TEMA I: EL ANILLO DE POLINOMIOS

Matemática Discreta
García Muñoz, M.A.

OBJETIVOS GENERALES

1. **Conocer la estructura algebraica de anillo.**
2. **Reconocer el anillo de polinomio, sus propiedades y operaciones.**
3. **Conocer el concepto de divisibilidad polinómica y la factorización de un polinomio y su conexión.**

OBJETIVOS ESPECÍFICOS

- ✓ **Reconocer polinomios en una variable y conocer sus términos.**
- ✓ **Saber cuando dos polinomios son iguales.**
- ✓ **Saber calcular el grado de un polinomio.**
- ✓ **Conocer la estructura algebraica de anillo.**
- ✓ **Reconocer el conjunto de los polinomios como un anillo.**
- ✓ **Conocer las unidades del anillo de polinomios.**
- ✓ **Conocer la relación de divisibilidad en el anillo de polinomios.**
- ✓ **Saber cuando un polinomio es irreducible.**
- ✓ **Saber calcular el máximo común divisor y el mínimo común múltiplo de dos polinomios.**

OBJETIVOS ESPECÍFICOS

- ✓ **Saber usar el algoritmo de la división entre polinomios.**
- ✓ **Saber calcular el máximo común divisor de dos polinomios mediante el algoritmo de Euclides.**
- ✓ **Reconocer cuando un número es una raíz de un polinomio.**
- ✓ **Saber calcular las raíces de un polinomio en los distintos anillos de polinomios.**
- ✓ **Conocer el teorema del resto y su consecuencia, el teorema del factor.**
- ✓ **Conocer la división por Ruffini de un polinomio por otro de grado 1.**
- ✓ **Conocer los criterios de factorización en los distintos anillos de polinomios.**

BIBLIOGRAFÍA

- **“Matemática discreta para la computación”. M.A. García-Muñoz. Servicio de Publicaciones Univ. Jaén. 2010. (disponible en línea)**
- **“Métodos computacionales en álgebra para informáticos: matemática discreta y lógica”. M.A. García-Muñoz, J.F. Ruiz y C. Ordóñez. Servicio de Publicaciones Univ. Jaén. 2006.**
- “Números, grupos y anillos”. J. Dorronsoro. Addison-Wesley: Universidad Autónoma de Madrid, 1999.
- “Álgebra”. J. L. Cárdenas. Grupo Editorial Patria, 2014. (disponible en línea)
- “Conjuntos numéricos, estructuras algebraicas y fundamentos del álgebra lineal”. Volumen II. R. Rodríguez Vallejo, 2013. (disponible en línea)
- “Álgebra moderna e introducción al algebra geométrica”. R. Castro Puche. Ecoe Ediciones, 2013. (disponible en línea)

DESARROLLO TEÓRICO

I.1 Introducción.
I.2 Estructuras algebraicas.
I.3 El anillo de polinomios.
I.3 Divisibilidad de polinomios.
I.4 Factorización de polinomios.

1. INTRODUCCIÓN

Al plantear en términos matemáticos problemas de distintas áreas (economía, física, ingeniería, biología, etc.), aparece el problema de determinación de los ceros de ciertas funciones, es decir, los valores para los cuales la función se anula. Después de las funciones lineales, las funciones polinómicas en una variable son las más simples.

Estudiar los ceros (raíces) de funciones polinómicas tiene un gran interés ya que muchas veces es posible traducir de alguna manera el problema original de hallar ceros de una función cualquiera al de calcular las raíces de ciertos polinomios (que “aproximan” a la función original).

2. Estructuras algebraicas

Cuando decimos que un conjunto está dotado de **estructura algebraica** entendemos que en dicho conjunto tenemos definidas una o varias operaciones o leyes de composición internas que satisfacen diversas propiedades.

Un **grupo** G es un conjunto no vacío junto con una ley de composición interna * como en la definición anterior que satisface:

i) la propiedad asociativa,
ii) la existencia de elemento neutro y
iii) la existencia de elemento simétrico para todo elemento de G, es decir, $\forall a \in G$ existe $a' \in G$ tal que $a * a' = e = a' * a$.

Si, además, dicha operación satisface la propiedad conmutativa, se dice que es un **grupo abeliano** o **conmutativo**.

