Universidad de Jaén

Grado en Ingeniería Informática
ÁLGEBRA

TEMA 1. EL ANILLO DE LOS POLINOMIOS

Grado en Ingeniería Informática
TEMA 1. EL ANILLO DE LOS POLINOMIOS

Bibliografía básica:

Métodos computacionales en álgebra para informáticos: matemática discreta lógica. Edición: -. Autor: García Muñoz, Miguel A., Ordóñez Cañada, Carmen, Ruiz Ruiz, JF. Editorial: [Jaén]: Área de Álgebra, Universidad de Jaén, 2006

Números, grupos y anillos. Edición: 2ª reimp.. Autor: Dorronsoro, José. Editorial: Madrid [etc.]: Addison-Wesley: Universidad Autónoma de Madrid, 1999

Grado en Ingeniería Informática
TEMA 1. EL ANILLO DE LOS POLINOMIOS

ÍNDICE:

1. El anillo de los polinomios
2. Divisibilidad de polinomios
3. Factorización de polinomios

Definiciones. Sea A un anillo, $x \notin A$. Llamamos *polinomio con coeficientes en A en la indeterminada x*, a toda expresión formal del tipo

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

donde $a_0, a_1, a_2 \ldots a_n \in A$, $n \geq 0$.

- Dos polinomios $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ y $q(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m$ son *iguales* sii $n=m$ y $a_i=b_i$ para todo $i=1,\ldots, n$
- El *grado* del polinomio es:
    - el mayor n, para el que $a_n \neq 0$;
    - $gr(0) = -\infty$
- Si $p(x)$ es de grado n, el coeficiente líder (a_n) y término independiente(a_0).
- Polinomio mónico y polinomio constante

- Operaciones algebraicas con polinomios (Anillo):

  -Suma (cero y opuestos)

  Si $p(x)$ y $q(x)$ son polinomios no nulos, entonces

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

  -Producto (uno y unidades)

  Si $p(x)$ y $q(x)$ son polinomios no nulos, entonces

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

Proposición. Si $p(x), q(x) \in A[x]$, no nulos, entonces

$$\mathrm{gr}(p(x)q(x)) = \mathrm{gr}(p(x))+\mathrm{gr}(q(x)) \text{ sii } A \text{ es D.I}$$

Proposición. Sea A un anillo, entonces $A[x]$ es un anillo. Además:

- Si A es conmutativo, $A[x]$ es conmutativo
- Si A es D.I., $A[x]$ es D.I.
- Si A es DI entonces $U(A[x])=U(A)$

Observación: Si A es anillo, entonces existe una aplicación inyectiva tal que $A \subseteq A[x]$

Algoritmo de la división. Sea A un anillo. Entonces, para todo $p(x)$ y $q(x) \in A[x]$, $q(x) \neq 0$ y con coeficiente líder una unidad, existen polinomios únicos $c(x)$ y $r(x) \in A[x]$, de forma que:

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

$$\mathrm{gr}(r(x)) < \mathrm{gr}(q(x))$$

A $c(x)$ le llamamos cociente y $r(x)$ es el resto.

Definiciones. Sean $p(x), q(x) \in A[x]$. Diremos que $p(x)$ *divide* a $q(x)$,

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

En este caso, $p(x)$ es *divisor* de $q(x)$ o $q(x)$ es múltiplo de $p(x)$

- $p(x)$ y $q(x)$ son *asociados* sii $\exists u \in U(A[x])$ tal que $q(x) = p(x)\,u$.
- Sean $p(x), q(x) \in A[x]$, no nulos. Llamaremos *máximo común divisor* de $p(x)$ y $q(x)$, y lo notaremos $(p(x), q(x))$ o m.c.d.$\{p(x), q(x)\}$, a todo $d(x) \in A[x]$ verificando:

  i) Es un divisor común:

  $$d(x) \mid p(x) \quad \text{y} \quad d(x) \mid q(x)$$

  ii) Es el mayor de los divisores comunes:

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

- Sean $p(x)$, $q(x) \in A[x]$, no nulos. Llamaremos *mínimo común múltiplo* de $p(x)$ y $q(x)$, y lo notaremos $[p(x), q(x)]$ o m.c.m.$\{p(x), q(x)\}$, a todo $m(x) \in A[x]$ verificando:

  i) Es un múltiplo común:

  $$p(x) \mid m(x) \quad \text{y} \quad q(x) \mid m(x).$$

  ii) Es el menor de los múltiplos comunes:

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

Se verifica la existencia y son únicos salvo asociados.

