Capítulo 1

ANÉIS DE POLINÔMIOS

Neste capítulo apresentaremos um breve, porém importante, estudo sobre Anéis de polinômios.

Definição 1.1: Seja F um corpo. Por *anel de polinômios* na indeterminada x, indicado por $F[x]$, entendemos o conjunto de todas as expressões da forma $a_0 + a_1x + \ldots + a_nx^n$, onde n pode ser qualquer inteiro não negativo e os coeficientes $a_0, a_1, \ldots, a_n$ pertencem a F.

Definição 1.2: Se $p(x) = a_0 + a_1x + \ldots + a_ix^i + \ldots + a_mx^m$ e $q(x) = b_0 + b_1x + \ldots + b_ix^i + \ldots + b_nx^n$ estão em $F[x]$, então $p(x) = q(x)$ se, e somente se, para todo inteiro $i \geq 0$, $a_i = b_i$.

Assim dois polinômios são ditos iguais se, e somente se, seus coeficientes correspondentes são iguais.

Para que $F[x]$ seja um anel precisamos definir uma adição e uma multiplicação de elementos de $F[x]$ de modo que os axiomas estabelecidos para anéis valham para $F[x]$. Então vejamos:

Definição 1.3: Se $p(x) = a_0 + a_1x + \ldots + a_ix^i + \ldots + a_mx^m$ e $q(x) = b_0 + b_1x + \ldots + b_ix^i + \ldots + b_nx^n$, com $n \geq m$, estão ambos em $F[x]$, então

$$p(x) + q(x) = c_0 + c_1x + \ldots + c_ix^i + \ldots + c_nx^n,$$

onde para cada i, $c_i = a_i + b_i$.

Exemplo 1.1: Sejam $p(x) = 1 + x$ e $q(x) = 3 - 2x + x^2$. Considerando $1 + x$ como $1 + x + 0x^2$ de acordo com a definição dada,
$p(x) + q(x) = (1 + x) + (3 - 2x + x^2) = 4 - x + x^2$.

Definição 1.4: Se $p(x) = a_0 + a_1x + \ldots + a_ix^i + \ldots + a_mx^m$ e $q(x) = b_0 + b_1x + \ldots + b_ix^i + \ldots + b_nx^n$, então $p(x) \cdot q(x) = c_0 + c_1x + \ldots + c_ix^i + \ldots + c_kx^k$, onde $c_{i+j} = a_ib_j + a_{i+1}b_{j-1} + a_{i+2}b_{j-2} + \ldots + a_jb_i$, com $i = 0, 1, \ldots, m$, $j = 0, 1, \ldots, n$ *e* $m \leq n$.

Exemplo 1.2: Sejam $p(x) = 1 + x - x^2$ e $q(x) = 2 + x^2 + x^3$.
Neste caso,

$$a_0 = 1,\ a_1 = 1,\ a_2 = -1,\ a_i = 0,\ i \geq 3.$$
$$b_0 = 2,\ b_1 = 0,\ b_2 = 1,\ b_3 = 1,\ b_j = 0,\ j \geq 4.$$

Assim,
$c_0 = a_0b_0 = 2,$
$c_1 = a_1b_0 + a_0b_1 = 2,$
$c_2 = a_2b_0 + a_1b_1 + a_0b_2 = -1,$
$c_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 = 2,$
$c_4 = a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4 = 0,$
$c_5 = a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5 = -1$
$c_6 = a_6b_0 + a_5b_1 + a_4b_2 + a_3b_3 + a_2b_4 + a_1b_5 + a_0b_6 = 0$
$c_k = 0,\ k \geq 6.$

Portanto, de acordo com nossa definição, $p(x) \cdot q(x)$ é:
$(1 + x - x^2)(2 + x^2 + x^3) = c_0 + c_1x + \ldots + c_kx^k = 2 + 2x - x^2 + 2x^3 - x^5$.

Dessa forma, afirmamos que $F[x]$ é um anel com estas operações, cuja multiplicação é comutativa e possui elemento unidade.

Definição 1.5: Seja $f(x) = a_0 + a_1x + \ldots + a_nx^n$, não nulo. Se $a_n \neq 0$, então o grau de $f(x)$, indicado por $gr[f(x)]$, é n.

Isto é, o grau de $f(x)$ é o maior inteiro i para o qual o i-ésimo coeficiente de $f(x)$ é diferente de 0. Dizemos que o polinômio é *constante* se seu grau é zero.