Un **anillo** A es un conjunto no vacío con dos leyes de composición internas + y ·, usualmente llamadas adicción y multiplicación

$$+ : A \times A \longrightarrow A \qquad \cdot : A \times A \longrightarrow A$$
$$(a, b) \longmapsto a + b \qquad (a, b) \longmapsto a\,b = a \cdot b$$

verificando que A junto con la operación + tiene estructura de grupo abeliano, es decir, satisface las propiedades asociativa, existencia de elemento neutro (en el caso de la adición llamado **cero**), existencia de elemento simétrico (en el caso de la adición llamado **opuesto**) y conmutativa, y la operación · satisface las propiedades asociativa y distributivas respecto de la ley +, es decir, $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(a + b) \cdot c = a \cdot c + b \cdot c$ para cualesquiera $a, b, c \in A$.

Si, además, la operación $\cdot$ tiene elemento neutro, es decir, existe un elemento $u \in A$ tal que $a \cdot u = a = u \cdot a$ para cualquier $a \in A$, diremos que el anillo A es un **anillo unitario**.

Por otra parte, diremos que A es un **anillo conmutativo** si la segunda operación satisface la propiedad conmutativa ($a \cdot b = b \cdot a, \forall a, b \in A$).

Un **dominio de integridad** es un anillo que no posee divisores de cero, es decir, si $a \cdot b = 0$ entonces $a = 0$ ó bien $b = 0$.

Si A es un anillo con elemento unidad u, diremos que un elemento $a \in A$ distinto del elemento cero es **invertible**, si existe otro elemento $a^{-1} \in A$ tal que $a \cdot a^{-1} = u = a^{-1} \cdot a$.

Por último, un anillo A para el que todo elemento distinto del neutro para la primera operación (distinto del cero) es invertible, diremos que es un **cuerpo**. Si, además, el anillo es conmutativo entonces diremos que A es un **cuerpo conmutativo**.

Proposición 1.1. Todo cuerpo es un dominio de integridad, es decir, no tiene divisores de cero.

3. El anillo de polinomios

Sea A un anillo, y sea $x \notin A$ una **indeterminada**.

Llamaremos **polinomio** en la indeterminada x con coeficientes en el anillo A a toda expresión del tipo:

$$p(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n,$$

donde $a_i \in A$ para i = 0, 1,..., n. Cada polinomio se suele denotar por p(x), q(x), r(x), etc. Al conjunto de todos los polinomios en x con coeficientes en A lo denotamos por A[x].

Dado un polinomio no nulo $p(x) = a_0 + a_1 \cdot x + ... + a_n \cdot x^n \in A[x]$, al mayor valor $n \in A$ para el cual $a_n \neq 0$, recibe el nombre de **grado** del polinomio p(x) y lo denotaremos por gr(p(x)) = n. A tal $a_n \neq 0$ lo llamaremos **coeficiente líder del polinomio**. Además llamaremos **término independiente** de p(x) al coeficiente a_0. Diremos que p(x) es **mónico** si el coeficiente líder $a_n = 1$.

Llamamos **monomio** a un polinomio en el que un único coeficiente es distinto de cero. Diremos que dos monomios en A[x] son **semejantes** si ambos tienen el mismo grado.

Diremos que un polinomio p(x) es **constante** si gr(p(x)) = 0. Por convenio, se considera que el grado del polinomio p(x) = 0 es $-\infty$.

Diremos que un polinomio es **completo** de grado n si todos sus coeficientes son distintos de cero desde el término independiente hasta el coeficiente líder de grado n ambos inclusive.

Dados dos polinomios $p(x) = a_0 + a_1 x + ...+ a_m x^m$ y $q(x) = b_0 + b_1 x +...+ b_n x^n$ en A[x], diremos que son **iguales**, p(x) = q(x), si n = m (tienen el mismo grado) y $a_i = b_i$ para todo i = 0, 1,..., n.

Dados los polinomios

$$p(x) = a_0 + a_1 x + \ldots + a_m x^m \quad y \quad q(x) = b_0 + b_1 x + \ldots + b_n x^n$$

en A[x], definimos la **suma** de ambos como un nuevo polinomio en A[x], que vendrá dado por:

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1) x + \ldots + (a_r + b_r) x^r$$

donde $r = \max\{m, n\}$.

Proposición 1.2.

$$gr(p(x) + q(x)) \leq \max\{gr(p(x)), gr(q(x))\}$$

Proposición 1.3. Sea A un anillo, entonces A[x] junto con la operación anterior tiene estructura de grupo abeliano.

