Polinomios

Sea $(R, +, \cdot)$ un anillo arbitrario, un polinomio en R es una expresión de la forma

$$p(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \dots + a_n x^n$$

donde $n \in \mathbb{N}$, los coeficientes $a_i \in R$ $0 \leq i \leq n$ y x es un símbolo que no está en R, llamado indeterminada.

Vamos a adoptar la convención de que un término $a_i x^i$ donde $a_i = 0$ no necesita ser escrito.

Los polinomios $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{n} b_i x^i$ son iguales

si $a_i = b_i$ para todo $0 \leq i \leq n$

y podemos definir la suma $f(x) + g(x)$ como

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

Para definir el producto de dos polinomios sobre R dados

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{y} \quad g(x) = \sum_{j=0}^{m} b_j x^j$$

definimos

$$f(x) \cdot g(x) = \sum_{k=0}^{n+m} c_k x^k$$

donde $\quad c_k = \sum_{\substack{i+j=k \\ 0 \le i \le n,\ 0 \le j \le m}} a_i b_j .$

Ejemplo: $\quad f(x) = (a_0 + a_1 x) \quad g(x) = (b_0 + b_1 x + b_2 x^2)$

$0 \le i \le 1 \qquad 0 \le j \le 2$

$$f(x) \cdot g(x) = \sum_{k=0}^{3} c_k x^k$$

$c_0 = a_0 b_0 \qquad c_1 = a_0 b_1 + a_1 b_0$

$c_2 = a_0 b_2 + a_1 b_1 \qquad c_3 = a_1 b_2$

$$f(x) \cdot g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1) x^2 + (a_1 b_2) x^3$$

Con estas definiciones de suma y producto se puede ver que el conjunto de polinomios sobre R forma un anillo (Ejercicio)

Def: El anillo formado por los polinomios sobre R con la suma y producto definidos antes se llama **anillo de polinomios** sobre R y se escribe

$$R[x].$$

Def: Sea $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ que no sea el polinomio nulo, entonces podemos suponer que $a_n \neq 0$.

En este caso

- a_n se llama **coeficiente principal**
- a_0 se llama **término constante**
- n se llama **grado del polinomio** y se denote $n = \deg(f) = \deg(f(x))$

Por convención se define $\deg(0) = -\infty$ y si $\deg(f) \leq 0$ decimos que f es un **polinomio constante**

En el caso R es un anillo con unidad 1 y el coeficiente principal de un polinomio es $a_n = 1$ entonces decimos que f es un **polinomio mónico**.

Teorema: Sean $f, g \in R[x]$ entonces

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$$

$$\deg(f.g) \leq \deg(f) + \deg(g)$$

En el caso R sea un dominio integral, entonces

$$\deg(f.g) = \deg(f) + \deg(g)$$

Si identificamos los elementos de R con los polinomios constantes de $R[x]$ podemos pensar a R como un <u>subanillo</u> de $R[x]$ y en este caso tenemos propiedades heredadas.

Teorema: Sea R un anillo, entonces

i) $R[x]$ es conmutativo si y sólo si R es conmutativo

ii) $R[x]$ es un anillo con identidad si y sólo si R es un anillo con identidad

iii) $R[x]$ es un dominio integral si y sólo si R es un dominio integral

(Pruebas de ejercicio: usar teo anterior)

En el caso particular que nos interese $F[x]$ donde F es un cuerpo, podemos también considerar la noción de divisibilidad.

Un polinomio $g(x) \in F[x]$ divide a otro $f(x) \in F[x]$ si existe un polinomio $h(x) \in F[x]$ tal que

$$f(x) = g(x) \cdot h(x).$$

Decimos también que g es un divisor de f o que f es un múltiplo de g.

Teorema (Algoritmo de la división) Sea $g(x) \in F[x]$ y $g \neq 0$. Entonces para cualquier $f \in F[x]$ existen $q, r \in F[x]$ tales que

$$f(x) = q(x) \cdot g(x) + r(x)$$

donde $\deg r < \deg g$.

Def Un polinomio $f \in F[x]$ se dice irreducible sobre F (o también irreducible en $F[x]$ o primo en $F[x]$) si tiene grado positivo y cada vez que $f(x) = g(x) \cdot h(x)$ entonces o bien g o bien h es un polinomio constante.

Si un polinomio en $F[x]$ no es irreducible se llama reducible.

