WYKŁAD 4

4. Konstrukcja pierścienia wielomianów jednej zmiennej

<u>Uwaga 1:</u> Niech $(P,+,\cdot)$ będzie pierścieniem. W zbiorze:

$$P^{\mathbb{N}} = \{(a_n)_{n\in\mathbb{N}} : a_n \in P,\ n\in\mathbb{N}\}$$

ciągów elementów pierścienia P określamy:

- element zerowy:

$$(0,0,0,\dots)$$

- jedynkę:

$$(1,0,0,\dots)$$

- dodawanie jako:

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n+b_n)_{n\in\mathbb{N}}$$

- element przeciwny względem dodawania:

$$-(a_n)_{n\in\mathbb{N}} = (-a_n)_{n\in\mathbb{N}}$$

- mnożenie – iloczyn Cauchy'ego:[*]

$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}},\quad c_n = \sum_{i=0}^{n} a_{n-i} b_i$$

Wówczas $(P^{\mathbb{N}},+,\cdot)$ jest pierścieniem. Nazywamy go <u>pierścieniem formalnych szeregów potęgowych jednej zmiennej o współczynnikach z P</u> ∎

<u>Uwaga 2:</u> Niech $(P,+,\cdot)$ będzie pierścieniem, $(P^{\mathbb{N}},+,\cdot)$ pierścieniem jego szeregów potęgowych. Wówczas odwzorowanie $\varphi: P \to P^{\mathbb{N}}$ dane wzorem:

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

jest [illegible] [illegible] pierścieni. ∎

<u>Uwaga terminologiczna:</u> Niech $(P,+,\cdot)$ będzie pierścieniem, $(P^{\mathbb{N}},+,\cdot)$ pierścieniem jego szeregów potęgowych. [illegible] [illegible] jest [illegible] [illegible]:

$$a := (a,0,0,0,\dots) \qquad \text{dla } a\in P$$

$$X := (0,1,0,0,\dots)$$

Wynika stąd przez indukcję: [illegible]

$$X^n = (0,0,\dots,0,\underset{n}{1},0,\dots)$$

$$aX^n = (0,0,\dots,0,\underset{n}{a},0,\dots)$$

$$\sum_{n=0}^{m} a_n X^n = a_0 + a_1X + \dots + a_mX^m = (a_0,a_1,\dots,a_m,0,\dots)$$

$$\sum_{n=0}^{\infty} a_n X^n = a_0 + a_1X + \dots = (a_0,a_1,\dots)$$

Z kolei [illegible] dodawanie, element przeciwny i mnożenie [illegible] jako:

$$\sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty} (a_n+b_n) X^n$$

$$-\sum_{n=0}^{\infty} a_n X^n = \sum_{n=0}^{\infty} -a_n X^n$$

$$\sum_{n=0}^{\infty} a_n X^n \cdot \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_{n-i} b_i\right) X^n$$

Pierścień [illegible] [illegible] [illegible] oznaczamy $P[[X]]$ a jego elementy [illegible]:

$$f = [illegible] = \sum_{n=0}^{\infty} a_n X^n$$ ∎

---

[*] A. L. Cauchy (1789–1857) – matematyk francuski

Uwaga 3: Niech $(P,+,\cdot)$ będzie pierścieniem, $(P[[X]],+,\cdot)$ pierścieniem jego szeregów formalnych. Zbiór:

$$P[X] = \{ \sum_{n=0}^{\infty} a_n X^n : a_n = 0 \text{ dla prawie wszystkich } n \in \mathbb{N} \}$$

jest podpierścieniem pierścienia $P[[X]]$ i nazywamy go pierścieniem wielomianów jednej zmiennej o współczynnikach z P ■

Def.: Niech $(P,+,\cdot)$ będzie pierścieniem, $(P[X],+,\cdot)$ pierścieniem wielomianów o współczynnikach z P. Niech ponadto:

$$f(X) = \sum_{n=0}^{m} a_n X^n \in P[X]$$

(i) Elementy $a_0, a_1, \ldots, a_m$ nazywamy współczynnikami wielomianu f.

(ii) Współczynnik a_0 nazywamy wyrazem wolnym wielomianu f.

(iii) Współczynnik a_m nazywamy najstarszym (najwyższym) współczynnikiem wielomianu f.