Ejercicio 1. Calcular, en cada caso, p(x) + q(x) y su grado.

a) $p(x) = x^3 - 3x + 2$ y $q(x) = x^2 + 5x - 3$ en $\mathbb{Z}[x]$,

b) $p(x) = 2x^3 - 3x^2 + 2x + 1$ y $q(x) = 3x^3 + 5x - 1$ en $\mathbb{Z}_5[x]$,

Por otra parte, definimos el **producto** de los polinomios

$p(x) = a_0 + a_1 x + \ldots + a_m x^m$ y $q(x) = b_0 + b_1 x + \ldots + b_n x^n$

en A[x], como un nuevo polinomio en A[x] que denotaremos p(x) q(x) y que vendrá dado por:

$$p(x)\,q(x) = (a_0 b_0) + (a_0 b_1 + a_1 b_0)\,x + \ldots + \left(\sum_{i+j=k} a_i a_j\right)x^k + \ldots + (a_m b_n)\,x^{m+n}$$

Proposición 1.4. gr(p(x) q(x)) ≤ gr(p(x)) + gr(q(x)). Además se da la igualdad si y sólo si A es un dominio de integridad.

Proposición 1.5. Sea A un anillo, entonces A[x] junto con las dos operaciones suma y producto anteriores tiene estructura de anillo. Si, además, A es conmutativo, entonces A[x] es un anillo conmutativo.

Ejercicio 2. Para los polinomios del ejercicio anterior calcular, en cada caso, p(x) q(x) y su grado.
Dar un ejemplo donde gr(p(x) q(x)) < gr(p(x)) + gr(q(x)).

Proposición 1.6.

- Si A es un dominio de integridad, entonces A[x] es también un dominio de integridad.
- Si A es un cuerpo, entonces A[x] es un dominio de integridad.

Proposición 1.7. Si A es un dominio de integridad, entonces el conjunto de unidades de A[x] y de A coinciden, es decir, los únicos polinomios de A[x] que tienen inverso son los polinomios constantes (o lo que es igual los elementos de A) que tienen inverso.

Observación: Si A es un anillo, entonces existe una aplicación inyectiva de $A \longrightarrow A[x]$.

Ejercicio 3. Comprobar que $2x^2 + 1 \in \mathbb{Z}_4[x]$ es una unidad cuyo inverso es el mismo.

3. Divisibilidad de polinomios

Dados $p(x), q(x) \in A[x]$. Diremos que $p(x)$ es **divisor** de $q(x)$, y lo representamos mediante $p(x) \mid q(x)$, si y sólo si existe un polinomio $c(x) \in A[x]$ tal que $p(x)\, c(x) = q(x)$, es decir,

$$p(x) \mid q(x) \Leftrightarrow \exists c(x) \in A[x] \text{ tal que } p(x)\, c(x) = q(x)$$

En tal caso también se dice que $p(x)$ **divide** a $q(x)$, $p(x)$ es **factor** de $q(x)$ o bien que $q(x)$ es **múltiplo** de $p(x)$.

Proposición 1.8. La relación de divisibilidad en $A[x]$ es reflexiva y transitiva, es decir, es un preorden. Sin embargo, esta relación binaria no es simétrica ni antisimétrica.

Ejercicio 4. Dados $p(x), q(x) \in A[x]$ con A un dominio de integridad, demostrar que si $p(x) \mid q(x)$ entonces $gr(p(x)) \leq gr(q(x))$. Comprobar que lo anterior no es cierto para $p(x) = 2x^2 + 1$ y $q(x) = 2x + 2$ en $\mathbb{Z}_4[x]$, ¿por qué?

Diremos que dos polinomios $p(x), q(x) \in A[x]$ son **asociados** si se diferencian en el producto por unidades, es decir, existe una unidad $u(x)$ en $A[x]$ tal que $p(x) = q(x)\, u(x)$.

Si A es un dominio de integridad, $p(x)$ y $q(x)$ son **asociados** si existe $u \in A$ (unidad en $A[x]$) tal que $p(x) = q(x) \cdot u$.

Ejercicio 5. Comprobar que los polinomios $p(x), q(x) \in A[x]$ son asociados:

a) $p(x) = 2x^2 + 3x+4$ y $q(x) = x^2 + 5x + 2$ en $\mathbb{Z}_7[x]$,

b) $p(x) = 2x^3 + 3x - 1$ y $q(x) = -x^3 - \frac{3}{2}x + \frac{1}{2}$ en $\mathbb{R}[x]$, y

c) $p(x) = 2x^2 + 2x + 1$ y $q(x) = 2x + 1$ en $\mathbb{Z}_4[x]$.