Proposição 1.1: Se $f(x)$, $g(x)$ são dois elementos não nulos de $F[x]$, então $gr[(f(x) \cdot g(x))] = gr[f(x)] + gr[g(x)]$.

Demonstração: Suponhamos que $f(x) = a_0 + a_1x + \ldots + a_mx^m$ e $g(x) = b_0 + b_1x + \ldots + b_nx^n$ e que $a_m \neq 0$ e $b_n \neq 0$. Portanto, $gr[f(x)] = m$ e $gr[g(x)] = n$. Pela definição, $f(x) \cdot g(x) = c_0 + c_1x + \ldots + c_kx^k$ onde $c_k = a_kb_o + a_{k-1}b_1 + \ldots + a_1b_{k-1} + a_0b_k$. Afirmamos que $c_{m+n} = a_mb_n \neq 0$ e $c_i = 0$ para $i > m + n$. Que $c_{m+n} = a_mb_n$ pode ser visto imediatamente por sua definição. c_i é a soma dos termos da forma a_jb_{i-j}; como $i = j + (i - j) > m + n$, então $j > m$ ou $i - j > n$. Mas então a_j ou b_{i-j} é 0, de modo que $a_jb_{i-j} = 0$; como c_i é a soma de um feixe de zeros ele também é zero, e nossa afirmação foi estabelecida. Assim o maior coeficiente não nulo de $f(x) \cdot g(x)$ é c_{m+n}, donde $gr[f(x) \cdot g(x)] = m + n = gr[f(x)] + gr[g(x)]$. ■

Corolário 1.1.1: Se $f(x)$, $g(x)$ são elementos não nulos em $F[x]$, então $gr[f(x)] \leq gr[f(x) \cdot g(x)]$.

Demonstração: Como $gr[f(x)g(x)] = gr[f(x)] + gr[g(x)]$, e $gr[g(x)] \geq 0$ o resultado é imediato a partir da Proposição 1.1. ■

Corolário 1.1.2: $F[x]$ é um anel de integridade.

Proposição 1.2 (O algorítimo da divisão) Dados dois polinômios $f(x)$ e $g(x) \neq 0$ em $F[x]$, então existem dois polinômios $t(x)$ e $r(x)$ em $F[x]$ tais que $f(x) = t(x) \cdot g(x) + r(x)$, onde $r(x) = 0$ ou $gr[r(x)] < gr[g(x)]$.

Definição 1.6: Um polinômio $p(x)$ em $F[x]$ é dito *irredutível* sobre F se sempre que $p(x) = a(x) \cdot b(x)$, com $a(x)$, $b(x) \in F[x]$, então $a(x)$ ou $b(x)$ tem grau 0 (isto é, uma constante).

A irredutibilidade depende do corpo; por exemplo, o polinômio $x^2 + 1$ é irredutível sobre o corpo real mas não o é sobre o corpo complexo, pois neste caso $x^2 + 1 = (x + i)(x - i)$, onde $i^2 = -1$.

Exemplo 1.3: Considerando $f(x) = x^3 + x + \overline{1} \in \mathbb{Z}_5[x]$ temos que $f(x)$ é irredutível sobre $\mathbb{Z}_5$.

De fato: $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

$f(\overline{0}) = \overline{0}^3 + \overline{0} + \overline{1} = \overline{1}$

$f(\overline{1}) = \overline{1}^3 + \overline{1} + \overline{1} = \overline{1} + \overline{1} + \overline{1} = \overline{3}$

$f(2) = \overline{2}^3 + \overline{2} + \overline{1} = \overline{3} + \overline{2} + \overline{1} = \overline{1}$

$f(\overline{3}) = \overline{3}^3 + \overline{3} + \overline{1} = \overline{2} + \overline{3} + \overline{1} = \overline{1}$

$f(\overline{4}) = \overline{4}^3 + \overline{4} + \overline{1} = \overline{4} + \overline{4} + \overline{1} = \overline{4}$

Assim, não existe $\alpha \in \mathbb{Z}_5$ tal que $f(\alpha) = \alpha^3 + \alpha + \overline{1} = 0$. Logo $f(x)$ é irredutível sobre $\mathbb{Z}_5$, isto é, $f(x) = \overline{1} \cdot f(x)$, $\overline{1} \in \mathbb{Z}_5[x]$.