(iv) Wielomian nazywamy unormowanym, jeśli jego najstarszy współczynnik to 1

(v) Liczbę:

$$\deg(f) = \begin{cases} m, & \text{jeśli } \quad m > 0 \text{ lub } m = 0 \text{ i } a_0 \neq 0 \\ -\infty, & \text{jeśli } \quad m = 0 \text{ i } a_0 = 0 \end{cases}$$

nazywamy stopniem wielomianu f.

(vi) Wielomian:

$$f(X) = X$$

nazywamy zmienną.

(vii) Wielomian:

$$f(X) = a_0$$

nazywamy wielomianem stałym ■

Umowa notacyjna: Przy liczeniu stopni wielomianów przyjmujemy umowę:

- $\bigwedge_{n \in \mathbb{N}} \quad n > -\infty$
- $(-\infty) + (-\infty) = -\infty$
- $\bigwedge_{n \in \mathbb{N}} \quad -\infty + n = -\infty$ ■

Uwaga 4: Niech $(P,+,\cdot)$ będzie pierścieniem, $(P[X],+,\cdot)$ pierścieniem wielomianów o współczynnikach z P. Niech ponadto:

$$f(X) = \sum_{k=0}^{m} a_k X^k \in P[X], \quad g(X) = \sum_{k=0}^{n} b_k X^k \in P[X]$$

(i) $\deg(f \cdot g) \leqslant \deg(f) + \deg(g)$

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

(iii) Jeśli:

$$f \neq 0 \quad \wedge \quad g \neq 0 \quad \wedge \quad (a_m - \text{regularny} \quad \vee \quad b_n - \text{regularny})$$

to:

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

(iv) Jeśli:

$$\deg(f) \neq \deg(g)$$

to:

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

(v) Jeśli:

$$f \neq 0 \quad \wedge \quad g \neq 0 \quad \wedge \quad P \text{ - całkowity}$$

to:

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

<u>Dowód:</u>

(i) Niech $h = f\cdot g = \sum_{k=0}^{\infty} c_k X^k$, prawie wszystkie $c_k = 0$

Ustalmy $k > n+m = \deg(f) + \deg(g)$. Mamy:

$$c_k = \sum_{i=0}^{k} a_{k-i} b_i$$

Jeśli $i \in \{0,\dots,m\}$, to $k-i \in \{n+1,\dots,k\}$, więc $a_{k-i} = 0$

Jeśli $i \in \{m+1,\dots,k\}$ to $b_i = 0$.

Zatem $c_k = 0$, a więc $\deg(f\cdot g) \leqslant \deg(f) + \deg(g)$

(ii) Niech $h = f+g = \sum_{k=0}^{\infty} c_k X^k$, prawie wszystkie $c_k = 0$

Ustalmy $k > \max\{n,m\} = \max\{\deg(f), \deg(g)\}$. Mamy:

$$c_k = a_k + b_k = 0 + 0 = 0$$

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

(iii) Niech $h = f\cdot g = \sum_{k=0}^{\infty} c_k X^k$ prawie wszystkie $c_k = 0$. Mamy:

$$c_{n+m} = \sum_{i=0}^{n+m} a_{n+m-i} b_i = \underset{0}{a_{n+m}} b_0 + \underset{0}{a_{n+m-1}} b_1 + \dots + a_n b_m + a_{n-1} \underset{0}{b_{m+1}} + \dots + a_0 \underset{0}{b_{n+m}} =$$

$$= a_n b_m$$

Ponieważ a_n lub b_m jest regularny, więc $c_{n+m} \neq 0$

(iv): oczywiste

(v): wynika z (iii) <u>QED</u>

<u>Wniosek 1:</u> Niech $(P,+,\cdot)$ będzie pierścieniem, $(P[X],+,\cdot)$ pierścieniem wielomianów o współczynnikach z P. Niech ponadto:

$$f(X) = \sum_{k=0}^{n} a_k X^k \in P[X]$$

(i) Jeśli a_n jest regularny w P, to $f(X)$ jest regularny w $P[X]$

(ii) Każdy wielomian unormowany jest elementem regularnym w $P[X]$

(iii) Jeśli P jest całkowity, to $P[X]$ jest całkowity ∎

<u>Tw. 1 (o dzieleniu wielomianów z resztą):</u> Niech $(P,+,\cdot)$ będzie pierścieniem, $(P[X],+,\cdot)$ pierścieniem wielomianów o współczynnikach z P. Niech ponadto:

$$f(X) = \sum_{k=0}^{n} a_k X^k \in P[X], \quad g(X) = \sum_{k=0}^{m} b_k X^k \in P[X]$$