Proposición 1.9. La relación de divisibilidad satisface:

1. El polinomio cero es múltiplo de cualquier polinomio en $A[x]$.
2. Las unidades de A son divisores de todo polinomio en $A[x]$.
3. Todo polinomio $p(x) \in A[x]$ es divisible por $(u\, p(x))$ para cualquier unidad $u \in A$.

Veamos ahora un concepto análogo al de número primo en $\mathbb{Z}$:

Un polinomio $p(x) \in A[x]$, no nulo y no unidad, se dice **irreducible** en $A[x]$ si su único divisor, salvo asociados, es el mismo, es decir, si $p(x) = p_1(x)\, p_2(x)$, entonces $p_1(x)$ o $p_2(x)$ es una unidad en $A[x]$. En otro caso diremos que $p(x)$ es **reducible** en $A[x]$, o sea, se puede descomponer en producto de polinomios de grado inferior que pertenecen a $A[x]$.

Observación: Todo polinomio de grado 1 es irreducible en $\mathbb{K}[x]$, con $\mathbb{K}$ un cuerpo cualquiera.

Ejercicio 6. Comprobar que el polinomio $x^2 - 3$ es irreducible en $\mathbb{Z}[x]$, pero es reducible en $\mathbb{R}[x]$.

Si cada uno de los polinomios en los que se descompone un polinomio reducible es irreducible tenemos una descomposición de p(x) en producto de polinomios irreducibles; en otro caso, alguno de los nuevos polinomios se podrá escribir como producto de otros dos polinomios que no sean unidades en A[x]. Este proceso es finito, nunca podremos aplicar este proceso de descomposición más veces que el grado del polinomio, y al finalizarlo obtendremos una descomposición de p(x) en producto de polinomios irreducibles.

Ejercicio 7. Comprobar que el polinomio $x^2 + x + 1$ es irreducible en $\mathbb{R}[x]$, pero es reducible en $\mathbb{C}[x]$.

Un dominio de integridad A es un **dominio de factorización única (DFU)** si todo elemento de A, no nulo ni unidad, tiene una factorización, única salvo el orden y producto por unidades, en elementos irreducibles.

Teorema 1.10. (Teorema de factorización única) Sea A un DFU. Todo polinomio p(x) en A[x] distinto del polinomio cero admite una descomposición única (salvo el orden y asociados) como un elemento de A por un producto de polinomios mónicos irreducibles en A[x], es decir:

$$p(x) = a\, p_1(x)^{\alpha_1} p_2(x)^{\alpha_2} \ldots p_r(x)^{\alpha_r}$$

donde $a \in A$, para todo $i = 1, 2, \ldots, r$, $p_i(x)$ son polinomios mónicos irreducibles distintos en A[x] tales que $gr(p_i(x)) < gr(p_j(x))$ si $i < j$ y α_i son números naturales. A la expresión de p(x) anterior se le conoce como **descomposición en factores irreducibles** de dicho polinomio.

Los conceptos de máximo común divisor y mínimo común múltiplo son análogos en el anillo de polinomios:

Dados $p(x), q(x) \in A[x]$. Llamaremos **máximo común divisor** de $p(x)$ y $q(x)$ al un polinomio $d(x) \in A[x]$ que satisface:

i) $d(x) \mid p(x)$ y $d(x) \mid q(x)$, es decir, $d(x)$ es un divisor de $p(x)$ y de $q(x)$.

ii) Si existe $d'(x) \in A[x]$ tal que $d'(x) \mid p(x)$ y $d'(x) \mid q(x)$, entonces $d'(x) \mid d(x)$.

Al máximo común divisor de $p(x)$ y $q(x)$ lo denotamos por:

$$d(x) = (p(x), q(x)) = \text{mcd}\{p(x), q(x)\}.$$

Diremos que $p(x), q(x) \in A[x]$ son **primos relativos** si $\text{mcd}\{p(x), q(x)\}$ es una unidad en A.

Dados $p(x), q(x) \in A[x]$. Llamaremos **mínimo común múltiplo** de $p(x)$ y $q(x)$ al polinomio $m(x) \in A[x]$ que satisface:

i) $p(x) \mid m(x)$ y $q(x) \mid m(x)$, es decir, $m(x)$ es un múltiplo de $p(x)$ y de $q(x)$.

ii) Si existe $m'(x) \in A[x]$ tal que $p(x) \mid m'(x)$ y $q(x) \mid m'(x)$, entonces $m(x) \mid m'(x)$.

