Anel de polinômios

Seja A um anel (comutativo com 1). Considere o conjunto $\mathcal{A}$ de todas as sequência

$$(a_0, a_1, a_2, \dots), \quad a_i \in A,$$

em que no máximo um número finito dos a_i é $\neq 0$.

Podemos definir operações:

$$(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0+b_0, a_1+b_1, a_2+b_2, \dots),$$

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots),$$

em que

$$c_m = \sum_{i+j=m} a_i b_j, \qquad m = 0, 1, 2, \dots$$

Defina:

$$1 = (1, 0, 0, \dots), \quad X = (0, 1, 0, \dots).$$

Então

$$A \cong \{(a, 0, 0, \dots) \mid a \in A\} = \{a \cdot 1 \mid a \in A\},$$

$$X^m = (\underbrace{0, 0, \dots, 0}_{m \text{ zeros}}, 1, 0, 0, \dots).$$

Daí

$$(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots) = a_0 \cdot 1 + a_1 \cdot X + a_2 \cdot X^2 + \ldots + a_n \cdot X^n.$$

Denota-se tal anel por $A[X]$ (anel de polinômios em 1 variável com coeficientes em A).

Def. Dado $f(X) = a_n X^n + \ldots + a_1 X + a_0 \in A[X]$, com $a_n \neq 0$, dizemos que:

(i) $n = gr\, f$ é o grau do polinômio,

(ii) a_n é o coef. líder,

(iii) dizemos que f é mônica se $a_n = 1$.

Lema. (a) Se A é domínio, então $gr(fg) = gr(f) + gr(g)$.

(b) O anel A é domínio $\Leftrightarrow A[X]$ é domínio.

Def (i) Sejam $f, g \in A[X]$. Dizemos que g divide f se existe $h \in A[X]$ tal que $f = gh$.

(ii) f é dito ser irredutível se $f = gh$, com $g, h \in A[X]$ implica em $g \in (A[X])^*$ $h \in (A[X])^*$.

Seja $\mathbb{F}$ corpo. Então dados $f, g \in \mathbb{F}[X]$, existem $q, r \in \mathbb{F}[X]$ com $r = 0$ ou $gr\, r < gr\, g$ tais que

$$f(X) = g(X)\, q(X) + r(X).$$

Lema. Sejam $f \in \mathbb{F}[X]$ e $\alpha \in \mathbb{F}$. Então $f(\alpha) = 0 \iff (X - \alpha)$ divide f.

Todo ideal de $\mathbb{F}[X]$ é principal, isto é, se $I \subseteq \mathbb{F}[X]$ é ideal, então existe $f(X) \in \mathbb{F}[X]$ com

$$I = (f(X)) = f(X) \cdot \mathbb{F}[X] = \{f(X) g(X) \mid g \in \mathbb{F}[X]\}$$

Se escolhermos f mônico, então o polinômio é único.

Lema. Se f é irredutível, então (f) é maximal.

Todo $f \in \mathbb{F}[X]$ pode ser escrito da forma

$$f(X) = \alpha\, p_1(X) \cdots p_m(X),$$

com $\alpha \in \mathbb{F}$ e $p_1(X), \ldots, p_m(X) \in \mathbb{F}[X]$ mônicos e irredutíveis.

Def. Dados $f, g \in F[X]$, o $mdc(f,g)$ é o polinômio mônico $h \in F[X]$ tal que:

(i) h divide f e g,

(ii) se $h_0 \in F[X]$ divide f e g, então h divide h_0.

Critério de Eisenstein.

Seja $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ e assuma que existe $p \in \mathbb{Z}$ primo tal que: $p \mid a_i$, $i = 0, 1, \ldots, n-1$, $p^2 \nmid a_0$ e $p \nmid a_n$. Então f é irredutível em $\mathbb{Q}[X]$.

Homomorfismos.

Sejam A e B anéis e $\psi : A \to B$ um homomorfismo. Então $\overline{\psi} : A[X] \longrightarrow B[X]$ tal que

$$\overline{\psi}\left(a_n X^n + \cdots + a_1 X + a_0\right) = \psi(a_n) X^n + \cdots + \psi(a_1) X + \psi(a_0).$$

