ANILLOS DE POLINOMIOS

Sea A un anillo conmutativo. El conjunto $A[X]$ de polinomios sobre A esta formado por los elementos

$$\sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n.$$

Se definen dos operaciones en $A[X]$, la suma de polinomios

$$(a_0+a_1X+a_2X^2+...+a_nX^n)+(a'_0+a'_1X+a'_2X^2+...+a'_nX^n) =$$

$$(a_0 + a'_0) + (a_1 + a'_1)X + (a_2 + a'_2)X^2 + ... + (a_n + a'_n)X^n$$

y el producto de polinomios

$$(\sum_{i=0}^{n} a_i X^i)(\sum_{i=0}^{m} b_i X^i) = \sum_{i=0}^{n+m} (\sum_{i+j=k} a_i b_j) X^k.$$

Con estas operaciones $A[X]$ es un anillo conmutativo.

Definición. El grado de un polinomio $f \in A[X]$, $gr(f)$, se define como el mayor i tal que $a_i \neq 0$.

Si A es un dominio de integridad $gr(fg) = gr(f) + gr(g)$.

Proposición. Si A es un dominio de integridad, entonces $A[X]$ es un dominio de integridad.

Teorema *Algoritmo de la divisón.* Sea K un cuerpo y $a(x), b(x) \in K[x]$, $b(x) \neq 0$, entonces existen polinomios $q(x)$ y $r(x)$ tales que

$$a(x) = b(x)q(x) + r(x)$$

y se tiene que $r(x) = 0$ o $gr(r) < gr(b)$.

Ceros de polinomios

Definición. Un elemento $a \in F$ se llama un cero o raíz de un polinomio $f(x) \in F[x]$ si $f(a) = 0$.

Teorema del resto. Si $f(x)$ es un polinomio con coeficientes en un cuerpo F, y a está en F, entonces $f(a)$ es el resto de dividir $f(x)$ entre $x - a$.

Teorema de los ceros. Si $f(x) \in F[x]$, F un cuerpo, y $a \in F$, entonces $f(a) = 0$ si y sólo si $x - a$ divide a $f(x)$.

Corolario (*D'Alambert*) Cualquier ecuación de grado n sobre un cuerpo tiene a lo más n ceros.

Corolario Si dos polinomios f y g tienen grado a lo más n en $F[x]$ coinciden en $n+1$ valores entonces $f = g$.

Teorema de Descartes. Si $f(x) = a_n x^n + a_{n-1} x^{n-1} ... + a_1 x + a_0$ está en $\mathbf{Z}[x]$ y tiene a $x = r/s$ como un cero, con r, s primos entre sí, entonces s divide a a_n y r divide a a_0.

Polinomios Irreducibles

Un polinomio p en $F[x]$ es irreducible si p no es una unidad y si $p = fg$ implica que f o g es una unidad.

Proposición. Si p es irreducible y f es un polinomio que no es divisible por p entonces el $mcd(f, p) = 1$.

Factorización en polinomios irreducibles

Teorema de factorización. Cualquier polinomio de grado ≥ 1 en $F[x]$, F un cuerpo, es irreducible o se puede escribir como un producto de polinomios irreducibles.

Definición. Dos polinomios tales que cada uno es un múltiplo escalar del otro se llaman asociados.

Teorema de unicidad de la factorización. En $F[x]$, F un cuerpo, si $f = p_1 p_2 ... p_n = q_1 q_2 ... q_m$ son dos factorizaciones de f como producto de polinomios irreducibles en $F[x]$ entonces $n = m$ y reordenando cada p_i es asociado a un q_i para $i = 1, ..., n$.

Polinomios irreducibles sobre $\mathbf{R}$

Teorema fundamental del álgebra. Cada polinomio $p(x)$ en $\mathbf{C}$ de grado ≥ 1 tiene un cero en $\mathbf{C}$.

Corolario. No existen polinomios irreducibles en $\mathbf{R}[x]$ de grado > 2.

Proposición. Si $f(x) = x^2 + bx + c$ es un polinomio de grado 2 en $\mathbf{R}[x]$, entonces $f(x)$ es irreducible si y sólo si $b^2 - 4c < 0$.

Factorización en $\mathbf{Q}$[x]

Definición. Un polinomio f con coeficientes enteros se llama primitivo si el máximo común divisor de los coeficientes es uno.

Lema de Gauss. Sea $f(x)$ un polinomio con coeficientes enteros. Supongamos que $f(x) = a(x)b(x)$ con $a(x), b(x) \in \mathbf{Q}[x]$. Entonces existen polinomios $a_1(x)$ y $b_1(x)$ en $\mathbf{Z}[x]$ asociados a $a(x)$ y b(x) respectivamente tales que $f(x) = a_1(x)b_2(x)$.