Al mínimo común múltiplo de $p(x)$ y $q(x)$ lo denotamos por:

$$m(x) = [p(x), q(x)] = \text{mcm}\{p(x), q(x)\}.$$

De forma análoga podemos definir el máximo común divisor y mínimo común múltiplo de n polinomios $p_1(x), p_2(x),..., p_n(x) \in A[x]$ con $n > 2$.

Nótese que ambos son únicos salvo asociados, es decir, salvo producto por unidades.

De nuevo el teorema de factorización única (teorema 1.10.) proporciona un método de cálculo del máximo común divisor y del mínimo común múltiplo de dos polinomios a partir de su descomposición en factores irreducibles.

Proposición 1.11. Dados p(x) y q(x) $\in$ A[x], no unidades en A y no nulos tales que:

$$p(x) = a\, p_1(x)^{\alpha_1} p_2(x)^{\alpha_2} \ldots p_r(x)^{\alpha_r}$$

$$q(x) = b\, p_1(x)^{\beta_1} p_2(x)^{\beta_2} \ldots p_r(x)^{\beta_r}$$

con $\alpha_i, \beta_j \geq 0$, $\forall i = 1, 2, \ldots, r$. Entonces:

$$d(x) = (p(x), q(x)) = (a, b)\, p_1(x)^{f_1} p_2(x)^{f_2} \ldots p_r(x)^{f_r}$$

con $f_i = \min\{\alpha_i, \beta_i\}$ $\forall i = 1, 2, \ldots, r$ y

$$m(x) = [p(x), q(x)] = [a, b]\, p_1(x)^{g_1} p_2(x)^{g_2} \ldots p_r(x)^{g_r}$$

con $g_i = \max\{\alpha_i, \beta_i\}$ $\forall i = 1, 2, \ldots, r$.

Si p(x) y q(x) $\in \mathbb{K}[x]$, con $\mathbb{K}$ un cuerpo, teniendo en cuenta que todo elemento no nulo en $\mathbb{K}$ es una unidad, podemos desechar el máximo común divisor y el mínimo común múltiplo de a y b.

De hecho, el mcd{p(x), q(x)} es el producto de los factores irreducibles mónicos que aparecen en común en las factorizaciones de p(x) y q(x), elevados a la mínima potencia con la que aparecen y el mcm{p(x), q(x)} es el producto de los factores irreducibles mónicos comunes y no comunes que aparecen en las factorizaciones de p(x) y q(x), elevados ahora a la máxima potencia con la que aparecen.

$$d(x) = (p(x), q(x)) = p_1(x)^{f_1} p_2(x)^{f_2} \ldots p_r(x)^{f_r}$$

$$m(x) = [p(x), q(x)] = p_1(x)^{g_1} p_2(x)^{g_2} \ldots p_r(x)^{g_r}$$

con $f_i = \min\{\alpha_i, \beta_i\}$ y $g_i = \max\{\alpha_i, \beta_i\}$ $\forall i = 1, 2, \ldots, r$.

El siguiente teorema nos permite también calcular el mínimo común múltiplo de dos polinomios p(x) y q(x) a partir del máximo común divisor:

Teorema 1.12. Sean p(x) y q(x) $\in$ A[x], entonces

$$[p(x), q(x)]\,(p(x), q(x)) = p(x)\,q(x).$$

Veamos ahora el teorema que nos permite dividir en el anillo de polinomios:

Teorema 1.13. (Algoritmo de la división) Sea A un anillo y p(x), q(x) $\in$ A[x] con q(x) $\neq$ 0 y con coeficiente líder una unidad. Entonces existen polinomios c(x) y r(x) únicos, ambos en A[x], tales que

$$p(x) = q(x)\,c(x) + r(x)$$

y gr(r(x)) < gr(q(x)). A c(x) lo llamamos **cociente** y a r(x) **resto**.

Corolario 1.14. En el anillo de polinomios $\mathbb{K}[x]$, con $\mathbb{K}$ un cuerpo, podemos aplicar el algoritmo de la división a cualquier par de polinomios siempre y cuando uno de ellos sea no nulo.

Ejercicio 8. ¿Es posible aplicar el algoritmo de la división a los polinomios $p(x) = 2x^2 + 2x + 3$ y $q(x) = 3x - 3$ en $\mathbb{Z}[x]$? ¿y en $\mathbb{Q}[x]$? En caso afirmativo, obtener cociente y resto de la división.