Wówczas istnieje liczba $l \in \mathbb{N} \cup \{0\}$ oraz wielomiany $q(X), r(X) \in P[X]$ takie, że:

$$a_n^l g(X) = q(X) \cdot f(X) + r(X)$$

oraz $\deg(r) < \deg(f)$

<u>Dowód:</u>

Jeśli $\deg(g) = m < n = \deg(f)$, to $l = 0$, $q(X) = 0$, $r(X) = g(X)$

Jeśli $\deg(g) = m = n = \deg(f)$, to $l = 1$, $q(X) = b_m$, $r(X) = a_n g(X) - b_m f(X)$

Istotnie, zauważmy że $\deg(r) < n = \deg(f)$

Jeśli $\deg(g) = m > n = \deg(f)$, to zasadę przeprowadzimy metodą indukcji po $\deg(g) = m$.

Załóżmy, że dla $m_1 \in \{n+1,\dots,m-1\}$ i dla wielomianu:
$$g_1(X) = \sum_{k=0}^{m_1} b_k^1 X^k \in P[X]$$
istnieje liczba $l_1 \in \mathbb{N}\cup\{0\}$ oraz wielomiany $h_1(X), r_1(X) \in P[X]$ takie, że:
$$a_n^{l_1} g_1(X) = h_1(X)\cdot f(X) + r_1(X)$$
oraz $\deg(r_1) < \deg(f)$.

Połóżmy:
$$g_1(X) := a_n g(X) - b_m X^{m-n} f(X)$$
Mamy, że:
$$\deg(g_1) \in \{n+1,\dots,m-1\}$$
zatem istnieje liczba $l_1 \in \mathbb{N}\cup\{0\}$ oraz wielomiany $h_1(X), r_1(X)\in P[X]$ takie, że:
$$a_n^{l_1} g_1(X) = h_1(X)\cdot f(X) + r_1(X) \quad \text{oraz} \quad \deg(r_1)<\deg(f)$$
czyli:
$$a_n^{l_1}(a_n g(X) - b_m X^{m-n} f(X)) = h_1(X)\cdot f(X) + r_1(X) \quad \text{oraz } \deg(r_1)<\deg(f)$$
$$a_n^{l_1+1} g(X) = (h_1(X)+a_n^{l_1} b_m X^{m-n}) f(X) + r_1(X) \quad \text{oraz } \deg(r_1)<\deg(f)$$
Więc kładąc $l = l_1+1$, $h(X) = h_1(X) + a_n^{l_1} b_m X^{m-n}$ oraz $r(X)=r_1(X)$, otrzymujemy tezę. QED

<u>Wniosek 2:</u> Niech $(P,+,\cdot)$ będzie pierścieniem, $(P[X],+,\cdot)$ pierścieniem wielomianów o współczynnikach z P. Niech ponadto:
$$f(X)=\sum_{k=0}^n a_k X^k \in P[X], \quad g(X)=\sum_{k=0}^m b_k X^k\in P[X]$$
(i) Jeśli $a_n = 1$, to istnieją wielomiany $h(X), r(X)\in P[X]$ takie, że:
$$g(X) = h(X)\cdot f(X)+r(X)$$
oraz $\deg(r)<\deg(f)$

(ii) Jeśli $a_n \in U(P)$, to istnieją wielomiany $h(X), r(X)\in P[X]$ takie, że:
$$g(X) = h(X)\cdot f(X)+r(X)$$
oraz $\deg(r)<\deg(f)$

(iii) Jeśli P jest ciałem, to istnieją wielomiany $h(X), r(X)\in P[X]$ takie, że:
$$g(X) = h(X)\cdot f(X)+r(X)$$
oraz $\deg(r)<\deg(f)$