Exemplos (1) Um polinômio em $f \in \mathbb{Z}[X]$, então podemos ver este polinômio em $f \in \mathbb{F}_p[X]$, em que $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$. Isso porque temos

$$\psi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}.$$

(2) Um polinômio $f \in \mathbb{Z}[X]$ pode ser visto como um elemento de $\mathbb{Q}[X]$. Isso porque temos inclusão

$$\mathbb{Z} \longrightarrow \mathbb{Q}.$$

Sejam A e B anéis e assuma que $A \subseteq B$ é subanel ($1_A = 1_B$). Para cada $\alpha \in B$, temos um único homomorfismo de anéis

$$\psi_\alpha : A[X] \longrightarrow B$$

satisfazendo:

$$\psi_\alpha|_A = id_A \ , \ \psi_\alpha(X) = \alpha.$$

Este homomorfismo satisfaz o seguinte: Se $f = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$, então

$$\psi_\alpha(f) = \psi_\alpha(a_n X^n + \cdots + a_1 X + a_0) = \cdots =$$

$$= a_n \alpha^n + \cdots + a_1 \alpha + a_0 =: f(\alpha).$$

Exemplo. Dado $f(X) = X^2 + 1 \in \mathbb{R}[X]$ e $1+i \in \mathbb{C}$, faz sentido calcular $f(1+i) = (1+i)^2 + 1 = \cdots$.

Quocientes

Seja F um corpo e $I \subseteq F[X]$ um ideal. Então existe $p(X) \in F[X]$ tal que $I = (p(X))$. Qual a estrutura de $F[X]/I$?

Seja $\pi : F[X] \longrightarrow F[X]/I$ natural, e identifique

$$1 = \pi(1) = 1 + I$$

$$x = \pi(X) = X + I.$$

Então cada elemento de $F[X]/I$ é da forma $\pi(f(X))$. Mas se $f(X) = a_n X^n + \cdots + a_1 X + a_0$, então

$$\pi(f(X)) = \pi(a_n)(\pi(X))^n + \cdots + \pi(a_1)\pi(X) + \pi(a_0)$$
$$= a_n x^n + \cdots + a_1 x + a_0 = f(x).$$

Então os elementos de $F[X]/I$ são $f(x)$, $f \in F[X]$.

Temos que

$$f(x) = g(x) \iff f - g \in I \iff p \text{ divide } f - g.$$

Como são as operações?

- $f(x)+g(x) = \pi(f(X)) + \pi(g(X)) = \pi\left(f(X)+g(X)\right)$

$= \pi\left((f+g)(X)\right) = (f+g)(x)$,

- $f(x)\cdot g(x) = \pi\left(f(X)\right)\pi(g(X)) = \pi\left(f(X)g(X)\right)$

$= (fg)(x)$.

As operações de $\mathbb{F}[X]/I$ são "as mesmas" que as de $\mathbb{F}[X]$, salvo a relação $p(x)=0$.

O espaço $\mathbb{F}[X]/(p(X))$ é um $\mathbb{F}$-esp. vetorial com base $\{1, x, x^2, \dots, x^{m-1}\}$ em que $m = gr(p)$.

Daí $\dim_{\mathbb{F}} \mathbb{F}[X]/(p(X)) = gr(p)$.

Exemplo. Estude $\mathbb{Q}[X]/(X^3)$.

Então, $\{1, x, x^2, x^3, x^4, \dots\}$ gera $\mathbb{Q}[X]/(X^3)$ como um $\mathbb{Q}$-esp. Entretanto,

$x^3 = 0 \iff X^3 \in (X^3)$ $\left(x^m = 0,\ m \geq 3\right)$

Daí $\{1, x, x^2\}$ é $\mathbb{Q}$-base de $\mathbb{Q}[X]/(X^3)$.

Exemplo. $\mathbb{R}[X]/(X^2+1)$.

Temos que $f = X^2+1$ é irredutível em $\mathbb{R}[X]$.

Daí (X^2+1) é maximal, e portanto, $\mathbb{R}[X]/(X^2+1)$ é corpo.

$$\mathbb{R}[X]/(X^2+1) = \{a+bx \mid a,b \in \mathbb{R}\}, \quad x^2+1=0 \iff x^2 = -1.$$

Temos

$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}, \quad (a+bx \mapsto a+bi)$$

mas como constroi o isomorfismo?

$$\varphi : \mathbb{R}[X] \longrightarrow \mathbb{C}$$

Tal que $\varphi(f(X)) = f(i)$,

$$\ker \varphi = (X^2+1).$$

Daí, por Teo. do Iso. vale o isomorfismo.

Se definisse

$$\varphi(f(X)) = f(-i) \qquad (a+bX \mapsto a-bi)$$

também funciona!

Se

$$\psi : \mathbb{R}[X]/(X^2+1) \longrightarrow \mathbb{C}$$

é isomorfismo, então

$$0 = \psi(X^2+1) = (\psi(X))^2 + 1$$

Isso significa que $\psi(X)$ satisfaz $X^2+1=0$.