Ejercicio 9. ¿Es posible aplicar el algoritmo de la división a los polinomios $p(x) = 3x^2 + 2x + 3$ y $q(x) = 2x + 1$ en $\mathbb{Z}_4[x]$? ¿y en $\mathbb{Z}_3[x]$? En caso afirmativo, obtener cociente y resto de la división.

Lema 1.15. Dados $p(x), q(x) \in A[x]$, y $q(x) \neq 0$ con coeficiente líder una unidad. Si $p(x) = q(x)\, c(x) + r(x)$ con $c(x), r(x) \in A[x]$ los polinomios cociente y resto obtenidos al aplicar el algoritmo de la división a $p(x)$ y $q(x)$, entonces

$$\text{mcd}\{p(x), q(x)\} = \text{mcd}\{q(x), r(x)\}.$$

El resultado anterior nos permite obtener el **algoritmo de Euclides**. En el caso de los polinomios nos encontramos con la salvedad de que dos polinomios no siempre se podrán dividir en A[x] con A un anillo (es necesario que el coeficiente líder del divisor sea una unidad). Sin embargo, si A es un cuerpo esta salvedad desaparece y el algoritmo que vimos para números enteros puede adaptarse para polinomios utilizando como función euclídea el grado en lugar del valor absoluto.

Dados $p(x), q(x) \in A[x] - \{0\}$, sin perdida de generalidad podemos suponer que $gr(p(x)) \geq gr(q(x))$, en otro caso sólo tendríamos que renombrarlos. Aplicando el algoritmo de la división obtenemos dos polinomios $c_1(x)$ y $r_1(x)$ satisfaciendo:

$$p(x) = q(x)\, c_1(x) + r_1(x) \text{ con } gr(r_1(x)) < gr(q(x)),$$

con lo que reducimos el problema de calcular el $mcd\{p(x), q(x)\}$ al cálculo del $mcd\{q(x), r_1(x)\}$ que son polinomios de grado menor. De hecho, puede ocurrir que:

- $r_1(x) = 0$, entonces $mcd\{p(x), q(x)\} = mcd\{q(x), 0\} = q(x)$.
- $r_1(x) \neq 0$, en cuyo caso podemos volver a aplicar el algoritmo de la división a $q(x)$ y $r_1(x)$ y obtendríamos:

$$q(x) = r_1(x)\, c_2(x) + r_2(x) \text{ con } gr(r_2(x)) < gr(r_1(x)).$$

y el problema de nuevo se reduce a calcular el $mcd\{r_1(x), r_2(x)\}$, pudiendo ocurrir que:

- $r_2(x) = 0$, y entonces $\text{mcd}\{ p(x), q(x)\} = \text{mcd}\{ q(x), r_1(x)\} = \text{mcd}\{r_1(x), 0\} = r_1(x)$, o
- $r_2(x) \neq 0$, y así podríamos volver a aplicar el algoritmo de la división ahora entre $r_1(x)$ y $r_2(x)$, obteniendo

$$r_1(x) = r_2(x)\, c_3(x) + r_3(x) \text{ con } gr(r_3(x)) < gr(r_2(x)).$$

Así sucesivamente se irían calculando sucesivas divisiones entre polinomios con restos cada vez de menor grado. De hecho, los grados de tales polinomios

$$gr(r_1(x)) > gr(r_2(x)) > gr(r_3(x)) > \ldots,$$

constituyen una sucesión de números naturales decrecientes y acotada por el 0, tras un número finito de pasos obtendremos un resto igual a $r_s(x) = 0$, es decir, $r_{s-1}(x)$ divide a $r_{s-2}(x)$:

……

$$r_{s-3}(x) = r_{s-2}(x)\, c_{s-1}(x) + r_{s-1}(x) \text{ con } gr(r_{s-1}(x)) < gr(r_{s-2}(x)),$$

$$r_{s-2}(x) = r_{s-1}(x)\, c_s(x) + 0.$$

y así se tiene:

$\mathrm{mcd}\{p(x), q(x)\} = \mathrm{mcd}\{q(x), r_1(x)\} = \mathrm{mcd}\{r_1(x), r_2(x)\} = \ldots =$
$\mathrm{mcd}\{r_{s-2}(x), r_{s-1}(x)\} = \mathrm{mcd}\{r_{s-1}(x), 0\} = r_{s-1}(x),$

es decir, el máximo común divisor de $p(x)$ y $q(x)$ vendrá dado por el último resto distinto de 0.