Proposición. Sean $p(x)$, $q(x) \in A[x]$, no nulos, entonces

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

Algoritmo de Euclides en el anillo de polinomios. Consideremos $\mathbb{K}$ un cuerpo y $a(x)$, $b(x) \in \mathbb{K}[x] - \{0\}$. Entonces

$a(x) = b(x)q_1(x) + r_1(x);$	$gr(r_1(x)) < gr(b(x))$
$b(x) = r_1(x)q_2(x) + r_2(x);$	$gr(r_2(x)) < gr(r_1(x))$
$r_1(x) = r_2(x)q_3(x) + r_3(x);$	$gr(r_3(x)) < gr(r_2(x))$
$\vdots$	$\vdots$
$r_{n-2}(x) = r_{n-1}(x)q_n(x) + \boldsymbol{r_n(x)};$	$gr(r_n(x)) < gr(r_{n-1}(x))$
$r_{n-1}(x) = \boldsymbol{r_n(x)}q_{n+1}(x);$	

y $(a(x), b(x)) = \boldsymbol{r_n(x)}$

Definición. Un *polinomio, p(x),* (no nulo, no unidad) es *irreducible* sii toda descomposición en A[x] de la forma $p(x) = q(x)r(x)$ verifica que $q(x)$ es unidad o $r(x)$ es unidad.

Proposición. Si $\mathbb{K}$ es un cuerpo, entonces $\mathbb{K}[x]$ es un DFU.

RAICES DE UN POLINOMIO

Definición. Llamaremos *raíz* de $p(x)$, a todo elemento $a \in A$ tal que $p(a)=0$.

- Multiplicidad algebraica de a, α.

Teorema (del resto). Si $p(x) \in A[x]$, entonces para cada $a \in A$, existe un único polinomio $c(x) \in A[x]$, tal que

$$p(x) = (x - a)\, c(x) + p(a)$$

Corolario (del factor). Sea $p(x)$ es un polinomio. Entonces:

$$a \text{ es raíz de } p(x) \Leftrightarrow (x - a) \text{ es factor de } p(x)$$

Observemos que un polinomio $p(x)$ *es factor o divisor de* $q(x)$, $p(x) \mid q(x)$, si y sólo si existe un polinomio $c(x)$ tal que $q(x)=c(x)\, p(x)$; esto es, el resto de dividir q(x) entre p(x) es cero.

- Es obvio que todo polinomio factorizará a través de sus raíces, si las tiene; es decir, si *A* es D.I. y $\lambda_1, \lambda_2 \ldots \lambda_k$ son raíces distintas de un polinomio *p(x)* $\in A[x]$, entonces

$$p(x) = a_n (x - \lambda_1)(x - \lambda_2) \ldots (x - \lambda_k)$$

siendo a_n el coeficiente líder de *p(x)*

Corolario. Sea *A* D.I., $p(x) \in A[x]$. Entonces:

1. Si *p(x)* tiene k raíces distintas, entonces gr(*p(x)*)≥k.
2. Si gr(*p(x)*) = k, entonces como máximo tiene k raíces. (***Teorema de Gauss***)

Regla de Ruffini. División por $x - a$

CRITERIOS DE FACTORIZACIÓN DE UN POLINOMIO

- En $\mathbb{Z}$: Un número entero *a es raíz de p(x)* si a es divisor del término independiente de *p(x)*

- En $\mathbb{Q}$: Un número racional *a/b es raíz de p(x)* si *a* es divisor del término independiente de *p(x)* y *b* es divisor del coeficiente líder de *p(x)* (Los polinomios con coeficiente líder 1, no tienen raíces fraccionarias que no sean enteras)

- En $\mathbb{C}$: Si un número complejo *a + bi es raíz de p(x)* entonces su conjugado también es raíz de *p(x)*

Universidad de Jaén

Grado en Ingeniería Informática
ÁLGEBRA

TEMA 1. EL ANILLO DE LOS POLINOMIOS

uja.es