))$, *se verifica que,*

1. *si* $\text{m. c. d.}(a(x), p(x)) = 1$ *entonces* $[a(x)]$ *es unidad en el anillo* $K[x]/(p(x))$.

2. *Si* $\text{m. c. d.}(a(x), p(x)) \neq 1$ *entonces* $[a(x)]$ *es un divisor de cero en el anillo* $K[x]/(p(x))$.

(Demostración similar al caso $\mathbb{Z}_m$).
De modo análogo a lo que se tenía para $\mathbb{Z}_m$, se verifica el siguiente resultado

Corolario 2.5.2 *El anillo cociente* $K[x]/(q(x))$ *es un cuerpo si y sólo si* $q(x)$ *es un polinomio irreducible. En ese caso, su característica coincide con la característica de* K.

Demostración. La primera afirmación se prueba de forma análoga al caso $\mathbb{Z}_n$. La característica de $K[x]/(q(x))$ coincide con la característica del cuerpo K pues para todo natural n se verifica que $n \cdot [1_K] = [0_K]$ si y sólo si $n \cdot 1_K = 0_K$.

Podemos describir la construcción de cuerpos finitos cuyo cardinal sea distinto de un número primo. Consideramos como cuerpo base $\mathbb{Z}_p$, siendo p un número primo y $q(x)$ un polinomio irreducible de grado n con coeficientes en $\mathbb{Z}_p$. Por lo visto anteriormente el anillo $F = \mathbb{Z}_p[x]/(q(x))$ tiene estructura de cuerpo, su cardinal es p^n y su característica es p.

Todo cuerpo finito F tiene la estructura descrita en el párrafo anterior. Es decir, si F es un cuerpo finito, su caracteristica es un número primo p y su cardinal es un potencia de p, siendo F isomorfo a un cuerpo $\mathbb{Z}_p[x]/(q(x))$ con $q(x)$ un polinomio irreducible de grado n.

Ejemplo 2.5.3

1. $p(x) = x^2 + x + 1$ *es irreducible en* $\mathbb{Z}_2[x]$, *el cuerpo* $\mathbb{Z}_2[x]/(p(x))$ *tiene* $2^2 = 4$ *elementos que son de la forma* $ax + b$ *con* $a, b \in \mathbb{Z}_2$, $\mathbb{Z}_2[x]/(x^2 + x + 1) = \{0, 1, x, 1 + x\}$. *Teniendo en cuenta que* $x^2 + x + 1 = 0$ *en el anillo cociente, se pueden facilitar los cálculos en el cociente. Por ejemplo,* $x^2 + 1 = -x = x$, *entonces* $(x + 1)(x + 1) = x^2 + 1 = x$.

2. *El mismo polinomio* $p(x) = x^2+x+1$ *no es irreducible en* $\mathbb{Z}_3[x]$, *de hecho,* $p(1) = 0$ *y* $p(x) = (x-1)^2$. *El anillo cociente* $\mathbb{Z}_3[x]/(x^2 + x + 1)$ *no es un cuerpo, como lo demuestra, entre otras cosas que* $(x - 1)(x - 1) = p(x) = 0$. *Aunque algunos elementos tienen inverso, por ejemplo,* $(x + 1)$ *ya que* $(x + 1)2x = 2x^2 + 2x = 1$ *en* $\mathbb{Z}_3[x]/(x^2 + x + 1)$.