Ejercicio 10. Aplicar el algoritmo de Euclides para calcular el máximo común divisor de $p(x) = 2x^3 - 3x^2 - x + 1$ y $q(x) = 2x^2 + x - 1$ en $\mathbb{R}[x]$.

Ejercicio 11. ¿Es posible aplicar el algoritmo de Euclides para calcular el máximo común divisor de $p(x) = x^5 + 2x^3 + 2x + 3$ y $q(x) = 3x^2 + 2$ en $\mathbb{Z}_8[x]$? ¿Y en $\mathbb{Z}_7[x]$? Cuando sea posible, obtener también el mínimo común múltiplo de ambos.

4. Factorización de polinomios

Matemática Discreta
García Muñoz, M.A.

Sea A un anillo y $p(x) = a_0 + a_1 x + ... + a_n x^n \in A[x]$. Llamaremos **valor numérico** del polinomio p(x) en a, al valor que se obtiene al sustituir la variable x por el valor a en el polinomio, es decir, $p(a) = a_0 + a_1 a + ... + a_n a^n \in A$.

Diremos que $a \in A$ es una **raíz** o un **cero del polinomio** p(x) si el valor numérico de p(x) en a es cero, esto es, p(a) = 0.

Diremos que un entero positivo k es la **multiplicidad (algebraica)** de a si p(x) es divisible por $(x - a)^k$ y no lo es por $(x - a)^{k+1}$. Cuando k = 1, decimos que a es una **raíz simple** del polinomio p(x) y en caso contrario diremos que la a es una **raíz múltiple**.

Ejercicio 12. Dado $p(x) = x^2 + 5x$ en $\mathbb{Z}_6[x]$. Comprobar que $\overline{0}$, $\overline{1}$, $\overline{3}$ y $\overline{4}$ son raíces de p(x).

Teorema 1.16. (Teorema del resto) Sea A un anillo y $p(x) \in A[x]$, entonces para todo $a \in A$ existe un único polinomio $c(x) \in A[x]$ tal que $p(x) = c(x)(x - a) + p(a)$.

Corolario 1.17. (Teorema del factor) Sea A un anillo y $p(x) \in A[x]$ un polinomio en x. Un elemento $a \in A$ es una raíz de p(x) si y sólo si $(x - a) \mid p(x)$.

Teorema 1.18. Sea A un dominio de integridad y $p(x) \in A[x]$. Si $x_1, x_2, ..., x_k$ son k raíces distintas de p(x) entonces

$$((x - x_1)(x - x_2)...(x - x_k)) \mid p(x).$$

Corolario 1.19. Sea A un dominio de integridad y $p(x) \in A[x]$. Se tiene:

i) Si p(x) tiene k raíces distintas entonces $gr(p(x)) \geq k$.

ii) Si $gr(p(x)) = k$, entonces tiene a lo sumo k raíces.

Ejercicio 13. Observar, a través del ejercicio anterior, que lo que nos asegura el corolario 1.19. no es cierto si A no es un dominio de integridad.

Corolario 1.20. Si A es un dominio de integridad, $p(x) \in A[x]$ es un polinomio de grado n y $x_1, x_2, ..., x_n$ son sus raíces en A, entonces $p(x) = a_n (x - x_1) (x - x_2) ... (x - x_n)$ donde a_n es el coeficiente líder de p(x).

Factorización y cálculo de raíces en $\mathbb{Z}[x]$:

Proposición 1.21. Un número entero $a \in \mathbb{Z}$ es una raíz de q(x) si es divisor de su término independiente.

Factorización y cálculo de raíces en $\mathbb{Z}[x]$:

Dado $p(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}[x]$, tratamos de factorizarlo calculando para ellos las raíces enteras de $p(x)$.

Paso 1: Sacar factor común los factores que aparezcan en todos los términos del polinomio. Así

$$p(x) = b\, x^i (b_0 + b_1 x + \ldots + b_r x^r)$$

Paso 2: Tras lo anterior tendremos un polinomio sin factorizar $q(x) = b_0 + b_1 \cdot x + \ldots + b_r \cdot x^r$ con término independiente $b_0 \neq 0$. Factorizamos $q(x)$ buscando sus raíces entre los divisores enteros de b_0, lo podemos hacer usando la **regla de Ruffini** que nos permite dividir $q(x)$ entre el binomio $(x - a)$.

