ANÉIS DE POLINÔMIOS

Seja R um anel comutativo com unidade.
Uma sequência de elementos de R é uma função $f: \mathbb{N} = \{0, 1, 2, 3, \ldots\} \longrightarrow R$.
Para cada $n \in \mathbb{N}$, $f(n) = a_n \in R$.
Denotamos a sequência por $(a_n)_{n \in \mathbb{N}}$.

DEF: Uma sequência $(a_n)_{n \in \mathbb{N}}$ é QUASE NULA se existir $N \in \mathbb{N}$ tq $a_n = 0$ $\forall n > N$.
(Se $N = 0$, então $(a_n)_{n \in \mathbb{N}}$ é tq $a_n = 0$, $\forall n > 0$. Essa é a sequência nula, que é, obviamente quase-nula.) (Na sequência nula $a_0 = 0$ também)

Seja $Q = \{$ sequências quase-nulas de elementos de $R \}$

Vamos definir em Q duas operações, adição e multiplicação.
- Sejam $(a_n)_{n \in \mathbb{N}}$ e $(b_n)_{n \in \mathbb{N}}$ elementos de Q.

Definimos
$$+ : Q \times Q \longrightarrow Q$$
$$\left((a_n)_{n \in \mathbb{N}}, (b_n)_{n \in \mathbb{N}} \right) \stackrel{+}{\longmapsto} (c_n)_{n \in \mathbb{N}}.$$
onde $c_n = a_n + b_n$ $\forall n$
soma no anel

$$\cdot : Q \times Q \longrightarrow Q$$
$$\left((a_n)_{n \in \mathbb{N}}, (b_n)_{n \in \mathbb{N}} \right) \stackrel{\cdot}{\longrightarrow} (c_n)$$
onde $c_n = \sum_{i=0}^{n} a_{n-i} \cdot b_i$ $\forall n \in \mathbb{N}$,
mult. no anel

Precisamos mostrar que $(Q,+,\cdot)$ é um anel com as operações assim definidas.
Antes de todo, ver porque $+$ e $\cdot$ estão bem definidas.

Para a adição:

Sejam $(a_n), (b_n) \in Q$. Mostrar que $(a_n)+(b_n) \in Q$.

Como (a_n) e (b_n) estão em Q, existem inteiros N_1 e N_2 em $\mathbb{N}$ tal que

$a_n = 0 \quad \forall\ n > N_1$. Se $N = \max\{N_1, N_2\}$,
$b_n = 0 \quad \forall\ n > N_2$
é claro que $a_n + b_n = 0 \quad \forall\ n > N$.

É fácil ver que $(Q,+)$ é um grupo abeliano.
$0 = (0,0,0,\ldots\ldots)$ é o elemento neutro da adição
$(a_n) \in Q$, $-(a_n) = (-a_n)$

E é claro que as propriedades associativa e comutativa para a adição são válidas em Q porque valem em $\mathbb{R}$.

Para a multiplicação já é mais complicado! (Ou trabalhoso)

Primeiro temos que mostrar que $(a_n)\cdot(b_n)$ é uma sequência quase-nula se $(a_n), (b_n) \in Q$.

Mostrar que se $(a_n), (b_n) \in Q \Rightarrow$
$(a_n)(b_n) \in Q$,

Sejam $N_1 \in \mathbb{N}$ tal que $a_n = 0 \ \forall n > N_1$ e
$N_2 \in \mathbb{N}$ tal que $b_n = 0 \ \forall n > N_2$.

Vamos provar que $c_n = 0 \ \forall n > N_1 + N_2$,

Seja então $\underline{n > N_1 + N_2}$

$$c_n = a_0 b_n + a_1 b_{n+1} + \dots + a_{N_1} b_{n-N_1} + a_{N_1+1} b_{n-(N_1+1)}$$
$$+ \dots + a_{N_1+N_2} b_{n-(N_1+N_2)} + \dots + a_n b_0$$
$$= \underbrace{\sum_{i=0}^{N_1} a_i b_{n-i}}_{(I)} + \underbrace{\sum_{i=N_1+1}^{n} a_i b_{n-i}}_{(II)}$$

Em (I): $0 \leq i \leq N_1 \Rightarrow 0 \geq -i \geq -N_1$
$\Rightarrow n \geq n-i \geq n - N_1 > N_2$
$b_{n-i} = 0$, já que $n-i > N_2$.

Em (II), $a_i = 0$, pois $i > N_1$.

Logo $(I) + (II) = 0$, $c_n = 0$ se $n > 0 \ \forall$
$n > N_1 + N_2$,

Assim, $(a_n)(b_n) \in Q$.

(Note que se $n = N_1 + N_2$, então
$(I) = a_{N_1} b_{N_2}$ e $II = 0$, pois $a_i = 0$ para $i >$

Seja agora $(a_n) \in Q$, $(a_n) \neq 0$.