<u>Dowód:</u>

(i): oczywiste

(ii): $a_n^{-1}a_n = 1$, zatem istnieją wielomiany $h_1(X), r_1(X)\in P[X]$ takie, że:
$$g(X) = h_1(X)\, a_n^{-1} f(X) + r_1(X)$$
oraz $\deg(r_1) < \deg(a_n^{-1} f) = \deg(f)$. Zatem kładąc $h(X) = h_1(X)a_n^{-1}$ oraz $r(X) = r_1(X)$ otrzymujemy tezę

(iii): wynika z (ii) QED

<u>Tw. 2 (o jednoznaczności dzielenia z resztą):</u> Niech $(P,+,\cdot)$ będzie pierścieniem, $(P[X],+,\cdot)$ pierścieniem wielomianów o współczynnikach z P. Niech ponadto:
$$f(X)=\sum_{k=0}^n a_k X^k \in P[X], \quad g(X)=\sum_{k=0}^m b_k X^k\in P[X]$$
Jeśli a_n jest regularny, to istnieje co najwyżej jedna para takich wielomianów $h(X), r(X)\in P[X]$, że:
$$g(X) = h(X)\cdot f(X) + r(X)$$
oraz $\deg(r)<\deg(f)$

<u>Dowód:</u> Niech:

$$g(X) = h_1(X)\cdot f(X) + r_1(X), \quad \deg r_1 < \deg f, \quad h_1(X), r_1(X) \in P[X]$$
$$g(X) = h_2(X)\cdot f(X) + r_2(X), \quad \deg r_2 < \deg f, \quad h_2(X), r_2(X) \in P[X]$$

Stąd:

$$0 = (h_1(X) - h_2(X))\cdot f(X) + r_1(X) - r_2(X)$$
$$r_2(X) - r_1(X) = (h_1(X) - h_2(X))\cdot f(X)$$

Wobec uwagi 2.(iii):

$$\deg(f) > \deg(r_2 - r_1) = \deg((h_1 - h_2) f) = \deg(h_1 - h_2) + \deg(f)$$

Zatem $\deg(h_1 - h_2) = -\infty$, a więc $h_1(X) - h_2(X) = 0$, skąd też $r_2(X) = r_1(X)$ <u>QED</u>

<u>Wniosek 3:</u> Niech $(P,+,\cdot)$ będzie pierścieniem, $(P[X],+,\cdot)$ pierścieniem wielomianów o współczynnikach z P. Niech ponadto:

$$f(X) = \sum_{k=0}^{n} a_k X^k \in P[X], \quad g(X) = \sum_{k=0}^{m} b_k X^k \in P[X]$$

(i) Jeśli P jest całkowity, to istnieje co najwyżej jedna para takich wielomianów $h(X), r(X) \in P[X]$, że:

$$g(X) = h(X)\cdot f(X) + r(X)$$

oraz $\deg r < \deg f$

(ii) Jeśli $a_n = 1$, to istnieje dokładnie jedna para takich wielomianów $h(X), r(X) \in P[X]$, że:

$$g(X) = h(X)\cdot f(X) + r(X)$$

oraz $\deg r < \deg f$

(iii) Jeśli $a_n \in U(P)$, to istnieje dokładnie jedna para takich wielomianów $h(X), r(X) \in P[X]$, że:

$$g(X) = h(X)\cdot f(X) + r(X)$$

oraz $\deg r < \deg f$

(iv) Jeśli P jest ciałem, to istnieje dokładnie jedna para takich wielomianów $h(X), r(X) \in P[X]$, że:

$$g(X) = h(X)\cdot f(X) + r(X)$$

oraz $\deg r < \deg f$ ■

<u>Def. 2:</u> Niech $(P,+,\cdot)$ będzie pierścieniem, $(P[X],+,\cdot)$ pierścieniem wielomianów o współczynnikach z P. Niech ponadto:

$$f(X) = \sum_{k=0}^{n} a_k X^k \in P[X], \quad g(X) = \sum_{k=0}^{m} b_k X^k \in P[X]$$

Jeśli istnieją wielomiany $h(X), r(X) \in P[X]$ takie, że:

$$g(X) = h(X)\cdot f(X) + r(X)$$

oraz $\deg r < \deg f$ to mówimy, że w pierścieniu $P[X]$ wykonalne jest <u>dzielenie z resztą</u> wielomianu g przez wielomian f. Wielomian $h(X)$ nazywamy <u>ilorazem</u>, a wielomian $r(X)$ <u>resztą</u> ■