Paso 3: Una vez encontrada una raíz entera x_0 el polinomio $q(x)$ se descompone mediante $q(x) = (x - x_0)\, c(x)$, luego

$$p(x) = b\, x^i (x - x_0)\, c(x).$$

Factorización y cálculo de raíces en $\mathbb{Z}[x]$:

Paso 4: Continuaríamos buscando raíces ahora de c(x), volveríamos a probar con x_0 por si es una raíz múltiple del polinomio y con el resto de divisores de b_0 que no hubiesen sido descartados como raíz previamente, hasta agotar todos los divisores. Cuando el polinomio no tenga más raíces enteras concluiremos la factorización.

Puede ocurrir que el polinomio no tenga raíces enteras y pueda factorizarse como producto de polinomios de grado mayor o igual a 2. En este caso es difícil obtener la factorización y la forma de hacerlo dependerá de cada caso. Por ejemplo, **polinomio bicuadrado**: $(ax^4 + bx^2 + c)$, podemos factorizarlo realizando el cambio de variable $t = x^2$.

Ejercicio 14. Factorizar en $\mathbb{Z}[x]$el polinomio:

$$p(x) = 2x^6 - 2x^5 - 4x^4 + 4x^3 - 6x^2 + 6x$$

Factorización y cálculo de raíces en $\mathbb{Q}[x]$:

Proposición 1.22. (Teorema de Descartes) Si p(x) tiene coeficientes enteros, un número racional $\frac{a}{b} \in \mathbb{Q}$, con (a, b) = 1, es una raíz de p(x) si a es divisor del término independiente a_0 de p(x) y b es divisor del coeficiente líder a_n de p(x).

Corolario 1.23. Todo polinomio mónico con coeficientes enteros carece de raíces racionales.

Ejercicio 15. Factorizar en $\mathbb{Q}[x]$ los polinomios:

$$p(x) = 6x^3 - 5x^2 - 3x + 2 \quad \text{y} \quad q(x) = 2x^5 + \frac{7}{3}x^4 + \frac{5}{3}x^3 + \frac{5}{3}x^2 - \frac{1}{3}x - \frac{2}{3}$$

Usar lo anterior para calcular m.c.d.{p(x), q(x)} y m.c.m.{p(x), q(x)}.

Factorización y cálculo de raíces en $\mathbb{R}[x]$ y en $\mathbb{C}[x]$:

Proposición 1.24. Si $p(x) = x^2 + b\,x + c$ es un polinomio mónico de grado 2 en $\mathbb{R}[x]$, entonces $p(x)$ es irreducible si y sólo si $b^2 - 4\,c$ es menor que cero.

Proposición 1.25. Si un número complejo $a + bi \in \mathbb{C}$ es una raíz de un polinomio $p(x)$ con coeficiente reales entonces su conjugado $a - bi$ también es una raíz de $p(x)$.

Teorema 1.26. Cualquier polinomio $p(x) \in \mathbb{C}[x]$ de grado n tiene n raíces en $\mathbb{C}$ teniendo en cuenta las multiplicidades.

Ejercicio 16. Factorizar en $\mathbb{R}$ [x] y en $\mathbb{C}[x]$ el polinomio $p(x)$ del ejercicio 14.

Factorización y cálculo de raíces en $\mathbb{Z}_n[x]$:

Primero observamos si n es o no un número primo: si lo es $\mathbb{Z}_n$ es un D. I., y la factorización será única, en otro caso, la factorización no será única.

Como los anillos $\mathbb{Z}_n$ son finitos, buscaremos una raíz del polinomio evaluando p(x) en sus elementos:

Cuando encontremos un elemento $\overline{a}$ tal que $p(\overline{a}) = \overline{0}$, dividimos p(x) entre $(x - \overline{a})$, para obtener el cociente c(x) tal que $p(x) = (x - \overline{a})\, c(x)$, (regla de Ruffini teniendo en cuenta que los coeficientes son elementos de $\mathbb{Z}_n$).

Tras obtener c(x) volveríamos a probar si $\overline{a}$ es de nuevo raíz de c(x), en otro caso, continuaríamos probando con los demás elementos de $\mathbb{Z}_n$ hasta encontrar otra raíz y procederíamos como antes hasta acabar con los elementos de $\mathbb{Z}_n$ o bien factorizar totalmente p(x).

Ejercicio 17. Calcular las raíces y factorizar $p(x) = x^5 + x^3 + 13\,x + 5$ en $\mathbb{Z}_5[x]$.

Ejercicio 18. Calcular el máximo común divisor y el mínimo común múltiplo de los polinomios $p(x) = x^5 - x^3 + 13x - 6$ y $q(x) = x^4 + 8x^2 + 5$ en $\mathbb{Z}_7[x]$.