¡Cuidado! La reducibilidad o no de un polinomio depende fuertemente de F.

Ejemplo: $f(x) = x^2 - 2$ es irreducible en $\mathbb{Q}[x]$ pero es reducible en $\mathbb{R}[x]$

$$f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

Los polinomios irreducibles actúan como los números primos:

Lema: Si un polinomio irreducible $p \in F[x]$ divide a un producto $f_1 \dots f_m$ de polinomios en $F[x]$ entonces al menos uno de esos factores $f_1, \dots, f_m$ es divisible por p.

Teorema (Factorización única en $F[x]$) Cualquier polinomio $f(x) \in F[x]$ de grado positivo puede ser escrito de manera única (salvo por el orden) en la forma

$$f = a\, p_1^{e_1} \cdots p_k^{e_k}$$

donde $a \in F$, $p_1, \ldots, p_k$ son polinomios mónicas e irreducibles en $F(x)$ todos distintos y $e_1, \ldots, e_k$ son enteros positivos.

Demostración (por inducción en el grado de f)

PASO BASE: Si $\deg(f) = 1$ (Ejercicio) $f(x) = a \cdot \underbrace{(a^{-1} f(x))}_{P(x).}$

PASO INDUCTIVO: Supongamos ahora que el resultado de la factorización vale para todo polinomio de grado positivo menor a n.

Sea f tal que $\deg(f) = n$. Si f es un polinomio irreducible escribimos

$$f = a \cdot \underbrace{(a^{-1} f)}_{P(x)} \quad \text{donde } a = \text{coef ppal de } f$$

Si f no es irreducible, entonces existen $g, h \in F[x]$ tales que

$$f(x) = g(x) \cdot h(x)$$

con $1 \leq \deg(g) < n$ y $1 \leq \deg h < n$.

Por la hipótesis inductiva, tanto g como h pueden escribirse en la forma deseada y por lo tanto f también.

Para probar la unicidad, supongamos que tenemos dos factorizaciones

$$f = a p_1^{e_1} \cdots p_k^{e_k} = b q_1^{d_1} \cdots q_r^{d_r}$$

Por la def de igualdad y comparación de los coef ppales tenemos que $a = b$.

Como p_1 es mónico e irreducible y p_1 divide a

$$b q_1^{d_1} \cdots q_r^{d_r}$$

por el Lema anterior p_1 debe dividir a un q_i $1 \leq i \leq r$. Como q_i es irreducible y tanto q_i como p_1 son mónicos, debe ser que $p_1 = q_i$. Siguiendo con un argumento similar, podemos ver que los dos factorizaciones son iguales salvo por el orden.

Teorema: Para $f \in F[x]$ el anillo de clases residuales $F[x]/(f)$ es un cuerpo si y solo si f es irreducible en $F[x]$.

Recordemos:

- Un ideal J de un anillo R es un subanillo de R tal que para todo $a \in J$ y $r \in R$ se tiene que $a \cdot r \in J$ y $r \cdot a \in J$.

- Un ideal J se dice que es principal si existe a que lo genera es decir

$$J = (a) = \{r \cdot a : r \in R\}$$ si R es un anillo con unidad

o en general $J = (a) = \{ra + n.a : r \in R \quad n \in \mathbb{Z}\}$

- La clase residual de un $a \in R$ modulo un ideal J denotado por $[a]$ es

$$[a] = a + J = \{a + c : c \in J\}$$

y dos clases son iguales $[a] = [b]$ $(a + J = b + J)$ si $a - b \in J$.

- Como antes se pueden definir

La suma

$$[a]+[b] = (a+J)+(b+J) = (a+b)+J$$
$$= [a+b]$$

el producto

$$(a+J).(b+J) = [a].[b] = [a.b] = (a.b)+J$$

- El anillo de clases residuales de R módulo J se denota R/J y es el anillo formado por las clases módulo J con las dos operaciones anteriores.

En el caso $F[x]/(f)$ tenemos que

(f) es el ideal generado por f

$$(f) = \{ g(x).f(x) \ : \ g(x) \in F[x] \}$$

$[h(x)] \in F[x]/(f)$ si $[h(x)] = h(x) + \underbrace{(f(x))}_{g(x).f(x)}$

$F = \mathbb{F}_p$ $\quad\quad$ $\mathbb{F}_p(x)/(f)$