Criterios de irreducibilidad

1. Reducción módulo m Sea $f(x) = x^n + a_{n-1}x^{n-1} ... + a_1x + a_0$ un polinomio mónico en $\mathbf{Z}[x]$, si $\overline{f}(x) = x^n + \overline{a_{n-1}}x^{n-1} ... + \overline{a_1}x + \overline{a_0}$ en $\mathbf{Z}_m[x]$ es irreducible para algún m entonces $f(x)$ es irreducible.

Ejemplo. $x^5 + 2x^3 + x^2 + 4x + 5$ es irreducible.

2. Eisenstein Supongamos $f(x) = a_nx^n + a_{n-1}x^{n-1} ... + a_1x + a_0$ está en $\mathbf{Z}[x]$ y que exista un primo p tal que

i) p divide a $a_{n-1}, ..., a_1, a_0$,

ii) p no divide a a_n,

iii) p^2 no divide a a_0.

Entonces $f(x)$ es irreducible en $\mathbf{Q}[x]$.

Ejemplo. $x^4 + 3x^2 + 6x + 12$

Congruencias módulo un polinomio.

En esta sección los polinomios tienen coeficientes en un cuerpo F.

Definición. Dos polinomios $f(x)$ y $g(x)$ se dicen congruentes módulo otro polinomio $p(x)$ (escribiremos $f(x) \equiv g(x)\ (mod\, p(x))$) si $f(x) - g(x)$ es un múltiplo de $p(x)$.

Ejemplo. En $\mathbf{Z}_2[x]$ se tiene que

$$x^4 + 1 \equiv x^2 + x + 1\ (mod\, x^2 + x + 1).$$

Ecuaciones en congruencias. La ecuación

$$f(x)z(x) \equiv h(x)\ (mod\, p(x))$$

tiene solución en $z(x)$ si y sólo si $mcd(f(x), p(x))$ divide a $h(x)$.

Teorema chino del resto. Sean $a_1(x), ..., a_n(x)$ polinomios arbitrarios y $p_1(x), ..., p_n(x)$ polinomios dos a dos primos relativos . Entonces existe un polinomio $f(x)$ tal que

$$f(x) \equiv a_1(x) \, (mod \, p_1(x))$$
$$\vdots$$
$$f(x) \equiv a_n(x) \, (mod \, p_n(x)).$$

Si $f_1(x)$ y $f_2(x)$ son dos soluciones, entonces

$$f_1(x) \equiv f_2(x) \, (mod \, p_1(x) \cdots p_n(x).$$

Corolario. (Interpolación de polinomios.) Si $r_1, ..., r_n$ son elementos distintos de F y $s_1, ..., s_n$ son elementos arbitrarios de F, existe un único polinomio $q(x)$ en $F[x]$ de grado $< n$ tal que $q(r_i) = s_i$ para cada $i = 1, ..., n$.

Algoritmo de factorización de Berlekamp

Sea $f(x)$ un polinomio de $\mathbf{Z}_p[x]$ de grado d. Sea A la matriz $d \times d$ cuya fila i-ésima es el vector de coeficientes del resto $r_i(x)$ donde

$$x^{ip} = f(x)q_i(x) + r_i(x)$$

para $i = 0, 1, ..., d-1$.

Sea $b = (b_0, b_1, ..., b_{d-1})$ una solución de la ecuación

$$b(A - I) = 0$$

y sea $g(x) = b_0 + b_1 x + ... + b_{d-1}x^{d-1}$.

Si $g(x)$ tiene grado mayor o igual que 1, entonces para algún $s \in \mathbf{Z}_p$, $g(x) - s$ y $f(x)$ tienen un divisor común de grado mayor o igual que 1.

Algoritmo de factorización de Berlekamp

Sea $f(x)$ un polinomio de $\mathbf{Z}_p[x]$ de grado d. Sea A la matriz $d \times d$ cuya fila i-ésima es el vector de coeficientes del resto $r_i(x)$ donde

$$x^{ip} = f(x)q_i(x) + r_i(x)$$

para $i = 0, 1, ..., d-1$.

Sea $b = (b_0, b_1, ..., b_{d-1})$ una solución de la ecuación

$$b(A - I) = 0$$

y sea $g(x) = b_0 + b_1 x + ... + b_{d-1}x^{d-1}$.

Si $g(x)$ tiene grado mayor o igual que 1, entonces para algún $s \in \mathbf{Z}_p$, $g(x) - s$ y $f(x)$ tienen un divisor común de grado mayor o igual que 1.