Definimos

$$\boxed{\text{grau}\,(a_n) = \max\{n \in \mathbb{N} \mid a_n \neq 0\}}$$

Seja $S = \{n \mid a_n \neq 0\}$

$S \neq \phi$, pois $(a_n) \neq 0$.

S é limitado superiormente, pois (a_n) é quase nula (existe $N \in \mathbb{N}$ tal que $a_n = 0$ para todo $n > N$).

Logo, pelo Princípio da Boa Ordem, S tem máximo.

O grau da sequência nula não é definido, se você quiser pode colocar grau $0 = -\infty$.

Pelo que foi visto anteriormente temos:

$$\text{grau}\,((a_n) + (b_n)) \leq \max\{\text{grau}\,(a_n), \text{grau}\,(b_n)\}$$

$$\text{grau}\,((a_n)(b_n)) \leq \text{grau}\,(a_n) + \text{grau}\,(b_n).$$

Observação 1

$$\text{grau}\,(a_n) = \min\{N \in \mathbb{N} \text{ tq } a_n = 0 \ \forall n > N\}$$

Observação 2

Se R é um domínio de integridade, então $\text{grau}\,(a_n)(b_n) = \text{grau}\,(a_n) + \text{grau}\,(b_n)$.

Agora, só falta provar que
$(Q, +, \cdot)$ é um anel comutativo
com unidade.

Para isso ainda falta verificar que
$$((a_n)(b_n))(c_n) = (a_n)((b_n)(c_n))$$
$$(a_n)(b_n) = (b_n)(a_n)$$
Existe $1 \in Q$ tq $(a_n) \cdot 1 = 1 \cdot (a_n)$ $\forall (a_n) \in Q$
$$(a_n)[(b_n) + (c_n)] = (a_n)(b_n) + (a_n)(c_n).$$
(Verifique!)

$\boxed{Q \text{ é o anel de polinômios!}}$

Em Q sejam $0 = (0, 0, \ldots)$
$1 = (1, 0, \ldots)$

Seja $X = (0, 1, 0, \ldots)$.

ou seja $X = (a_n)$, onde $a_n = 0$ se $n \neq 1$ e $a_1 = 0$

Vamos mostrar que para todo $r \geq 1$
$X^r = (b_n)$, onde $\begin{cases} b_n = 0 \text{ se } x \neq r \\ b_r = 1 \end{cases}$

Por indução em r.

Se $r = 1$, OK

Suponha que $r \geq 1$ e que

$X^r = (b_n)$ onde $b_n = \begin{cases} 1 & \text{se } n = r \\ 0 & \text{se } n \neq r \end{cases}$

Então $X^r . X = (b_n)(a_n) =$

(c_n), onde $c_n = \sum_{i+j=n} b_i a_j$.

Se $i \neq r$ ou $j \neq 1$ temos que

$b_i a_j = 0$.

Assim só temos $i = r$ e $j = 1$ que é

$c_{r+1} = b_r a_1 = \underline{1}$

Logo (c_n) é a sequência

$c_n = 0$ se $n \neq r+1$

$c_{r+1} = 1$

Assim $X^r X = X^{r+1}$. ▫

Assim $X^m = (x_n)$, com $\begin{cases} x_n = 0 \text{ se } n \neq m \\ x_m = 1 \end{cases}$

$\forall\, m \geq 1$.

Mostre que $(a, 0, \ldots). X^m$

$= (0, 0, \ldots, 0, \underset{\substack{\uparrow \\ m}}{a}, 0, \ldots)$

Assim, se (a_n) é uma sequência quase nula qualquer. temos que

$$(a_n) = (a_0, a_1, a_2, \ldots, a_N, 0, \ldots)$$

$$= (a_0, 0, \ldots)(1, 0, \ldots) + (a_1, 0, \ldots)(0, 1, 0, \ldots) + \ldots + (a_N, 0, \ldots)(0, \ldots, 0, \underset{\underset{N}{\downarrow}}{1}, 0, \ldots)$$

Se $\varphi : R \to Q$ é tal que

$\varphi(a) = (a, 0, \ldots, 0)$

φ é homo de anéis e é injetora.

Assim *identificamos $a \in R$ um elemento do anel R, com $(a, 0, \ldots, 0, \ldots) \in Q$.

Assim, (a_n) é igual a

$a_0 + a_1 X + \ldots + a_N X^n$.

Escrevemos $Q = R[X]$, ANEL DOS POLINÔMIOS COM COEFICIENTES em R na indeterminada

um elemento em Q

$$f(X) = \sum_{i=0}^{N} a_i X^i$$ polinômio com coeficientes em R na indeterminada X,

*(Na verdade, é "renomear" $(a, 0, \ldots, 0)$ como simplesmente a.)

Já temos que:

PROPOSIÇÃO: Se R é um domínio de integridade, então $R[X]$ é um domínio de integridade.

Se K é um corpo, é claro que $K[X]$ é um domínio de integridade.

O corpo de frações de $K[X]$, denotado por $K(x)$ é chamado de corpo das frações racionais.